UNIVERSITAT DE BARCELONA

Protection of personal data in cyberspace: the EU-US E-market regime

Tossapon Tassanakunlapan

UNIVERSITAT DE BARCELONA

FACULTAT DE DRET

Programa de Doctorat en Dret i Ciència Política
Línia d'Investigació: Dret internacional públic i relacions internacionals

PROTECTION OF PERSONAL DATA IN CYBERSPACE: THE EU-US E-MARKET REGIME

Directora: Dra.MILAGROS CARMEN ALVAREZ VERDUGO
Tutor: Dr.ANDREU OLESTI RAYO

TOSSAPON TASSANAKUNLAPAN

BARCELONA, 2017

Protection of personal data in Cyberspace: the EU-US E-Market regime

Abstract

The object of study of this research is the right to Personal Data Protection within the framework of the EU-US E-Market legal regime. Its characteristics, as well as the features of the main actors participating into that E-Market, make possible to consider it as a proper basis for the development of an International/Universal legal system treaty-based.

The Actors and Relations included by the research are the duty bearers of Personal Data Protection law, both State and Private Entity Activities. Nonetheless, the Informal Power Relation between State and Private organization is also taken into account since there are some informal agreements or coordination between State Agencies and IT Corporations on data sharing and processing. The time frame of the research is 2001-2016 (after the terrorist's attack in USA on 9/11 until the most recent reform of the EU-US E-Market regime in 2016).

The research's point of departure is International Human Rights Law, as far as it recognizes a general framework to support and regulate personal data protection on cyberspace realm. Nonetheless, the distinctive characters of cyberspace demand a well designed, at universal level, specific regulation and mechanisms to guarantee such fundamental rights relating personal data protection internationally. Accordingly, Research Hypothesis is represented in double issues: first, effective personal data protection on cyberspace needs the establishment of an International/Universal legal system treaty-based; second, EU Regime on personal data protection in cyberspace and current EU-US agreements on this issue can be used as a model for initiating such International/Universal Treaty.

The structure of the thesis is divided into six chapters, being Chapter 1 the research design and Chapter 6 the conclusions and recommendations coming from the research. So, Chapter 2 analyzes Universal Legal Instruments, EU Laws and EU-US Agreements in force before 5th June 2013 (critical turning point date because of the revelations of Mass Electronic Surveillance presented then on World Wide Web).

Within this legal framework, Chapter 3 studies hard cases about personal data protection in US domestic courts and in the Court of Justice of European Union, in order to search for precise interpretation of the right to personal data protection in cyberspace that, later, had to be taken into account by US and EU in their further legal reforms. Chapter 4 analyses and reviews the legal instruments enacted through the reform of the EU personal data protection regime and the new EU-US Bilateral Agreements currently in force. Finally, Chapter 5 evaluates the possibility to initiate an International Treaty for regulating data using across borders. Considering the initiatives of either international governmental organizations or non-governmental movements in the field, the chapter shows how a set of principles can be extracted from the reforms in the EU and EU-US regime and how they can be used to create an International Regime for protection of personal data in cyberspace.

Keywords: Personal data protection; Cyberspace; E-Market; Human Rights; EU; USA

La Protección de Datos Personales en el Ciberespacio: el régimen del Mercado Electrónico de Unión Europea – Estados Unidos

Resumen

El objeto de estudio de esta investigación es el derecho a la protección de los datos personales en el marco del régimen jurídico aplicable al mercado electrónico UE-Estados Unidos. Sus características, así como las de los principales actores que intervienen en este mercado, permiten considerar este régimen jurídico como una base adecuada para el posible desarrollo de un tratado internacional de vocación universal sobre protección de datos personales en el ciberespacio.

Los actores y las relaciones incluidas en la investigación son los responsables de las obligaciones jurídicas en materia de protección de datos personales, tanto entidades públicas como privadas. No obstante, también se tienen en cuenta las 'relaciones informales de poder' entre Estado y organizaciones privadas, dada la existencia de acuerdos informales o coordinación entre ambos para el intercambio y procesamiento de datos. El marco temporal de la investigación es 2001-2016 (después de los atentados del 9/11 en Estados Unidos y hasta la más reciente reforma del régimen UE-EEUU culminada en 2016).

El punto de partida de la investigación es el Derecho Internacional de los Derechos Humanos, que contiene el marco general para el apoyo y regulación de la protección de datos personales en el ciberespacio. Sin embargo, los caracteres distintivos del ciberespacio exigen una regulación y mecanismos específicos bien diseñados, a nivel universal, para garantizar internacionalmente tales derechos fundamentales relativos a la protección de datos personales. Consecuentemente, la hipótesis de investigación se formula del siguiente modo: en primer lugar, la protección eficaz de los datos personales en el ciberespacio necesita el establecimiento de un sistema jurídico internacional de alcance universal basado en tratados; en segundo lugar, el régimen de la UE sobre protección de datos personales en el ciberespacio y los actuales acuerdos UE-Estados Unidos sobre esta cuestión pueden utilizarse como modelo para la elaboración de dicho Tratado Internacional.

La estructura de la tesis se divide en seis capítulos, siendo el Capítulo 1 el \diseño de la investigación y el Capítulo 6 las conclusiones y recomendaciones que se desprenden de la investigación. Así, el Capítulo 2 analiza los Instrumentos Jurídicos Universales, las normas de la UE y los acuerdos UE-EEUU vigentes antes del 5 de junio de 2013 (fecha crítica debido a las revelaciones sobre Vigilancia Electrónica en Masa presentadas mundialmente ese día). Dentro de ese marco jurídico, el Capítulo 3 realiza un análisis jurisprudencial y analiza una selección de casos sobre protección de datos personales suscitados ante los tribunales internos de Estados Unidos y ante el Tribunal de Justicia de la Unión Europea, con el objetivo de identificar la interpretación precisa del derecho a la protección de datos personales en el ciberespacio que, posteriormente, ha debido tener en cuenta la reforma normativa en Estados Unidos y en la UE sobre esta materia. El Capítulo 4 analiza y revisa los instrumentos jurídicos promulgados en virtud de la reforma del régimen de protección de datos personales de la UE y los nuevos acuerdos bilaterales entre la UE y los Estados Unidos actualmente en vigor. Por último, el Capítulo 5 evalúa la posibilidad de elaborar un Tratado Internacional de alcance universal que garantice el derecho a la protección de datos personales que 'circulan' en el ciberespacio. Teniendo en cuenta las iniciativas formuladas por organizaciones gubernamentales internacionales y por los movimientos no gubernamentales especializados, el capítulo muestra cómo se pueden extraer un conjunto de principios de las reformas de la UE y del régimen aplicable en el espacio UE-EEUU y cómo esos principios pueden utilizarse para la creación de un régimen internacional de protección de datos personales en el ciberespacio.

Palabras clave: Protección de datos personales; Ciberespacio; Mercado electrónico; Derechos Humanos; Unión Europea; Estados Unidos

La Protecció de Dades Personals en el Ciberespai: el règim del Mercat Electrònic UE-EE.UU

Resum

L'objecte d'estudi d'aquesta recerca és el dret a la protecció de les dades personals en el marc del règim jurídic aplicable al mercat electrònic UE-Estats Units. Les seves característiques, així com les dels principals actors que intervenen en aquest mercat, permeten considerar aquest règim jurídic com una base adequada per al possible desenvolupament d'un tractat internacional de vocació universal sobre protecció de dades personals en el ciberespai.

Els actors i les relacions incloses en la recerca són els responsables de les obligacions jurídiques en matèria de protecció de dades personals, tant entitats públiques com a privades. Malgrat això, també es tenen en compte les 'relacions informals de poder' entre Estat i organitzacions privades, donada l'existència d'acords informals o coordinació entre tots dos per a l'intercanvi i processament de dades. El marc temporal de la recerca és 2001-2016 (després dels atemptats del 9/11 a Estats Units i fins a la més recent reforma del règim UE-EUA culminada en 2016).

El punt de partida d'aquesta recerca és el Dret Internacional dels Drets Humans, que conté el marc general per al suport i regulació de la protecció de dades personals en el ciberespai. Ara bé, els caràcters distintius del ciberespai exigeixen una regulació i mecanismes específics ben dissenyats, a nivell universal, per garantir internacionalment els esmentats drets fonamentals relatius a la protecció de dades personals. Conseqüentment, la hipòtesi de recerca es formula de la següent manera: en primer lloc, la protecció eficaç de les dades personals en el ciberespai necessita l'establiment d'un sistema jurídic internacional d'abast universal basat en tractats; en segon lloc, el règim de la UE sobre protecció de dades personals en el ciberespai i els actuals acords UE-Estats Units sobre aquesta qüestió poden utilitzar-se com a model per a l'elaboració d'aquest Tractat Internacional.

L'estructura de la tesi es divideix en sis capítols, essent el Capítol 1 el disseny de la recerca i el Capítol 6 les conclusions i recomanacions que es desprenen de la recerca.

Així, el Capítol 2 analitza els Instruments Jurídics Universals, les normes de la UE i els acords UE-EUA vigents abans 5 de juny de 2013 (data crítica a causa de les revelacions sobre Vigilància Electrònica en massa, presentades mundialment aquest dia). Dins d'aquest marc jurídic, el Capítol 3 realitza una anàlisi jurisprudencial i analitza una selecció de casos sobre protecció de dades personals suscitades davant els tribunals interns d'Estats Units i davant el Tribunal de Justícia de la Unió Europea, amb l'objectiu d'identificar la interpretació precisa del dret a la protecció de dades personals en el ciberespai que, posteriorment, ha hagut de tenir en compte la reforma normativa a Estats Units i en la UE sobre aquesta matèria. El Capítol 4 analitza i revisa els instruments jurídics promulgats en virtut de la reforma del règim de protecció de dades personals de la UE i els nous acords bilaterals entre la UE i els Estats Units actualment en vigor. Finalment, el Capítol 5 avalua la possibilitat d'elaborar un Tractat Internacional d'abast universal que garanteixi el dret a la protecció de dades personals que 'circulen' pel ciberespai. Tenint en compte les iniciatives formulades per organitzacions governamentals internacionals i pels moviments no governamentals especialitzats, el capítol mostra com es poden extreure un conjunt de principis de les reformes de la UE i del règim aplicable a l'espai UE-EUA i com aquests principis poden utilitzar-se per a la creació d'un règim internacional de protecció de dades personals en el ciberespai.

Paraules clau: Protecció de dades personals; Ciberespai; Mercat electrònic; Drets Humans; Unió Europea; Estats Units

Index of Contents

Part 3 Present

La Protección de Datos Personales en el Ciberespacio: el régimen del Mercado Electrónico UE-EE.UU

Resumen ejecutivo

1. Introducción

En esta sección se describirán todas las cuestiones preliminares, los conocimientos previos, y el marco de referencia de la investigación, sobre la protección de datos personales en el ciberespacio.

1.1. El ciberespacio desde una perspectiva jurídica

El ciberespacio suscita importantes angustias para sus usuarios, especialmente en lo que se refiere a las lagunas de su legislación reguladora. Esta sección inicialmente dilucidará los factores de influencia que tal régimen de regulación debe tener en cuenta, es decir, la posibilidad sobre la protección de los derechos de los sujetos de datos por entidad diversa de la comunidad estatal, empresarial e internacional, explorando cualquier precaución para aplicar la regulación a diferentes relaciones y el Mercado electrónico relativo. Por lo tanto, investigará críticamente cómo las características de la variedad del ciberespacio han afectado cualquier entorno jurídico que se relaciona con él. Más concretamente, demostrará cómo las tesis homólogas de los teóricos, a saber, los excepcionalistas y los noexcepcionalistas, han descrito sus puntos de vista en contra de tales características. Finalmente, utilizando diversas perspectivas incluyendo la perspectiva de los Derechos Políticos, Económicos, Sociales y Culturales, examinará las situaciones complejas sobre cómo el ciberespacio está creando un lugar necesitado de regulación transfronteriza en términos de protección del derecho, obligación del titular y aplicación de la ley.

Desde el final de la Guerra Fría, los términos 'ciberespacio' y 'globalización' han sido prevalentes. El internet desencadenó un nuevo orden de interconexión y descentralización. En cuanto a los impactos del espacio cibernético sobre el derecho, los resultados de la ignorancia tecnológica en la comunidad jurídica pueden ser devastadores, con casos decididos y perdidos sobre la base de argumentos poco fundados de las partes o de un razonamiento

desacertado por los tribunales.[1] Así, el Juez Frank Easterbrook provocativamente declaró que el estudio de la ciber-ley como un campo de estudio independiente no sería diferente de estudiar la "ley del caballo" en el siglo XIX. [2] Su declaración refleja explícitamente que sólo requiere "reglas generales" sin la necesidad de inventar un nuevo régimen jurídico, sin desear nada específicamente llamado "ciber-ley".

No obstante, las discusiones sobre los derechos y la libertad en el ciberespacio se preocupan por las amenazas a los Derechos Fundamentales planteadas por el poder privado mencionado por Paul S. Berman que ubica entre los riesgos del ciberespacio "el papel del poder económico arraigado, la importancia de los regímenes jurídicos incrustados, el papel del Estado, la importancia de las comunidades no estatales en la construcción de normas"[3] implicando las necesidades de sensibilidad en la regulación del ciberespacio.

En contraste con los "non- excepcionalistas", los "excepcionalistas" del ciberespacio argumentaron que el medio mismo creaba problemas radicalmente nuevos que requerían un nuevo trabajo analítico.[4] En consecuencia, las nuevas tecnologías que alteran la cultura son precisamente los tipos de cambios que tienden a dar lugar a cambios en principios jurídicos bien establecidos.[5]

Los impactos del ciberespacio adoptan un enfoque estructural, haciendo hincapié en las fuerzas culturales, económicas, políticas y jurídicas a gran escala que son más fundamentales que el modo en que determinadas reglas jurídicas se aplicarán a determinados tipos de interacciones[6] pero cómo manejaría la comunidad jurídica este espacio a través de la transformación.

Además, hay un gran número de estudios de casos para apoyar los cambios y desafíos que causan obstáculos a las regulaciones del ciberespacio. Ya que la revolución de la tercera

---

[1] Svantesson, Dan J B. "The Times They Are a-Changin'(Every Six Months)--the Challenges of Regulating Developing Technologies." *Forum on public policy: A journal of the Oxford Round Table*, Forum on Public Policy, 2008.

[2] Easterbrook, Frank H. "Cyberspace and the Law of the Horse." *U. Chi. Legal F.*, 1996, pp. 207-216.

[3] Berman, Paul S. "Law and Society Approaches to Cyberspace." *Law and Society Approaches to Cyberspace*, Ashgate Publishing, Aldershot, 2007, p. xix.

[4] Ibid, p. xiv.

[5] Ibid.

[6] Ibid, p. xxiii.

ola ha continuado, el Estado Nación y la Comunidad Internacional se han preocupado si el principio universal del derecho puede aplicarse o no al Ciberespacio adecuadamente. [7]

Hay una mutabilidad en el principio de Persona en la "Sociedad Netizen"[8] porque los individuos en el Ciberespacio pueden cambiar o encubrir sus identidades para "crear múltiples identidades electrónicas que están enlazadas sólo por su progenitor común, que enlazar, invisible en el mundo virtual, es de gran importancia." [9] En este sentido, el Estado tiene el deber de asegurar la trazabilidad de la persona en caso de crimen o terrorismo. Sin embargo, el derecho a la privacidad y el derecho a saber y los datos personales deben ser corroborados también.

Las relaciones en el ciberespacio parecen ser vagas cuando tenemos que aplicar la ley a una línea virtual para las actividades de comunicación, ya sea en la esfera pública o privada. Ha mostrado el paisaje cambiante del derecho y también su consecuencia, que reduce la brecha entre la vida privada y pública. Además, obliga a proporcionar opciones para la construcción de marcos jurídicos con los que proteger y promover los derechos de los miembros de Social Media[10] para manejarlo con seguridad, suprimiendo los daños. En consecuencia, se deben trazar nuevas fronteras para establecer un alcance de certidumbre entre la esfera pública, en la cual la persona puede expresar su intimidad con responsabilidad hacia los demás, y la esfera privada, plenamente fundamentada sobre la base del derecho a la privacidad.

El desplazamiento más predominante es la jurisdicción sobre "lugar" porque las actividades en el ciberespacio son transfronterizas o relevantes para más de un Estado, [11] de modo que se pueden producir muchas situaciones de conflictos de leyes. En el pasado, los principios de jurisdicción legal "bien establecidos" veían la jurisdicción como arraigada casi

---

[7] Lloyd, Ian J. *Information Technology Law.* Oxford University Press, UK, 2011, p. 182.

[8] Cavanagh, Allison. *Sociology in the Age of the Internet.* Tata McGraw-Hill Education, Delhi, 2010, pp. 76 and 120.

[9] Basu, Subhajit and Jones, Richard. "Regulating Cyberstalking." *Journal of Information Law & Technology*, vol. 22, 2007, p. 10.

[10] Barwick, Hamish. "Social Networking Websites May Face Government Regulation." *Computerworld*, 16 Mar. 2012, www.computerworld.com.au/article/418730/social_networking_websites_may_face_ government_regulation/. Accessed 4 Nov. 2013.

[11] Fuchs, Christian. *Internet and Society: Social Theory in the Information Age.* Routledge, London, 2007, p. 119.

exclusivamente en el poder territorial del soberano,[12] pero ahora el principio absoluto llamado "doctrina de efectos" ha sido difícil de aplicar a la interacción en línea porque el material de un sitio web potencialmente crea efectos en cualquier lugar[13] independientemente del territorio del Estado.

Internet podría proporcionar una oportunidad a la gente pero garantizar el derecho al "Medio" es crucial. Además, la oportunidad de competir en una comunicación de alta tecnología es una clave antimonopolio[14] en todas las perspectivas. Aunque la penetración de Internet y la proporción de digitalización se difunden entre diferentes sociedades, dependen de las condiciones socioeconómicas: habilidades informáticas, alfabetización, ingresos y entornos regulatorios,[15] lo que podría afectar su capacidad de asimilación. Sin embargo, es imposible eliminar o bloquear el tráfico porque las técnicas de los controles intermedios son generalmente menos efectivas en las naciones pequeñas[16,] y tienen una matriz más grande de intermediarios para remontarse a las naciones superpotentes.

Con respecto a la posesión de "Tecnología", la comercialización en productos y servicios en mercancías[17] o bienes públicos es el punto del ciberespacio. Debido al derecho a la información, 'Internet Society' debe proporcionar a los individuos los medios para participar en la producción y distribución de la cultura.[18] En realidad, la libertad de expresión se encuentra en una relación incómoda con la ley de derechos de autor, ya que efectivamente censura el discurso en nombre de proporcionar incentivos para crear.[19] Por otra parte, podría

---

[12] Berman, Paul S. "Law and Society Approaches to Cyberspace." *Law and Society Approaches to Cyberspace*, Ashgate Publishing, Aldershot, 2007, p. xiv.

[13] Ibid, p. xv.

[14] Fuchs, Christian. *Internet and Society: Social Theory in the Information Age.* Routledge, London, 2007, p. 120.

[15] Klang, Mathias and Murray, Andrew. "Internet Service Providers and Liability." *Human Rights in the Digital Age.* Psychology Press, 2005, p. 88.

[16] Goldsmith, Jack and Wu, Tim. *Who Controls the Internet?: Illusions of a Borderless World.* Oxford University Press, UK, 2006, pp. 81-82.

[17] Fuchs, Christian. *Internet and Society: Social Theory in the Information Age.* Routledge, London, 2007, p. 139.

[18] Balkin, Jack M. "Digital Speech and Democratic Culture: A Theory of Freedom of Expression for the Information Society." *NYUL rev.*, vol. 79, 2004, pp. 1–58.

[19] Berman, Paul S. "Law and Society Approaches to Cyberspace." *Law and Society Approaches to Cyberspace*, Ashgate Publishing, Aldershot, 2007, p. xxi.

dar un poder al propietario de los derechos de autor para perseguir sus bienes mediante la detección de dispositivos.

El poder de las Corporaciones informáticas y la Autoridad del Estado provienen de la posesión de la "Tecnología" que luego comercializan en productos y servicios[20] pero la cuestión de si son bienes privados o bienes públicos es punto crucial de la regulación del ciberespacio. Debido al derecho a la protección de datos personales, la *Internet Society* debe proporcionar a los individuos los medios para participar en la producción y distribución de la cultura.[21] De hecho, la libertad de expresión se encuentra en una relación difícil con el derecho de propiedad intelectual, ya que este último censura la expresión en base al interés de proveer incentivos a la creación.[22]Aún más, podría dar un poder al propietario de la tecnología para maximizar el beneficio de sus bienes mediante el uso de dispositivos de rastreo.

Internet constituye una tecnología vital de la comunicación que está transformando en profundidad muchos aspectos de la vida humana.[23] En consecuencia, hay algunas características de los retos en 4 perspectivas principales: los derechos políticos, los derechos económicos, los derechos sociales y los derechos culturales, que el Estado y la comunidad internacional deben incorporar como consideraciones previas.

El principal argumento a este respecto es el enfrentamiento entre Autoridad y Poder con Liberación y Resistencia.[24] La Autopista de Información afecta al mundo mediante el acceso a la red 24 horas, generando comunicación bidireccional con participación múltiple individual sin obstáculos geográficos.[25] Se desencadena así la "democracia digital" mediante la información y la plena participación, sin embargo, los obstáculos contra la adhesión a

---

[20] Fuchs, Christian. *Internet and Society: Social Theory in the Information Age.* Routledge, London, 2007, p. 139.

[21] Balkin, Jack M. "Digital Speech and Democratic Culture: A Theory of Freedom of Expression for the Information Society." *NYUL rev.*, vol. 79, 2004, pp. 1–58.

[22] Berman, Paul S. "Law and Society Approaches to Cyberspace." *Law and Society Approaches to Cyberspace*, Ashgate Publishing, Aldershot, 2007, p. xxi.

[23] Cavanagh, Allison. *Sociology in the Age of the Internet.* Tata McGraw-Hill Education, Delhi, 2010, p. 2.

[24] Terranova, Tiziana. *Network Culture: Politics for the Information Age.* Pluto Press, London, 2004, p. 135.

[25] Bryan, Cathy and Tatam, James. "Political Participation and the Internet." *Liberating Cyberspace: Civil Liberties, Human Rights & the Internet.* Pluto Press, London, 1999, p. 162.

Internet podrían degenerar en "la aristocracia de la información"[26] de modo que la minoría de los proveedores privados ricos y el Estado podrían monopolizar la Arena Política.

En sentido económico, podría ser descrito por la confrontación de Monopolio y Dividendo con Asignación y adhesión.[27] La neutralidad de la red sería el punto sobre la competencia leal entre los proveedores de servicios,[28] sin embargo, en algunos casos de IT Corporaciones que tienen poder sobre el mercado podría recoger una gran cantidad de datos[29] e implicar la comercialización directa y masiva de vigilancia electrónica.

El reto que internet crea para la sociedad se resume en el planteamiento de Clase fragmentada y Exclusión con Redes e Inclusión.[30] La vida cibernética genera al Estado situaciones difíciles para el control de la violencia y los grupos criminales, lo que obliga al Estado a implementar normas de control y sanción al tiempo que debe permitir que las sociedades civiles disfruten de la necesaria libertad. También abre la puerta a la autorregulación por parte de empresarios y entes similares.[31]

El ciberespacio crea "comunidades virtuales" que podrían generar algún debate en varios casos entre Conservador y Dominación versus Diversidad y Pluralismo.[32] Internet podría ser utilizado por comunidades potencialmente marginadas dejando beneficios en la esfera cada vez más lucrativa de mundos simulados con multijugadores. Por otra parte, podría permitir a los extremistas no liberales encontrar una comunidad transnacional.[33]

---

[26] Carter, Dave. "Economic Regeneration and the Information Economy." *The governance of cyberspace: Politics, technology and global restructuring*, vol. 136, 1997, p. 137.

[27] Cavanagh, Allison. *Sociology in the Age of the Internet.* Tata McGraw-Hill Education, Delhi, 2010, p. 64.

[28] Mahabadi, Ladan. "Price of Monopoly and Democracy, Internet and Democracy Blog." *Price of Monopoly and Democracy*, 19 Aug. 2008, https://blogs.law.harvard.edu/idblog/2008/08/19/price-of-monopoly-and-democracy/. Accessed on 20 Nov. 2012.

[29] Solum, Lawrence B. "Models of Internet governance." *Internet Governance: Infrastructure and Institutions,* Lee A. Bygrave and Bing, Jon. (eds), Oxford University Press, UK, 2009, pp. 88-89.

[30] Cavanagh, Allison. *Sociology in the Age of the Internet.* Tata McGraw-Hill Education, Delhi, 2010, pp. 112-115.

[31] Berman, Paul S. "Law and Society Approaches to Cyberspace." *Law and Society Approaches to Cyberspace*, Ashgate Publishing, Aldershot, 2007, p. xxiii.

[32] Fuchs, Christian. *Internet and Society: Social Theory in the Information Age.* Routledge, London, 2007, pp. 333-334.

[33] Berman, Paul S. "Law and Society Approaches to Cyberspace." *Law and Society Approaches to Cyberspace*, Ashgate Publishing, Aldershot, 2007, p. xxii.

Esta tesis dibuja un marco de vigilancia de comunicaciones por parte de los Estados para el ejercicio de los Derechos Humanos a la intimidad y a la protección de datos personales. Al considerar el impacto de los avances tecnológicos significativos en las comunicaciones, el Estado puede necesitar emplear un sistema jurídico y un mecanismo para apoyar la integridad de la protección de datos personales en diferentes niveles; nacional, regional e internacional.

Estos impactos y sus retos derivados, a su vez, llevaron a la cuestión adicional del "régimen de regulación adecuado".[34] Sin embargo, no existe una solución única para la protección de datos. Las medidas adecuadas que sean apropiadas para su organización dependerán de sus circunstancias, por lo que la investigación posterior adopta un enfoque basado en los derechos para decidir qué nivel de régimen de protección se puede sugerir.

1.2. Impacto del procesamiento de datos sobre la protección de datos personales

Las implicaciones económicas y políticas del procesamiento de datos afectan a todos los derechos relacionados con la protección de datos personales. Particularmente, cuatro preguntas son relevantes: ¿Necesita la economía del conocimiento datos personales para procesar y el gobierno ahorrará muchos costes si permite que dicha recolección suceda y pueda explotarse? ¿Es aceptable la actitud de 'Zero Privacy'? ¿Es el "derecho fundamental" un obstáculo para el proyecto de sociedad de la información de Estados Unidos y la UE? Y ¿Necesita la protección de datos personales de una institución específica?

En primer lugar, no sólo existen las necesidades de los negocios, que prefieren un amplio margen para sus actividades comerciales a fin de crear un nuevo producto en forma de servicios de procesamiento de datos, sino que también existen necesidades de los propios gobiernos de los Estados (eficiencias y ahorro de costes). Sin embargo, existen argumentos sobre las condiciones económicas[35] y sociales "inevitables", que se contraponen a una política estricta de protección de datos.

---

[34] Goldsmith, Jack and Wu, Tim. *Who Controls the Internet?: Illusions of a Borderless World.* Oxford University Press, UK, 2006, pp. 179-184.

[35] Ruddick, Graham. "Online Shopping to Grow by £320bn in Three Years." *The Telegraph,* 7 Jun. 2015, www.telegraph.co.uk/finance/newsbysector/retailandconsumer/11657830/Online-shopping-to-grow-by-320bn-in-three-years.html. Accessed 2 May 2016.

El ciberespacio es apto para probar la teoría de la "gubernamentalidad" de Michel Foucault que revela la tecnología de poder del Estado moderno que penetra al individuo a través del espacio y la actividad pública.[36] Desde el estado ansioso por cambiar la línea al espacio privado anterior combinado con la ampliación de los espacios de comunicación pública, la Sociedad Legal tiene el deber de responder a los problemas sobre si los medios sociales son una esfera pública o un verdadero espacio privado. En este sentido, el sistema de procesamiento de datos de las autoridades estatales y las empresas privadas se utilizará como un poderoso dispositivo de vigilancia electrónica masiva.

El mismo problema se da para equilibrar el poder de los derechos estatales e individuales bajo algunas condiciones; la seguridad del Estado, la seguridad pública, los intereses monetarios del Estado o la supresión de delitos y la protección de los derechos de los demás. Estas excepciones son vagas y fáciles de usar como excusa para interferir en la esfera privada del individuo. Desde que la recopilación de datos y el procesamiento de la posmodernidad pasan a manos privadas de Corporación de IT,[37] poniendo a las autoridades estatales al borde del dilema. Por un lado Estado puede cooperar con los sectores privados para ganar más poder sobre la gente, por otro lado se mantienen en su posición para regular los malos comportamientos de las corporaciones, con la dificultad de que el Estado a menudo carece de poder técnico más avanzado para acceder a los datos. Los sueños de las personas de tener un Estado decente que proteja a las personas mediante la regulación de las empresas privadas pueden parecer ingenuo.

En lo que respecta a la armonización del mercado electrónico de la UE y los Estados Unidos, la intención de crear y ampliar el Gobierno Electrónico proviene de la cuestión del anonimato. En ese sentido, a pesar de que el anonimato es un derecho individual, supone una tremenda dificultad para gestionar a la población en el ciberespacio.[38] Por lo tanto, las amenazas a la protección de datos personales se originan también desde la vigilancia que se ha construido sobre la base del orden social.

---

[36] Loader, Brian. *The Governance of Cyberspace: Politics, Technology and Global Restructuring.* Psychology Press, Brighton, 1997, pp. 12-14.

[37] Koops, Bert-Jaap and Sluijs, Jasper P. "Network Neutrality and Privacy According to Art. 8 Echr." *European Journal of Law and Technology,* vol. 2, no. 3, 2012, p. 7.

[38] Ogura, Toshimaru. "Electronic Government and Surveillance-Oriented Society." *Theorizing surveillance: The Panopticon and Beyond*, Willan Publishing, London, 2006, p. 291.

Los instrumentos jurídicos sobre protección de datos personales se crean a partir de 1980, época en que Interrnet aún no se había expandido demasiado, así que cabe preguntase ¿cómo se aplican esos instrumentos a los problemas posteriores al milenio que suceden en casos de Corporationes de IT transnacionales; Google, Facebook, Yahoo, Microsoft, Apple, etc.? En consecuencia, las Autoridadades Internacionales, Regionales y Domésticas para la Protección de Datos deben interpretar y aplicar el derecho a casos específicos sobre la base del dinamismo, pero la independencia de esas instituciones debe garantizarse de modo transparente.

En cuanto a la evaluación de las Autoridades de Protección de Datos (DPA), esta investigación mostrará las decisiones tomadas por las DPA o los Tribunales en muchos casos en que hubo acusaciones de cooperación entre las Agencias de Seguridad Nacional y los Proveedores de Tecnología de la Información; Corporaciones de IT. La interacción entre ellos podría implicar alguna evidencia sobre la eficacia y transparencia de las DPA.

La investigación presentará los estudios de casos relevantes para escudriñar el éxito de la UE y los EE.UU. en la política de protección de datos. En consecuencia, dichos casos serán punto de referencia necesario para cualquier desarrollo normativo posterior adoptado o posible.

2. Diseño de la investigación

Esta sección ilustra el diseño de la investigación diferenciando 3 secciones. En primer lugar, se describirá el objeto de estudio y la Hipótesis de Investigación. En segundo lugar, se explican los principales métodos y metodologías que se tienen en cuenta para la investigación y cómo se ha accedido a las fuentes y materiales. Por último, se describirá la estructura en la que se ha organizado la investigación.

2.1. Objeto de estudio e hipótesis de investigación

Esta sección plantea el objeto de la investigación, alcance de la tesis y por último la hipótesis de investigación que contiene las preguntas de investigación para el estudio. Estos componentes ilustrarán el panorama general de toda la investigación.

El objeto de la investigación es el derecho a la protección de datos personales en el ciberespacio y sus limitaciones en el marco de la regulación del mercado electrónico UE-EE.UU. Por lo tanto, las limitaciones del régimen jurídico de la UE y los Estados Unidos para cumplir con el derecho a la protección de datos personales son cuestiones que pueden suponer un problema para los titulares de tales derechos. Por otra parte, la naturaleza del Mercado electrónico, que está dominado por las Corporaciónes de IT de EE.UU. que transfieren y procesan datos personales de los ciudadanos de la UE a través del Atlántico, genera más situaciones complicadas para iniciar un régimen común que proteja los datos personales entre EU y EE.UU. El nuevo régimen propuesto debe abordar dos grandes retos: 1) Excepciones sobre la base del estado de emergencia; Seguridad Nacional, Seguridad Pública, Moralidad, etc., al ejercicio del derecho a los datos personales, especialmente en el caso de ciudadanos no estadounidenses,

2) Las entidades estadounidenses, sometidas al sistema jurídico estadounidense y no al de la UE, deben garantizar la aplicación del derecho a la protección de datos personales en el mercado único UE-EE.UU.

Esta tesis se concentrará en la Protección de Datos Personales - no Privacidad –desde la perspectiva de los Derechos Humanos. Se centrará así mismo en los beneficios de seguridad internacional y los Derechos Humanos de los usuarios de Internet en todo el mundo.

Los actores y las relaciones incluidas en la investigación son los responsables de las obligaciones jurídicas en materia de protección de datos personales, tanto entidades públicas como privadas. No obstante, también se tienen en cuenta las 'relaciones informales de poder' entre Estado y organizaciones privadas, dada la existencia de acuerdos informales o coordinación entre ambos para el intercambio y procesamiento de datos. El marco temporal de la investigación es 2001-2016 (después de los atentados del 9/11 en Estados Unidos y hasta la más reciente reforma del régimen UE-EEUU culminada en 2016). Su 'ambito espacial' es el ciberespacio, especialmente el mercado electrónico, la transferencia de datos por Internet internacionalmente. No sólo estudia los instrumentos jurídicos propios de la UE, sino también de las relaciones transatlánticas, UE-EE.UU.

La Investigación selecciona 2 Áreas de estudio; UE y UE-EE.UU., y se basará en las evidencias de la práctica en cada área y otros análisis; Revisiones documentales y opiniones de expertos. Además, la información cualitativa; sentencias, resoluciones y opiniones de

organizaciones o de las autoridades estatales serán tomadas como pruebas o interpretaciones básicas.

Hipótesis de la investigación

El punto de partida de la investigación es el Derecho Internacional de los Derechos Humanos, que contiene el marco general para el apoyo y regulación de la protección de datos personales en el ciberespacio. Sin embargo, los caracteres distintivos del ciberespacio exigen una regulación y mecanismos específicos bien diseñados, a nivel universal, para garantizar internacionalmente tales derechos fundamentales relativos a la protección de datos personales. Consecuentemente, la hipótesis de investigación se formula del siguiente modo: en primer lugar, la protección eficaz de los datos personales en el ciberespacio necesita el establecimiento de un sistema jurídico internacional de alcance universal basado en tratados; en segundo lugar, el régimen de la UE sobre protección de datos personales en el ciberespacio y los actuales acuerdos UE-Estados Unidos sobre esta cuestión pueden utilizarse como modelo para la elaboración de dicho Tratado Internacional.

Preguntas de investigación

La hipótesis anterior puede transformarse en las siguientes preguntas para la realización de la investigacion:

1) ¿Cómo han regulado la protección de datos personales en el mercado electrónico las normas de la Unión Europea, los Estados Unidos de América y el acuerdo UE-EE.UU?

2) ¿Cómo se han resuelto los problemas cuando existen conflictos entre los Derechos Humanos protegidos de los individuos y la utilización por los Estados de datos procesados por las Corporaciones de IT?

3) ¿Cómo se han expresado las decisiones judiciales relativas a Corporaciones IT? ¿Y hasta qué punto establecen un precedente para el derecho a la protección de datos personales?

4) ¿Cuáles son los cambios sobre protección de datos que aportan las reformas de la UE y los Estados Unidos en la regulación de mercado electrónico?

5) ¿Qué debería ser formulado como Régimen Universal para regular el procesamiento de datos de las Corporaciones Transnacionales IT y las Autoridades del Estado de modo que posibilite el cumplimiento del derecho a la protección de datos personales a nivel nacional, regional e internacional?

2.2. Métodos y metodología de investigación

La investigación emplea la doctrina jurídica en el estudio sobre la historia de las normas sobre protección de datos y de su desarrollo al hilo del progreso de la tecnología de la información.

Sin embargo, parte de la investigación emplea un estudio jurídico no doctrinal para ilustrar la complejidad de la práctica de las Corporaciónes de IT y las agencias estatales y demostrar cómo la violación de derechos individuales se produce también por el desconocimiento de las autoridades del Estado.

En términos de investigación empírica, esta investigación emplea un estilo cuantitativo y cualitativo para reunir los datos en diferentes estudios de casos en circunstancias difíciles.

En cuanto al aspecto cuantitativo, los números estadísticos, informes y casos serán categorizados y representarán la operación y cooperación entre Corporación de IT y el Estado.

En el aspecto cualitativo, se tienen en cuenta la revisión de la literatura, entrevistas y comunicados de prensa de las partes interesadas, decisiones judiciales, informes oficiales y opiniones de las organizaciones de expertos a fin de identificar los problemas y perspectivas de la protección de datos personales.

Asímismo, el análisis de Estudio Jurídico Crítico sobre la economía política entre Estados y corporaciones se utilizará como marco principal para describir la relación entre ellos que debería estar sujeta por ciertos regímenes jurídicos para la protección de datos.

Finalmente, la investigación prescriptiva se empleará como marco para analizar las reformas del régimen de protección de datos de la UE y los Estados Unidos. En consecuencia, los estudios comparativos permitirán sintetizar los requisitos previos deducibles del régimen de la UE - EE.UU. que pueden servir de posible punto de partida para la progresiva realización de un Régimen Universal del derecho a la protección de datos personales de escala mundial.

El plan de investigación para completar el proyecto de investigación consta de

1) Revisión de la literatura jurídica.

2) Recopilación de datos empíricos para probar el procesamiento de datos por parte de las IT Corporations y su cooperación con el Estado en la recolección, procesamiento y compartición de datos.

3) Análisis de Economía Política sobre la legitimidad de la relación entre las IT Corporations y los Estados a partir de la evidencia empírica.

4) Análisis Socio-Legal sobre antiguas normas de protección de datos personales y su ejecución.

5) Investigación prescriptiva sobre jurisprudencia de los estudios de casos de la Corte Suprema y Tribunales de los Estados Unidos y Tribunal de Justicia de la Unión Europea.

6) Investigación Normativa sobre nuevas normas de protección de datos personales.

7) Síntesis de las perspectivas de promover un régimen de protección de datos personales a partir de la investigación.

Para cumplir con el plan de investigación necesité pasar tiempo en muchos lugares y visitar varios espacios para acceder a fuentes de material;

1) Bibliotecas; Facultad de Derecho de la Universidad de Barcelona, Facultad de Economía y Empresa de la Universidad de Barcelona, Facultad de Derecho de laUniversidad de Chiangmai. Estas bibliotecas no sólo permiten el acceso a los libros de papel y revistas académicas, sino también proporcionar el catálogo de la biblioteca digital que se describe a continuación.

2) Portales de Internet, Westlaw, Lexis-Nexis, Social Science Research Network (SSRN) y Legal Scholarship Network (LSN)

3) Sitio Oficial de las Organizaciones de Competencia, Naciones Unidas, Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos, Foro de Gobernanza de Internet (IGF), Unión Europea, Tribunal de Justicia de la Unión Europea, Comisión Europea Misión de Justicia, Comisión de Libertades Civiles, Justicia y Asuntos De Interior Comisión; Puerto Seguro, Escudo de Privacidad, Biblioteca del Congreso, Tribunales Gobierno de EE.UU.

4) Seminario anual internacional del Foro de Gobernanza de Internet de las Naciones Unidas.

2.3. Estructura de la investigación

La investigación se divide en 6 capítulos. El primer capítulo recoge el diseño de la investigación y el último engloba las conclusiones y las recomendaciones que pueden formularse a partir de la misma. Indicaremos a continuación los contenidos fundamentales de los capítulos 2, 3, 4 y 5 de la tesis en los que se recoge el desarrollo y resultados de nuestra investigación.

1) El antiguo régimen de Protección de Datos Personales

El capítulo 2 analiza los instrumentos universales, las normas de la UE y los acuerdos entre UE y EE.UU. antes del 5 de junio de 2013, partiendo de los antecedentes históricos de la protección de datos personales, la cristalización de la protección de datos personales a nivel institucional con diferentes estatutos jurídicos, junto a sus disposiciones sustantivas. Juntos forman parte del entorno regulador contemporáneo de protección de datos internacionales. En este capítulo, la investigación considera el STATUS QUO del régimen de protección de datos personales vigente antes del proceso de reforma en la UE y EE.UU. A pesar de la proliferación de las fuentes internacionales de las normas de protección de datos, su aplicación sigue siendo a nivel estatal. En efecto, dependiendo de las restricciones nacionales, corresponde a los gobiernos nacionales decidir si se debe introducir la legislación sobre protección de datos, qué modelo internacional aplicar, cómo aplicarlo y cómo equilibrarlo con otros derechos humanos u otras consideraciones; el régimen e importancia de la seguridad del estado, la lucha contra el crimen y el terrorismo. Consecuentemente, el régimen estadounidense de protección de datos personales se convierte en relevante, como se analiza en el Capítulo 2.

2) Principales Casos sobre protección de datos personales en la práctica y ante los Tribunales

Como las Corporaciones IT son los principales actores en el dilema entre Procesamiento de Datos y Protección de Datos, la relación entre los proveedores de servicios (SP) y las autoridades del Estado son cruciales para el análisis. Las amenazas a la protección de datos personales planteadas por agencias estatales o actores no estatales, en este caso Corporación de IT, proceden de la acumulación y posesión de grandes almacenes de datos trazables. El capítulo 3 reflejará los problemas existentes mediante la selección de las políticas y prácticas de la Agencia de Inteligencia de los Estados Unidos que penetran en los

sistemas de contenidos de las Corporations IT Transnacionales. Con el fin de buscar una interpretación precisa de la protección de datos personales, se estudian las decisiones judiciales en los tribunales nacionales de EE.UU. y el Tribunal de Justicia de la Unión Europea en aplicación de este conjunto normativo, antes de que se produjera la reforma. En ellos es posible encontrar un claro precedente sobre cómo se aplicó el derecho a la protección de datos personales en diversos escenarios. Dichos precedentes jurisprudenciales podrán servir de puntos de referencia para la reforma y creación del nuevo régimen de protección de datos personales en diferentes niveles; Nacional, Bilateral, Regional e Internacional.

3) Reformas de la UE y la UE-EE.UU. sobre la protección de datos personales en el ciberespacio

En el capítulo 4, se analiza el nuevo régimen de protección de datos personales de la UE y los acuerdos bilaterales UE-EE.UU. , fruto de las reformas operadas desde el 6 de junio de 2013. En primer lugar, el régimen nacional estadounidense de transición sobre protección de datos personales en el ciberespacio. El Gobierno de los Estados Unidos había lanzado una serie de iniciativas legislativas para reformar su actividad de vigilancia y proporcionar a los ciudadanos no estadounidenses un reforzamiento de sus derechos sobre protección de datos personales ante los Tribunales de los Estados Unidos. A continuación, la amplia revisión de los nuevos regímenes de la UE y EE.U.U., la UE aprueba el Reglamento General de Protección de Datos (GDPR) y la Directiva sobre asuntos judiciales y penales. Luego, la UE instó al gobierno de los Estados Unidos a firmar un nuevo acuerdo bilateral para aplicar esas normas; el *Privacy Shield* UE-EE.UU. Para la protección general de datos y el Acuerdo Conjunto UE-EE.UU. sobre asuntos judiciales y penales. Sin embargo, no ha habido un Tratado Internacional para la Protección de Datos de Carácter Personal. Los estudios sobre los regímenes de la UE y los Estados Unidos darán perspectivas sobre la eventualidad de iniciar la elaboración de instrumentos universales y regionales de protección de datos personales y otras medidas de derecho interno.

4) El enfoque universal para la creación de un nuevo Régimen de Protección de Datos Personales

Finalmente, el quinto capítulo evalúa la posibilidad de elaborar un Tratado Internacional de alcance universal que garantice el derecho a la protección de datos personales que 'circulan' en el ciberespacio. Teniendo en cuenta las iniciativas formuladas por organizaciones gubernamentales internacionales y por los movimientos no

gubernamentales especializados, el capítulo muestra cómo se pueden extraer un conjunto de principios de las reformas de la UE y del régimen aplicable en el espacio UE-EEUU y cómo esos principios pueden utilizarse para la creación de un régimen internacional de protección de datos personales en el ciberespacio.

3. Conclusiones y recomendaciones

Los usos de los datos personales de Internet ya no se no se limitan a interacciones en la esfera local, ni siquiera en espacios físicos bien delimitados.. Además, el procesamiento transfronterizo de datos personales se ha personalizado. Los organismos controladores de datos nacionales ya no son necesarios para que los sujetos titulares de los datos puedan transmitirlos a través de fronteras a otros controladores de datos de modo que se produzcan intercambios transfronterizos.[39] Hoy en día, las aplicaciones de redes sociales permiten a los usuarios subir sus datos personales a la "cuenta" o "página web", yendo y viniendo de un destino no identificado. En este contexto, por lo que se refiere a la protección de datos, debe decidirse cómo, en todo caso, los datos pueden ser protegidos en la misma medida en el ciberespacio que en el mundo "real".[40] Es habitual que los intentos de crear una sociedad "conectada" y segura resulten aún más difíciles que en un entorno sin conexión porque la cantidad de datos procesados es mucho mayor que en el pasado. En este contexto de problemas y retos generales, nuestra investigación permite extraer algunas conclusiones y formular recomendaciones que pueden ayudar a su solución y gestión.

3.1. Conclusiones

3.1.1. Protección de datos personales en el marco del régimen jurídico de la UE y del mercado electrónico de UE-EE.UU. antes de 2013: deficiencias y problemas principales

Si bien el objetivo de esta investigación es armonizar la provisión e implementación de la Protección de Datos Personales para la creación del Régimen Internacional, el punto de

[39] De Hert, Paul and Papakonstantinou, Vagelis. "Three Scenarios for International Governance of Data Privacy: Towards an International Data Privacy Organization, Preferably a UN Agency." *ISJLP*, vol. 9, 2013, p. 271.

[40] Metcalf, Katrin N. "Legal Aspects of Privacy Law and Data Protection." *The Right to Privacy as a Human Right and Everyday Technologies*, Institute of Human Rights NGO, 2014, p. 83.

partida muestra la superposición e insuficiencia de los instrumentos antiguos. Específicamente, el viejo conjunto de normas sobre protección de datos personales, promulgado antes del proceso de reforma de la UE y los Estados Unidos, se había basado en gran medida en la aplicación nacional del mismo.[41]

3.1.1.1. Predominio de las entidades estadounidenses y sus efectos sobre los Global Netizen

Destacadamente, los recelos y críticas sucitados por el sistema estadounidense en relación a la protección de datos personales se pusieron de manifiesto a raíz de la operación de inteligencia de EEUU. en el ámbito de la Seguridad Nacional.[42] La intención del gobierno Norteamericano de llevar a cabo una vigilancia electrónica masiva en las actividades relacionadas con el terrorismo, especialmente sobre extranjeros que están fuera de la protección constitucional norteamericana, puede conducir a los usuarios de Internet en todo el mundo a situaciones más que complicadas, desde el punto de vista de la protección de sus derechos sobre sus datos personales.[43] El hecho de que la mayoría de las principales corporaciones de IT se hallan radicadas en los EE.UU. o transferieren datos personales a servidores ubicados en territorio de EE.UU. implica que la principal amenaza para los usuarios de Internet no ciudadanos de los EE.UU, sería el acceso a la defensa de sus derechos en este país.

Las Corporación IT de EE.UU. está sujetas a las leyes internas de los Estados Unidos mientras que los derechos de los Global Neitizen entran al ámbito de la jurisdicción de los Estados Unidos cuando dichos datos se transfieren a territorio o entidades estadounidenses y pudiendo entonces verse comprometidos por el ejercicio de poderes de las autoridades estadounidenses.

El Controlador de Datos, Corporación IT de EE.UU., tiene la obligación de asegurar su sistema de datos y notificar a los sujetos de los datos ya la Autoridad de Protección de Datos de Estados Unidos (DPA), cualquier violación de los mismos que llegue

---

[41] De Hert, Paul and Papakonstantinou, Vagelis. "Three Scenarios for International Governance of Data Privacy: Towards an International Data Privacy Organization, Preferably a UN Agency." *ISJLP*, vol. 9, 2013, p. 275.

[42] Galetta, Antonella and De Hert, Paul. *A European perspective on data protection and access rights.* Vrije Universiteit, Brussels, 2013, p. 4.

[43] Weiss, Martin A and Archick, Kristin. "US-EU Data Privacy: From Safe Harbor to Privacy Shield." *Congressional Research Service*, 2016, p. 8.

a producirse. US DPA, la Comisión Federal de Comercio bajo el Ministerio de Comercio, tiene el deber de proporcionar consejos[44] preparatorios y de apoyo, especialmente cuando hubiese una amplia difusión masiva electrónica de vigilancia de datos por la Agencia de Seguridad Nacional de EE.UU. [45]Antes de las revelaciones del 5 de junio de 2013, tanto la DPA de EE.UU. como la Corporación IT no habían hecho nada. Para cumplir el Criterio de Adecuación de la UE,[46] la transferencia de datos a través del Atlántico había estado bajo la provisión del Acuerdo de Safe Harbor UE-EE.UU., legalizando los flujos de datos transfronterizos.

La eficacia de los regímenes de aplicación de la legislación en diversos países se basa en el alcance de la interpretación judicial y en otros aspectos comparativos de las leyes de protección de datos.[47] Existen procedimientos de solución de controversias en la UE, pero no en el Acuerdo de Safe Harbor.[48] La transferencia masiva de datos de ciudadanos no estadounidenses a empresas y autoridades estadounidenses y la falta de un mecanismo de reparación apropiado para tratar esta eventualidad es un tema de extrema preocupación.[49]

Los reguladores de protección de datos de la UE habían iniciado una investigación sobre las prácticas de retención de datos y privacidad de Google, que se extendió también a otros motores de búsqueda.[50] En 2012, el EPIC apeló ante el Tribunal de Distrito de los Estados Unidos en el Distrito de Columbia en busca de la divulgación de cualquier comunicación entre la Agencia de Seguridad Nacional (NSA) y Google Inc. en

---

[44] Boehm, Franziska. "Confusing Fundamental Rights Protection in Europe: Loopholes in Europe's Fundamental Rights Protection Exemplified on European Data Protection Rules." *University of Luxembourg, Law Working Paper Series, Paper no. 2009-01*, 2009, p. 17.

[45] Dowling Jr, Donald C. "International Data Protection and Privacy Law." *Practising Law Institute treatise International Corporate Practice*, 2009, p. 16.

[46] Reding, Viviane. "The Upcoming Data Protection Reform for the European Union." *International Data Privacy Law*, vol. 1, 2011, pp. 3-5.

[47] Greenleaf, Graham. "Sheherezade and the 101 Data Privacy Laws: Origins, Significance and Global Trajectories." *Journal Of Law, Information & Science*, 2013, p. 26.

[48] Dowling Jr, Donald C. "Preparing to Resolve Us-Based Employers' Disputes under Europe's New Data Privacy Law." *J. Alt. Disp. Resol.*, vol. 2, 2000, p. 31.

[49] Moraes, Claude. "Working Document on the US and EU Surveillance programmes and their impact on EU citizens fundamental rights." *LIBE Committee Inquiry on electronic mass surveillance of EU citizens*, Justice and Home Affairs, 2013, p. 72.

[50] Global Privacy Counsel. *Article 29 Working Party Letter to Mr. Peter Fleischer on Google*. 16 May 2007.

relación con el cifrado y la seguridad cibernética.[51] Muchos casos dieron a conocer la cooperación entre la NSA y la Corporación de TI y sus efectos sobre la Protección de Datos Personales.

Dado que el proyecto PRISM de NSA recopila datos de las corporaciones de TI más poderosas del mundo, como Google,[52] Yahoo, Facebook, etc. la identificación del lugar y la actividad de las personas podía rastrearse ordenadamente desde la Gran Colección de Datos [Big Data Collection][53] que se recoge del Ciberespacio, incluyendo a ciudadanos no estadounidenses fuera del territorio estadounidense.

Los Tribunales de los Estados Unidos han tomado decisiones que sientan precedente sobre Recolección y Compartición de Datos de la Corporación de TI y la Autoridad Estatal ya que ambos sujetos se encuentran bajo la jurisdicción de los Estados Unidos.[54] El 16 de diciembre de 2013, el Tribunal de Distrito de los Estados Unidos dictaminó en Klayman v. Obama que la recopilación a gran escala de registros de detalle de llamadas telefónicas nacionales probablemente violaba la Cuarta Enmienda (derecho a la privacidad y protección de datos personales).[55] Este caso reivindicaba el goce pleno de los derechos constitucionales de un ciudadano de los Estados Unidos, pero la protección de los ciudadanos no estadounidenses permanece en el aire.[56]

Desdel otro lado del Atlántico, el Tribunal de Justicia de la Unión Europea CJUE había adoptado una serie de decisiones relativas a la protección de datos personales por parte de la Corporación de TI y el Estado, especialmente el caso de Entidades de nacionalidad estadounidenses. Puesto que existía el Informe LIBE sobre Vigilancia Electrónica en Masa, el programa MUSCULAR, que recoge más del doble de puntos de datos comparados con

---

[51] United States District Court for the District of Columbia. *Case 11-5233 EPIC vs. NSA*. *Document #1373260*. 05 Nov. 2012.

[52] Lopez-Tarruella, Aurelio. "Introduction: Google Pushing the Boundaries of Law." *Google and the Law*, Springer, 2012, Preamble.

[53] Ingram, Mick."Google Publishes Figures on Government Requests for Data" *World Socialist Web Site*, 26 Apr. 2010, www.wsws.org/en/articles/2010/04/goog-a26.html. Accessed 31 Oct. 2013.

[54] Fahey, Elaine and Curtin, Deirdre. *A Transatlantic Community of Law: Legal Perspectives on the Relationship between the EU and US Legal Orders*. Cambridge University Press, UK, 2014.

[55] United States District Court for the District of Columbia. *Case 957 F. Supp. 2d 1 Klayman v. Obama.* 16 Dec. 2013.

[56] Kerr, Orin S. "The Fourth Amendment and the Global Internet." *GWU Law School Public Law Research Paper No. 2014-30*, 2014.

PRISM. El programa MUSCULAR no requiere órdenes judiciales[57] y opera mediante la coordinación con el Reino Unido; por tanto Reino Unido, como Estado miembro de la UE, había violado los datos personales de los interesados en todo el mundo.

El usuario de Facebook, que afirma que sus datos fueron violados por las Agencias de Estados Unidos, dio lugar al llamado Caso Schrems.[58] El fallo del TJUE determinó que los requisitos de seguridad nacional, de interés público y de aplicación de la ley de los Estados tienen "primacía" sobre los principios de Puerto Seguro y que las empresas estadounidenses están obligadas a ignorar, sin limitación, las normas protectoras establecidas por este régimen cuando entran en conflicto con tales requisitos.[59] Por consiguiente, el TJUE observó que el régimen Safe Harbor "permite la interferencia" de las autoridades estadounidenses "con los derechos fundamentales de las personas cuyos datos personales son o podrían ser transferidos de la UE a los Estados Unidos."[60]

El TJEU llegó a la conclusión de que la normativa de *Safe Harbor* y de los Estados Unidos no contempla la posibilidad de que un particular recurra a la vía judicial a fin de tener acceso a los datos personales que le atañen o para obtener la rectificación o el borrado de dichos datos, lo que compromete la esencia de su derecho fundamental a la intimidad, componente esencial del Estado de Derecho.[61] Por lo tanto, la Decisión de S*afe Harbo*r no contenía una medida correctiva suficiente para el individuo en caso de violación por Corporación de IT o la Autoridad Nacional del Estado.

Consecuentemente, TJEU invalidó el Acuerdo de *Safe Harbor* el 6 de octubre de 2015, colocando a UE y EE.UU. en la necesidad de renegociar un nuevo acuerdo para regular los flujos de datos entre ambos lados del Atlántico.

---

[57] Bowden, Caspar. "Directorate General For Internal Policies." *The US Surveillance Programmes and Their Impact on EU Citizens' Fundamental Rights,* 2013, p. 18.

[58] Weiss, Martin A and Archick, Kristin. "US-EU Data Privacy: From Safe Harbor to Privacy Shield." *Congressional Research Service*, 2016, p. 7.

[59] Gavilán, Elisa U. "Derechos Fundamentales Versus Vigilancia Masiva. Comentario a La Sentencia Del Tribunal De Justicia (Gran Sala) De 6 De Octubre De 2015 En El Asunto C-362/14 Schrems." *Revista de Derecho Comunitario Europeo*, no. 53, 2016, pp. 261-282.

[60] Ramos, Mario H. "Una Vuelta De Tuerca Más a Las Relaciones En Materia De Protección De Datos Entre La Ue Y Los Estados Unidos: La Invalidez De La Decisión Puerto Seguro." *Revista General de Derecho Europeo*, no. 39, 2016, pp. 27-31.

[61] CJEU. *Case C-362/14 Maximillian Schrems v Data Protection Commissioner*. 6 Oct. 2015, para. 95.

En conclusión, las dificultades provenían del fracaso del sistema jurídico estadounidense para proteger los datos personales de los interesados. El sistema estadounidense no satisfacía las necesidades normativas europeas referentes a la protección de datos personales. El programa del gobierno de los Estados Unidos para llevar a cabo la vigilancia electrónica en masa de las actividades relacionadas con el terrorismo, especialmente de los extranjeros no cubiertos por la protección constitucional EEUU, implica difíciles escenarios para los usuarios de Internet a nivel mundial en la defensa de sus derechos.

3.1.1.2. Estándares diferentes y las dificultades de una jurisdicción fragmentada

La protección de datos personales ha sido reconocida en diversos instrumentos, desde el seno de la Comunidad Internacional, hasta el Bloque Regional de la UE y el Acuerdo Bilateral UE-EE.UU. A causa de este escenario, las consecuencias jurídicas vinculantes de cada instrumento normativo difieren las unas de las otras porque dependen de la naturaleza jurídica de cada uno.[62] Las diferencias en la naturaleza jurídica de la legislación sobre protección de datos entre las culturas y los sistemas jurídicos han hecho más difícil llegar a un consenso internacional sobre el tema.[63]

Los puntos comunes y sobre todo las diferencias de definición y alcance en las diversas fuentes, trae complicaciones a la implementación de la protección de datos personales. Muchas actividades en el sector público o privado están bajo el alcance de los instrumentos de protección de datos personales que cubren gran cantidad de información.[64] Sin embargo, esto ha traído problemas a los individuos para ejercer sus derechos en otros países.[65] El principal inconveniente a efectos de jurisdicción es que el actor más poderoso que controla y procesa datos personales, la Corporación de IT, una Persona Jurídica

---

[62] Kuner, Christopher. "An International Legal Framework for Data Protection: Issues and Prospects." *Computer law & security review*, vol. 25, no. 4, 2009, p. 307.

[63] Kirby, Michael. "The History, Achievement and Future of the 1980 Oecd Guidelines on Privacy." *International Data Privacy Law*, vol. 1, no. 1, 2011, pp. 6-14.

[64] Cate, Fred H. "The Failure of Fair Information Practice Principles." *Consumer Protection in the Age of the Information Economy,* 2006.

[65] Kuner, Christopher. "Regulation of Transborder Data Flows under Data Protection and Privacy Law: Past, Present, and Future." *TILT Law & Technology Working Paper No. 016/2010*, 2010, p. 30.

Multilateral, está bajo la aplicación de la Ley de un territorio específico pero sus actividades son transfronterizas.[66]

Los instrumentos que reconocen el derecho a los datos personales han sido creados durante décadas, por lo que hay algunas disposiciones obsoletas en tales instrumentos jurídicos. Cuanto más avanza la tecnología, más complejidad trae en térinos jurídicos.[67] La aplicación del derecho de los interesados a la protección de los datos personales es cada vez más complicada debido a la naturaleza de los datos que se descentralizan a diversos tipos de organizaciones.[68]

El principio '*justo y lícito'* proporciona una *'lente'* a través de la cual deben interpretarse las demás disposiciones de la Directiva sobre protección de datos.[69] En la medida en que el procesador de datos no tiene ninguna obligación directa con respecto a los datos, ello afectará la forma en que se tratan los problemas de protección de datos en los negocios de procesamiento de datos y el intercambio de datos para la prevención y represión del crimen y el terrorismo,[70] especialmente cuando el Tercero es Sujeto a Jurisdicción Diferente.[71]

La jurisdicción de las normas de la UE y la aplicación extraterritorial de la legislación de protección de datos de la UE se reafirmó con mayor fuerza en el *Caso Google España.*[72]Al constatar que la ley de protección de datos de la UE se aplicaba en este caso, el Tribunal de Justicia observó que la Directiva debe interpretarse en el sentido de que tiene un

---

[66] Kuner, Christopher. "European Data Protection Law." *Corporate Compliance and Regulation,* Oxford University Press, UK, 2007, ch.2.37.

[67] De Hert, Paul and Schreuders, Eric. "The Relevance of Convention 108." *Proceedings of the Council of Europe Conference on Data Protection,* Warsaw, 2001, pp. 19-20, 34.

[68] Eberlein, Burkard and Newman, Abraham L. "Escaping the International Governance Dilemma? Incorporated Transgovernmental Networks in the European Union." *Governance*, vol. 21, no. 1, 2008, p. 40.

[69] Kuczerawy, Aleksandra and Coudert, Fanny. "Privacy Settings in Social Networking Sites: Is It Fair?." *IFIP PrimeLife International Summer School on Privacy and Identity Management for Life*, Springer, New York, 2010, pp. 237–238.

[70] Kuner, Christopher. "Regulation of Transborder Data Flows under Data Protection and Privacy Law: Past, Present, and Future." *TILT Law & Technology Working Paper No. 016/2010*, 2010, p. 29.

[71] Raab, Charles D. "Information Privacy: Networks of Regulation at the Subglobal Level." *Global Policy*, vol. 1, no. 3, 2010, pp. 291-302.

[72] CJEU. *Case C-131/12 Google Inc. v Agencia Española de Protección de Datos.* 13 May 2014.

alcance territorial particularmente amplio.[73] El TJUE también consideró que el derecho a suprimir datos en virtud de la Directiva de protección de datos de la UE se aplica a los resultados de los motores de búsqueda en Internet[74] (‘derecho al olvido" o ‘derecho a borrar’). Estos precedentes ofrecen a los usuarios de Internet de la UE un camino para ejercer sus derechos con las Corporaciones de IT transfronterizas, incluso aunque estas personas jurídicas no sean nacionales de la UE.

En la Unión Europea, diversos instrumentos jurídicos proporcionan a los individuos y a los reguladores un marco que permite la afirmación de derechos en relación con el procesamiento de datos en la UE. Por lo tanto, las autoridades de protección de datos de la UE están obligadas a cooperar entre sí,[75] y a menudo lo hacen en la práctica.[76] Las decisiones judiciales de un Estado miembro de la UE también pueden aplicarse con relativa facilidad en otro Estado miembro.[77] Sin embargo, los mismos instrumentos jurídicos no se aplican a situaciones en las que está implicado un país no perteneciente a la UE, lo que significa que no es posible que se realice esta cooperación reglamentaria reforzada ni que tampoco haya la misma facilidad de ejecución.[78] La dificultad de hacer valer los derechos en el extranjero no es exclusiva de la protección de datos, sino que deriva del hecho de que no existe un marco jurídico global para la afirmación de los derechos de los consumidores en el ciberespacio ni para el reconocimiento y la ejecución de decisiones judiciales en otros países.

[73] Rivero, Álvaro F. "Right to Be Forgotten in the European Court of Justice Google Spain Case: The Right Balance of Privacy Rights, Procedure, and Extraterritoriality." *European Union Working Papers*, no.19, Stanford-Vienna Transatlantic Technology Law Forum, 2017.

[74] CJEU. *Case C-131/12 Google Inc. v Agencia Española de Protección de Datos.* 13 May 2014. paras. 89-99.

[75] EU. *Directive 95/46/EC*. 1995, Article 28(6).

[76] For example, a DPA of an EU Member State informed the author that it receives 20 to 30 cooperation requests annually from other EU DPAs.

[77] European Council Regulation (EC) 44/2001 of 22 December 2000 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters, [2001] OJ L12/1.

[78] Kuner, Christopher. "Regulation of Transborder Data Flows under Data Protection and Privacy Law: Past, Present, and Future." *TILT Law & Technology Working Paper No. 016/2010*, 2010, p. 32.

3.1.1.3. Exenciones vagas y falta de supervisión de la vigilancia de datos en el procedimiento penal

Al igual que otros Derechos Humanos, el derecho a la protección de datos personales no es absoluto. Puede ser restringido en ciertas situaciones en especial cuando colisione con otros derechos.[79] En la mayoría de los casos se trata de la relación entre el estado de emergencia y la protección de datos personales.[80] Las autoridades estatales y los tribunales deben sopesar las razones para acceder a ciertos datos y el efecto potencial sobre una persona de tal vigilancia estatal.[81] Se debe prever una condición previa y una solución proporcionada, en la que se tengan en cuenta los intereses del Estado y del público, así como los intereses de la persona afectada.[82] Sin embargo, las corporaciones de IT más poderosas se encuentran bajo las leyes de seguridad nacional de los Estados Unidos, Ley Patriota, Ley de Seguridad Nacional y Ley de Vigilancia de Inteligencia Extranjera, que pueden comprometer el pleno disfrute de la protección de datos personales.

La mayoría de los instrumentos de protección de datos imponen una obligación similar a las autoridades públicas y a las personas privadas.[83] Después de todo, los Derechos Humanos tienen como objetivo principal limitar las acciones de las autoridades públicas a fin de proteger las actividades de las personas privadas, incluido el tratamiento de datos personales, de la interferencia del Estado.[84] Sin embargo, la efectividad del control de acceso de las excepciones de seguridad nacional es relevante para la existencia de puertas traseras u otros medios de acceso a datos personales no cifrados y abiertos por el proveedor de servicios, la Corporación de IT.

---

[79] Galetta, Antonella and De Hert, Paul. *A European perspective on data protection and access rights*. Vrije Universiteit, Brussel, 2013, p. 4.

[80] Nowak, Manfred. *United Nations Covenant on Civil and Political Rights: Ccpr Commentary.* Engel, Lancaster, 1993, p. 462.

[81] Human Rights Committee. *Communication No. 488/1992 Toonan v Australia*. 1992, para. 8.3; see also *communications Nos. 903/1999*. 1999, para.7.3; and *1482/2006*. 2006, paras.10.1 and 10.2.

[82] Mendel, Toby et al. *Global Survey on Internet Privacy and Freedom of Expression.* UNESCO, Paris, 2012, pp. 53 and 99.

[83] Kokott, Juliane and Sobotta, Christoph. "The Distinction between Privacy and Data Protection in the Jurisprudence of the Cjeu and the Ecthr." *International Data Privacy Law*, vol. 3, no. 4, 2013, p. 226.

[84] Masing, Johannes. "Herausforderungen Des Datenschutzes." *Neue Juristische Wochenschrift*, vol. 65, no. 33, 2012, pp. 2305-2306. ; Grimm, Dieter. “Der Datenschutz vor einer Neuorientierung” *Juristenzeitung*, 2013, p. 585.

En el caso *Centro de Información de Privacidad de Eletrónica v. Agencia de Seguridad Nacional*, el Circuito DC sostuvo que la respuesta *Glomar* de la NSA (permanece en silencio cuando la consulta es cara a cara) satisfizo suficientemente los requisitos de exención de la Ley de Libertad de Información porque la evaluación de amenaza es una función indiscutible de la NSA y esta no estaba obligada a confirmar o negar la existencia de ningún registro de respuesta.[85] Este caso afirmó el poder de excepción de Seguridad Nacional para ejercer la misión en secreto por encima de la protección de los derechos civiles.

Los problemas surgidos del conjunto de Leyes de Seguridad fueron dejados a la interpretación, en procedimientos secretos, en manos de órganos administrativos como el *Tribunal de Vigilancia de Inteligencia Extranjera* (FISC y el tribunal de revisión superior FISCR) cuyos jueces son nombrados exclusivamente por el Presidente del Tribunal Supremo. Parece que los tribunales de la FISA están de acuerdo con el argumento del gobierno de que es común en las investigaciones que algunos corpus de registros indefinidamente grandes sean considerados "pertinentes", a fin de descubrir las pruebas reales.[86] En consecuencia, la falta de supervisión es la principal amenaza para la protección de datos personales en todo el mundo, ya que se basa en decisiones administrativas relacionadas con los tribunales estadounidenses. Además, el ciudadano no estadounidense no tiene derecho a apelar en la Corte de los Estados Unidos por tales violaciones.

En el *Caso de Digital Rights Ireland,* cabe señalar en particular el principio de limitación del objetivo,[87] el derecho de acceso de los particulares a sus datos personales y el control por parte de las autoridades independientes de protección de datos.[88] En ese sentido, se señaló que la retención de datos necesita un fragmento de evidencia que sugiera que su conducta podría estar relacionada con un crimen grave y nadie está exento de esta regla. Se aplica incluso a aquellos cuyas comunicaciones están sujetas al secreto profesional, de

---

[85] United States Court of Appeal Second Circuit*. Case 678 F.3d Electronic Privacy Information Center v. National Security Agency*. 2012, paras. 934-5.

[86] Bowden, Caspar. "Directorate General For Internal Policies." *The Us Surveillance Programmes and Their Impact on EU Citizens' Fundamental Right,* European Parliament, Brussels, 2013, p. 12.

[87] CJEU. *ECLI:EU:C:2014:238 Joined cases C-293/12 and C-594/12*, *Digital Rights Ireland* (C-293/12) and *Seitlinger* (C-594/12). 2014.

[88] Control is an essential component of the protection of the individual: EU. *Directive 95/46/EC*. Recital 62; and case law of CJEU, *Case C-362/14 Schrems. 2014*, p. 42.

acuerdo con las normas nacionales.[89] Posteriormente, la Directiva sobre retención de datos fue invalidada por el TJUE el 8 de abril de 2014, ya que no cumplía el principio de la UE de excepciones proporcionadas y necesarias.

3.1.2. Mejoras y límites en la protección de datos personales tras las reformas de 2013 del régimen jurídico del Mercado electrónico de UE y UE-EE.UU..

Después de que todos las cuestiones suscitadas ante los tribunales de EE.UU. y la UE en los casos anteriores, el Gobierno de EE.UU. y la Unidad de Legislación de la UE pusieron en marcha un conjunto de normas en interés de la reforma.

Los EE.UU. y la UE nombraron una comisión para crear cambios a fin de lograr la mejor solución en el manejo de los problemas. Con este punto de partida, la UE aprobó el Reglamento General de Protección de Datos (GDPR) y la Directiva sobre asuntos judiciales y penales, luego consiguió que los Estados Unidos firmaran un acuerdo para aplicar las normas del UE-EE.UU. *Privacy Shield* para la protección general de datos en ambos territorios. Estas reformas tuvieron lugar desde abril de 2016 y entrarán plenamente en vigor en 2018.

Sin embargo, la génesis de estas reformas se remonta a los cambios provocados por Estados Unidos desde finales de 2013 debido a la presión internacional sobre los programas mundiales de vigilancia electrónica masiva de su Gobierno, especialmente la ejercida por la UE, su principal contraparte en el mercado único electrónico.

3.1.2.1. Respuestas de los Estados Unidos relativas a la protección de datos personales para ciudadanos no estadounidenses

Hay iniciativas de EE.UU. y la UE para abordar el problema de la protección de datos personales en la era digital. El Gobierno de los Estados Unidos había lanzado un conjunto de leyes para reformar su actividad de vigilancia y proporcionar a los ciudadanos no estadounidenses una mayor protección de sus datos personales.

[89] Ramos, Mario H. "Una Vuelta De Tuerca Más a Las Relaciones En Materia De Protección De Datos Entre La Ue Y Los Estados Unidos: La Invalidez De La Decisión Puerto Seguro." *Revista General de Derecho Europeo*, no. 39, 2016, p. 32.

En marzo de 2014, el gobierno de los Estados Unidos adoptó seis principios de privacidad para regular la vigilancia. Este marco Norteamericano declarado por el Presidente Obama en la Directiva Política Presidencial 28 (PPD-28) pretende proteger mejor los datos personales de todas las personas, incluidos los no ciudadanos de los EE.UU. en todo el mundo. [90]

La mejora fundamental es la Ley de reparación judicial, que extiende a los ciudadanos de la UE los mismos derechos de que disfrutan los ciudadanos de los EE.UU. en virtud de la Ley de Privacidad de 1974 con respecto a las obligaciones de los Estados Unidos en materia de protección de datos. Además, la Ley de Reparación Judicial otorga a los ciudadanos de la UE el acceso a los tribunales de los Estados Unidos para hacer cumplir los derechos de privacidad en relación con los datos personales transferidos a los Estados Unidos para fines de aplicación de la ley.[91]

El GDPR se aplica a las organizaciones establecidas en un tercer país si ofrecen bienes y servicios o vigilan el comportamiento de los individuos en la UE.[92] También introduce algunos nuevos instrumentos para las transferencias internacionales. Así mismo proporciona elementos más precisos y detallados que deben tenerse en cuenta al evaluar el nivel de protección de datos proporcionado en el ordenamiento jurídico de un tercer país.[93]

En virtud del Privacy Shield, el mecanismo de reparación informará a un denunciante de que un asunto de acceso o vigilancia ha sido debidamente investigado y obligado por ley estadounidense. En el caso de incumplimiento se solucionará adecuadamente.[94] Los ciudadanos de la UE tienen la capacidad de presentar quejas directamente a sus DPA locales. Los recursos y el modo en como se hayan establecidos

---

[90] Busby, Scott. "State Department on Internet Freedom at RightsCon", 4 Mar. 2014, www.humanrights.gov/2014/03/04/ state-department-on-internet-freedom-at-rightscon/. Accessed 14 Nov. 2015.

[91] European Commission. *EU-U.S. Privacy Shield: Frequently Asked Questions*. Brussels. 29 Feb. 2016.

[92] European Commission. *Communication From The Commission to The European Parliament and The Council Transatlantic Data Flows: Restoring Trust through Strong Safeguards, COM(2016) 117 final*. Brussels, 29 Feb. 2016, pp. 5-6.

[93] DLA Piper. "EU General Data Protection Regulation - Key Changes | DLA Piper Global Law Firm." www.dlapiper.com/en/uk/focus/eu-data-protection-regulation/key-changes/. Accessed 14 Jan. 2017.

[94] Weiss, Martin A and Archick, Kristin. "US-EU Data Privacy: From Safe Harbor to Privacy Shield." *Congressional Research Service*, 2016, p. 14.

determinan el período para las respuestas planteadas por los sujetos. El *Privacy Shield* también crea un nuevo derecho de arbitraje para las quejas no resueltas.[95]

No obstante, el Acuerdo marco no prevé la igualdad de derechos y recursos para los nacionales de la UE y de los Estados Unidos en los Estados Unidos de América y lo que es peor aún, los ciudadanos de terceros países que viven en Estados miembros de la UE que no son nacionales del Estado miembro afectado y cuyos datos pueden haber sido enviados a los EE.UU. no se contemplan en el Acuerdo.[96]

3.1.2.2. Armonizar la norma jurídica transatlántica

El GDPR se aplica a las organizaciones establecidas en un tercer país si ofrecen bienes y servicios o vigilan el comportamiento de los individuos en la UE.[97] Establece un régimen de sanciones eficaz armonizando las competencias de las autoridades nacionales de supervisión de la protección de datos (DPA). Sus facultades alcanzan a la imposición de multas de hasta 20 millones de euros o hasta un 4% del volumen de negocios sobre el total anual de una empresa.[98]

Los principios básicos de la protección de la intimidad entre la UE y los Estados Unidos son los mismos que en el *Safe Harbor* armonizando la protección de datos dentro del mercado único europeo. El *Privacy Shield* incluye declaraciones con respecto a órgano de cumplimiento, un nuevo derecho de arbitraje, así como respecto a revelaciones a las autoridades públicas y la responsabilidad de la compañía por transferencias posteriores.[99]

La Directiva de la UE sobre asuntos penales y judiciales incluye normas armonizadas para las transferencias internacionales de datos personales en el contexto de la

[95] Working Party Article29. *Opinion 01/2016 on the EU – U.S. Privacy Shield draft adequacy decision*. 13 Apr. 2016.

[96] Korff , Douwe. "EU-US Umbrella Data Protection Agreement : Detailed Analysis by Douwe Korff." *European Area of Freedom Security & Justice*, 14 Oct. 2015, https://free-group.eu/2015/10/14/eu-us-umbrella-data-protection-agreement-detailed-analysis-by-douwe-korff/. Accessed 12 Apr.2017.

[97] Hunton&Williams. *Overview of the EU General Data Protection Regulation*. 2016.

[98] European Commission. *Agreement on Commission's EU Data Protection Reform Will Boost Digital Single Market*. Brussels, 15 Dec. 2015, p. 2.

[99] Weiss, Martin A and Archick, Kristin. "US-EU Data Privacy: From Safe Harbor to Privacy Shield." *Congressional Research Service*, 2016, p. 14.

cooperación en la aplicación de la legislación penal.[100]Permitirá a las autoridades policiales y judiciales cooperar más eficazmente, tanto entre los Estados miembros como entre los Estados miembros y sus socios internacionales, para luchar contra la delincuencia y el terrorismo.[101] Insta al Estado a que proporcione autoridades nacionales independientes de protección de datos que ofrezcan a las personas recursos judiciales eficaces.[102]

Las garantías y salvaguardias del acuerdo marco UE-Estados Unidos se aplicarán a todos los intercambios de datos que tengan lugar en el contexto de la cooperación transatlántica en materia penal a todos los niveles. La disposición abarca todos los principios sustantivos de protección de datos de la UE; Normas de procesamiento, salvaguardias y derechos individuales.[103] El Acuerdo proporciona a los titulares de los datos derechos de reparación judicial relativos a las reformas del derecho interno estadounidense para apoyar al ciudadano de la UE. Sin embargo, contiene algunas deficiencias amenazantes para el estándar de protección de datos de la UE,como una definición diferente, acerca de los derechos del sujeto que reclame protección para sus datos personales, en especial cuando este sea nacional de un tercer Estado.[104]

3.1.2.3. Equilibrar los intereses entre los titulares del derecho y la autoridad estatal en materia penal

Tras una revisión por un grupo de independientes nombrado por el Presidente Obama, el ejecutivo de Estados Unidos hizo cambios significativos para mejorar el cumplimiento de sus prácticas de inteligencia extranjera adecuándolas al derecho

[100] European Commission. *EU Data protection reform on track: Commission proposal on new data protection rules in law enforcement area backed by Justice Ministers*. Luxembourg, 9 Oct. 2015, p. 1.

[101] European Commission. *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: The European Agenda on Security,* COM(2015) 185 final. Strasbourg, 28 Apr. 2015.

[102] European Commission. *Communication From The Commission to The European Parliament and The Council Transatlantic Data Flows: Restoring Trust through Strong Safeguards, COM(2016) 117 final*. Brussels, 29 Feb. 2016, p. 5.

[103] Working Party Article29. *Statement of the Working Party 29 on the EU – U.S. Umbrella Agreement*. Brussels, Oct. 2016, pp. 1-2.

[104] Korff , Douwe. "EU-US Umbrella Data Protection Agreement : Detailed Analysis by Douwe Korff." *European Area of Freedom Security & Justice*, 14 Oct. 2015, https://free-group.eu/2015/10/14/eu-us-umbrella-data-protection-agreement-detailed-analysis-by-douwe-korff/. Accessed 12 Apr.2017.

internacional y a los Derechos Humanos. Estos cambios incluyen sobre todo definiciones más específicas de los propósitos para los cuales se puede realizar la vigilancia.[105]

Desde marzo de 2014, el gobierno de los Estados Unidos adoptó la Directiva 28 (PPD-28), Marco de los Estados Unidos, para regir la vigilancia con seis principios de privacidad. Impone importantes limitaciones para las operaciones de inteligencia. Especifica que la recolección de datos por parte de los servicios de inteligencia debe tener un objetivo concreto. Adicionalmente, el PPD-28 limita el uso de la recolección de datos a gran escala a 6 propósitos: Detectar y contrarrestar las amenazas de espionaje, terrorismo, armas de destrucción masiva, amenazas a las Fuerzas Armadas o amenazas criminales transnacionales.[106] Los seis principios respaldados por los Estados Unidos son: 1) el estado de derecho; 2) el propósito legítimo; 3) la no arbitrariedad; 4) la autoridad externa competente; 5) la supervisión significativa; y 6) el aumento de la transparencia y la responsabilidad democrática.[107] Sin embargo, permanecen algunos solapamientos entre el Marco General EEUU y estos Principios que, en la práctica, puede llevar a incumplimientos por parte estadounidense, muy especialmente si se tiene en cuenta que el precendente del caso Glomar Response sigue vigente.

Además, Estados Unidos ha revisado la USA Freedom Act, impidiendo la recolección masiva de datos pues se exige un nexo a una investigación, aportando claridad a la Sección 215 de la Ley Patriota, aumentando la supervisión del FISC e introduciendo un defensor especial, aumentando la capacidad de las compañías para revelar solicitudes de datos de seguridad nacional gubernamental, e incrementando el poder de los órganos de supervisión interna, así como añadiendo controles externos.[108]

La mejora fundamental es la Ley de reparación judicial, que extiende a los ciudadanos de la UE el disfrute de la Ley de Privacidad de 1974 con respecto a las obligaciones de los Estados Unidos en materia de protección de datos. Sin embargo, su

---

[105] Obama, Barack. *US Presidential Policy Directive 28 – Signals Intelligence Activities*. The White House Office of the Press Secretary, 17 Jan. 2014.

[106] European Commission. *EU-U.S. Privacy Shield: Frequently Asked Questions*. Brussels, 29 Feb. 2016.

[107] Obama, Barack. *US Presidential Policy Directive 28 – Signals Intelligence Activities*. The White House Office of the Press Secretary, 17 Jan. 2014.

[108] Stepanovich, Amie and Mitnick, Drew and Robinson, Kayla. "United States: the necessary and proportionate principle and US Government." *Global Information Society Watch 2014: Communication Surveillance in Digital Age*, 2014, p. 265.

aplicación es limitada porque hay muchas excepciones y la inseguridad jurídica respecto de los organismos encargados de la aplicación de la citada Ley de reparación judicial no satisfacen el requisito de ofrecer un mecanismo de reparación efectivo a todas las personas involucradas en casos de vigilancia dirigidos desde Seguridad Nacional.[109] Además, la Ley de Reparación Judicial otorga a los ciudadanos de la UE el acceso a los tribunales de los Estados Unidos para hacer cumplir los derechos de privacidad en relación con los datos personales transferidos a los Estados Unidos para fines de aplicación de la ley.[110] Quienes no sean ciudadanos de la UE no tienen derecho a disfrutar de estos derechos.

El GDPR proporciona excepciones exhaustivas, detalladas y transparentes a la transferencia de datos personales fuera de la UE. La reforma aclara esas reglas de muchas maneras.[111] Las disposiciones sobre la independencia, las funciones y los poderes de las APD de la UE se expresan con más detalle y se mejoran sustancialmente. Esto incluye expresamente el poder de suspender los flujos de datos a un receptor en un tercer país o a una organización internacional.[112]

El *Privacy Shield* tiene límites de retención de datos claros, restricciones, salvaguardas y mecanismos de supervisión para el acceso de las agencias estatales con propósitos de aplicación de la ley y seguridad nacional. Transforma el sistema de supervisión de autorregulación a un sistema más activo y proactivo. La certificación y el proceso de recertificación anual permanecen, pero el Departamento de Comercio supervisará su cumplimiento mediante cuestionarios detallados.[113] Por otra parte, la Comisión Federal de Comercio mantendrá una "Flag List" para las organizaciones que están sujetas a la FTC o a órdenes judiciales en casos relativos al Privacy Shield.

La Directiva de la UE en materia penal establece normas transparentes, detalladas y exhaustivas para la transferencia de datos personales a terceros países, incluida la facultad de suspender los flujos de datos a un destinatario en un tercer país o a una

[109] European Data protection Supervisor. *Opinion 1/2016*. 12 Feb. 2016, p. 43.

[110] European Commission. *EU-U.S. Privacy Shield: Frequently Asked Questions*. Brussels, 29 Feb. 2016.

[111] European Commission. *Questions and Answers - Data protection reform*. Brussels. 21 Dec. 2015, p. 3.

[112] European Commission. *Agreement on Commission's EU Data Protection Reform Will Boost Digital Single Market*. Brussels, 15 Dec. 2015, p. 3.

[113] European Commission. *Communication From The Commission to The European Parliament and The Council Transatlantic Data Flows: Restoring Trust through Strong Safeguards, COM(2016) 117 final*. Brussels, 29 Feb. 2016, pp. 9-10.

organización internacional que no cumple la norma de adecuación.[114] La nueva Directiva elevará el nivel de protección de las personas. Las víctimas, los testigos y los sospechosos de crímenes están protegidos en el contexto de una investigación penal o de una acción de aplicación de la ley. La supervisión está garantizada por las autoridades nacionales independientes de protección de datos.[115]

El Acuerdo Paraguas UE-EEUU no contiene una cláusula general de Derechos Humanos que prohíba la "compartición" o "transferencia" de datos sobre personas de la UE, sujetos al Acuerdo, con otros organismos, en los EE.UU. Ello podría dar lugar a graves violaciones de los Derechos Humanos, como la retención y la detención arbitrarias, la tortura o incluso las ejecuciones extrajudiciales o "desapariciones" de los interesados u otras personas.[116] También expande a todo el ámbito de la aplicación de la ley el principio de supervisión independiente, incluyendo poderes efectivos para investigar y resolver quejas individuales.[117] Sin embargo, en términos de transparencia y supervisión, no cumple con las exigencias fundamentales de protección de datos y de Derechos Humanos en Europa, ya que las personas afectadas no pueden presentar su recurso ante el FISC.

Las reformas del régimen de la UE y de la UE-Estados Unidos establecen una normativa armonizada que puede servir de modelo para países liberales con una economía de mercado. La Comunidad Internacional podría utilizar este conjunto de normas como fundamento para redactar un Instrumento Internacional sobre Protección de Datos de Carácter Personal para su firma y adhesión. El enfoque más incluyente resolvería el problema de jurisdicción y haría posible el cumplimiento de la protección de datos personales a diferentes jurisdicciones.

---

[114] European Commission. *EU Data protection reform on track: Commission proposal on new data protection rules in law enforcement area backed by Justice Ministers*. Luxembourg, 9 Oct. 2015, p. 1.

[115] European Commission. *Communication From The Commission to The European Parliament and The Council Transatlantic Data Flows: Restoring Trust through Strong Safeguards, COM(2016) 117 final*. Brussels, 29 Feb. 2016, p. 5.

[116] Korff , Douwe. "EU-US Umbrella Data Protection Agreement : Detailed Analysis by Douwe Korff." *European Area of Freedom Security & Justice*, 14 Oct. 2015, https://free-group.eu/2015/10/14/eu-us-umbrella-data-protection-agreement-detailed-analysis-by-douwe-korff/. Accessed 12 Apr. 2017.

[117] European Commission. *Communication From The Commission to The European Parliament and The Council Transatlantic Data Flows: Restoring Trust through Strong Safeguards, COM(2016) 117 final*. Brussels, 29 Feb. 2016, p. 13.

3.2. Recomendaciones

Debido a la rápida difusión de Internet en las últimas dos décadas, ahora surge una nueva situación en la que las Corporaciones de TI multinacionales recogen una gran cantidad de datos personales directamente, pues el usuario pone sus datos en la Red Social y más aún indirectamente mediante la información alamacenada en la memoria de los buscadores o en la barra de pestañas. Muchas entidades privadas, incluidas corporaciones gigantes de TI o agencias estatales, tienen su propia "Regla" y diferentes estructuras para autorregular su sistema de información. Pero estas son las políticas que las propias organizaciones consideran apropiado promulgar y se basan principalmente en la autoverificación de tales Entidades. Además, la legislación nacional se promulga independientemente del hecho de que las empresas sean multinacionales y puede ser difícil buscar un vínculo directo con una jurisdicción determinada en un caso específico.[118] Esta diversificación de normativa entre la norma del Estado y la de la Corporación Internacional sumada a los problemas fácticos para determinar la competencia de la jurisdicción puede conducir con peligrosa facilidad a un punto muerto, desde la perspectiva de la protección de datos.

3.2.1. Conjunto único de normas comunes

Si bien la legislación sobre protección de datos tiene una dimensión transfronteriza, su posterior desarrollo adquirió características nacionales y regionales distintas. Con el fin de dar cabida a la cooperación internacional entre sistemas jurídicos de protección de datos fundamentalmente diferentes, se han emprendido una serie de iniciativas,[119] especialmente durante la última década.

El interesante esquema legal aplicado para el intercambio transatlántico de información personal es, en efecto, una solución legal de mosaico construida sobre bases bilaterales UE-EE.UU. Incluye el Escudo de Privacidad para intercambios fundamentales de datos personales y el Acuerdo Paraguas para la protección de las personas físicas con respecto al tratamiento de datos personales por las autoridades competentes con fines de

[118] Metcalf, Katrin N. "Legal Aspects of Privacy Law and Data Protection." *The Right to Privacy as a Human Right and Everyday Technologies*, Institute of Human Rights NGO, 2014, p. 85.

[119] De Hert, Paul and Papakonstantinou, Vagelis. "Three Scenarios for International Governance of Data Privacy: Towards an International Data Privacy Organization, Preferably a UN Agency." *ISJLP*, vol. 9, 2013, p. 293.

prevención, investigación, detección o enjuiciamiento de delitos o la ejecución de sanciones penales .

En cada lado del Atlántico, disposiciones en gran medida diferentes rigen el tratamiento respectivo una vez que se han transmitido los datos personales. El ejemplo UE-EE.UU. es un argumento poderoso para las ventajas de la introducción de un único instrumento internacional de protección de datos que hubiera salvado a ambas partes de una multitud de arreglos complejos y difíciles de seguir y, en última instancia, un importante desperdicio de recursos en la respectiva negociación y los procesos de redacción.[120]

A fin de cuentas, proporcionar un conjunto único de normas que se apliquen con uniformidad por las autoridades de supervisión de todo el mundo eliminaría los problemas presentes en muchos casos anteriores,[121] incluidas las disposiciones relativas a la situación de conflicto de leyes aplicables en diferentes jurisdicciones.

3.2.2 Regular una entidad transfronteriza de alta capacidad

Dado que las sentencias judiciales utilizaron en muchos casos el principio de territorialidad y el "Principio de adecuación" para abordar efectivamente la jurisdicción, la posibilidad de que algunas corporaciones de IT tendieran a seleccionar artificialmente la legislación nacional que debían cumplir y la autoridad nacional de protección de datos suponía un grave problema. Cuanto más se pueda introducir el "Principio de rendición de cuentas" para rastrear y perseguir la actividad de las Corporaciones Transnacionales de TI y las Agencias de Inteligencia Nacionales o Internacionales mayor seguridad habrá para los usuarios.

3.2.2.1. Regular una Corporación Transnacional de IT

Para emplear el principio de adecuación, se pueden utilizar las marcas de confianza relacionadas con la protección de datos, en particular los sellos web, representan la

[120] European Commission. *Agreement on Commission's EU Data Protection Reform Will Boost Digital Single Market*. Brussels, 15 Dec. 2015.

[121] Schmitt, Desirée. "Taking a Look at Two Cases in the Margin of the CJEU's "Privacy Spring", before and after the General Data Protection Regulation: Weltimmo and Bara." *Jean-Monnet-Saar*, 2016, http://jean-monnet-saar.eu/?p=1453. Accessed 10 Jan. 2017.

extensión práctica de los intentos de autorregulación por parte de las contrapartes del comercio electrónico. Mediante la colocación de sellos web en páginas de Internet, los miembros verifican el cumplimiento de las normas de protección de datos y las mejores prácticas más o menos de la misma manera que la notificación del tratamiento a las autoridades de protección de datos confirma su legalidad en el mercado electrónico. Véase el modelo de EE. UU. y su programa de sellos web TRUSTe (originalmente E-Trust) que se utiliza en un intento de convencer a la UE sobre la idoneidad de su protección de datos y más tarde en las negociaciones para la conclusión del Acuerdo *Safe Harbor*[122] así como *Privacy Shield* que permite que una empresa se registre. El *Privacy Shield* está controlado y garantizado por la Comisión Federal de Comercio de los Estados Unidos.[123]

Al adaptar el Principio de Rendición de Cuentas del Modelo de la OCDE, las organizaciones internacionales y regionales han publicado diversas leyes y normas de protección de datos personales. Estos códigos de conducta vienen en varios formatos y tipos.[124] Abarcan desde instrumentos de autorregulación de cumplimiento voluntario sin mecanismos de vigilancia o ejecución, hasta estrictas normas introducidas en cooperación con las autoridades nacionales de protección de datos e incluso ratificadas por la ley en estrictos sistemas de protección de datos similares a la UE. En efecto, se trata de códigos de conducta universales adoptados por grupos multinacionales de empresas y ratificados por las autoridades nacionales competentes en materia de protección de datos que definen la política global de protección de datos del grupo con respecto a las transferencias internacionales de datos personales dentro de un mismo grupo empresarial a entidades situadas en países que pueden no proporcionar un nivel adecuado de protección, según las normas de la UE.[125]

---

[122] Farrell, Henry. "Constructing the International Foundations of E-Commerce—the EU-US Safe Harbor Arrangement." *International Organization*, vol. 57, no. 02, 2003, p. 278.

[123] De Hert, Paul and Papakonstantinou, Vagelis. "Three Scenarios for International Governance of Data Privacy: Towards an International Data Privacy Organization, Preferably a UN Agency." *ISJLP*, vol. 9, 2013, p. 299.

[124] Kuner, Christopher. "Regulation of Transborder Data Flows under Data Protection and Privacy Law: Past, Present, and Future." *TILT Law & Technology Working Paper No. 016/2010*, 2010, p. 17

[125] *See* the relevant EU Commission data protection webpages, *available a*t http://ec.europa.eu/justice/policies/privacy/binding_rules/index_en.htm.

3.2.2.2. Regulación de la Agencia Estatal de Inteligencia

La parte encargada de la protección de datos para la policía y la justicia penal, especialmente las unidades de inteligencia nacionales e internacionales que combaten la delincuencia organizada y el terrorismo, debería tener en cuenta las necesidades específicas de la aplicación de la ley.[126] Debería proteger a todos, independientemente de que sean víctimas, delincuentes o testigos, y el Código de Inteligencia Internacional propuesto debería estar sujeto a serias consideraciones.[127] Todo proceso de aplicación de la ley en un Estado Parte debe cumplir con los principios de necesidad, proporcionalidad y legalidad, así como con las salvaguardias adecuadas para los individuos. La supervisión está garantizada por las autoridades nacionales de protección de datos, y así mismo deben proporcionarse recursos judiciales eficaces. Además, se aclaran las normas para la transferencia de datos personales a terceros países y los Estados parte pueden introducir un mayor nivel de protección en sus propias legislaciones nacionales.[128] Sin embargo, debe respetar las diferentes tradiciones jurídicas de los Estados Partes y ajustarse plenamente a los Tratados Internacionales de Derechos Humanos.[129]

3.2.3. Establecer la Institución Internacional de Protección de Datos

El régimen universal o internacional debería contener procedimientos innovadores e inventivos para la cooperación, la asistencia mutua, las operaciones conjuntas y un mecanismo de cooperacion.[130] Además, todas las autoridades nacionales de protección de datos deberían presentar anualmente informes de actividad, que se harían públicos.[131] Todo ello tiene por objeto garantizar la coherencia en la aplicación de la normativa por parte de las autoridades nacionales. El Régimen Universal debe imponer que el incumplimiento podría

[126] Milanovic, Marko. "Human Rights Treaties and Foreign Surveillance: Privacy in the Digital Age." *Harv. Int'l LJ*, vol. 56, 2015, pp. 88-93.

[127] Omtzigt, Pieter. *Mass Surveillance DOC.13734*. Committee on Legal Affairs and Human Rights Session, Brussels, 2015, p. 33.

[128] European Commission. *EU Data protection reform on track: Commission proposal on new data protection rules in law enforcement area backed by Justice Ministers*. Luxembourg, 9 Oct. 2015

[129] UN. *A/HRC/RES/17/4*. 2011.

[130] EU. *General Data Protection Regulation*. 2016. Articles. 60-76.

[131] Ibid, Article 59.

conducir a sanciones. Si las empresas no cumplen en la práctica se enfrentan a sanciones y la eliminación de la lista,[132] como Trustmark Emblems.

El Régimen Universal debe resolver la cuestión de la ventanilla única, las empresas y los individuos solo tendrán que lidiar con una sola autoridad supervisora. La ventanilla única para un denunciante individual sería un camino importante para un remedio eficaz y brindaría una mejor oportunidad al usuario de Internet de ponerse en contacto con el mecanismo de supervisión. Los mecanismos accesibles y asequibles de solución de controversias son ideales, a través de ellos la queja será resuelta por la propia compañía/autoridad, o por vías de soluciones de Resolución de Disputas Alternativas (ADR) gratuitas. El ADR debe ofrecerse si se trata de un caso de agotamiento del recurso interno; como último recurso habrá un mecanismo de arbitraje.[133] Además, la posibilidad de reparación en el ámbito de la seguridad nacional para los ciudadanos del Estado Parte debería ser manejada por un Defensor del Pueblo independiente de los servicios de inteligencia nacionales que participan.

La protección de datos para las autoridades policiales y de justicia penal necesita de la supervisión de autoridades nacionales independientes de protección de datos o de tribunales no parciales, capaces de proporcionar recursos judiciales eficaces para los afectados.[134]

El reconocimiento del poder de investigación de la autoridad nacional e internacional de supervisión debe diseñarse como un procedimiento para señalar las irregularidades a nivel internacional. Siempre que haya habido una constatación de incumplimiento, a raíz de una queja o una investigación, la Corporación de TI debe estar sujeta a una investigación específica de seguimiento[135] posterior.

---

[132] European Commission. *EU Commission and United States agree on new framework for transatlantic data flows: EU-US Privacy Shield*. Strasbourg, 2 Feb. 2016.

[133] European Commission. *European Commission launches EU-U.S. Privacy Shield: stronger protection for transatlantic data flows*. Brussels, 12 July 2016**.**

[134] European Commission. *Questions and Answers on the EU-US data protection "Umbrella agreement"*. Brussels, 1 Dec. 2016.

[135] European Commission. *Restoring Trust in EU-US data flows - Frequently Asked Questions*. Brussels, 27 Nov. 2013, p. 4.

Chapter 1 Designing the Research

The first chapter describe the structure of the research by differentiate into 7 sections. Primarily, the important words and legal terms will be defined within the context of personal data protection studies. Second, reviewing the effects Cyberspace has brought into Legal Atmosphere and the changes arise from various legal points. Third, the classical conflict between Human Rights and their limitations on the basis of Security will be explored. Forth, reflect the impacts Data Processing might put on the right to personal data protection. Five, it will describe how the research have been investigating through the next 5 chapters. The last two sections explain the main Methods and Methodologies taken into account for the research, the delimitation of our objective of study, and the Research Hypothesis.

1.1. Keywords, Terms and Definition

This section will make a clear perception on what to be mention in the rest of thesis by providing the explicit definition of important word relating personal data protection, Cyberspace and E-Market. These terms have different meaning in various contexts but the research will choose only the relevant definition for personal data protection studies. The definitions of the key words which are included are as follows;

1) Internet

Internet is a global computer network providing a variety of information and communication facilities which consisting of interconnected networks using standardized communication protocols.[1]

It is a network of networks that consists of millions of private, public, academic, business, and government networks, of local to global scope, that are linked by a broad array of electronic, wireless, and optical networking technologies. The Internet carries an extensive range of information resources and services, such as the inter-linked hypertext documents

[1] "Internet - Definition of Internet in English | Oxford Dictionaries", *Oxford Dictionaries | English*, https://en.oxforddictionaries.com/definition/internet. Accessed 2 May 2014.

and applications of the World Wide Web (WWW), the infrastructure to support email, and peer-to-peer networks for file.[2]

2) Cyberspace

Cyberspace is "the notional environment in which communication over computer networks occurs."[3] The term was first used in science fiction and cinema in the 1980s, was adopted by computer professionals and became a household term in the 1990s. During this period, the uses of the internet, networking, and digital communication were all growing dramatically and the term "cyberspace" was able to represent the many new ideas and phenomena that were emerging.[4]

The parent term of cyberspace is "cybernetics", derived from the Ancient Greek κυβερνήτης (kybernētēs, steersman, governor, pilot, or rudder), a word introduced by Norbert Wiener for his pioneering work in electronic communication and control science.[5]

As a social experience, individuals can interact, exchange ideas, share information, provide social support, conduct business, direct actions, create artistic media, play games, engage in political discussion, and so on, using this global network. Cyberspace is defined more by the social interactions involved rather than its technical implementation.[6] The term *cyberspace* has become a conventional means to describe anything associated with the Internet and the diverse Internet culture. Amongst individuals on cyberspace, there is believed to be a code of shared rules and ethics mutually beneficial for all to follow, referred to as cyberethics. Many view the right to privacy as most important to a functional code of

[2] "Internet: Need to Cite Wikipedia since It Is the Biggest Open "internet" Access Website for Common Definition", *Wikipedia*, https://en.wikipedia.org/wiki/Internet:_Need_to_cite_Wikipedia_since_it_is_the_biggest_open_%E2%80%98internet%E2%80%99_access_website_for_common_definition. Accessed 2 May 2014.

[3] "Cyberspace - Definition of Cyberspace in English | Oxford Dictionaries", *Oxford Dictionaries | English*, https://en.oxforddictionaries.com/definition/us/cyberspace. Accessed 2 May 2014.

[4] Strate, Lance. "The Varieties of Cyberspace: Problems in Definition and Delimitation", *Western Journal of Communication*, Vol.63, 1999, pp. 382–3.

[5] Crofton, Isaak. *Crypto Anarchy*. Lulu, 2015, p. 84.

[6] Morningstar, Chip and Randall, Farmer R. "The Lessons of Lucasfilm's Habitat." *The New Media Reader*. Ed. Wardrip-Fruin and Nick Montfort: The MIT Press, 2003, Massachusetts, pp. 664-667.

cyberethics.[7] Such moral responsibilities go hand in hand when working online with global networks, specifically, when opinions are involved with online social experiences.[8]

In the views of users, the computational medium in cyberspace is an augmentation of the communication channel between real people; the core characteristic of cyberspace is that it offers an environment that consists of many participants with the ability to affect and influence each other. They derive this concept from the observation that people seek richness, complexity, and depth within a virtual world.[9]

3) E-Market

E-Market is a Market in electronic form, especially the use of electronic data transfer for information exchange and economic transactions via the Internet.[10] By using the internet, E-Market is a space where organizations and consumers exchange information and do business.[11]

E-Market is open to several buyers and several sellers by being a trading platform, the E-Market itself does not sell nor buy goods or services traded on the platform but it has at least one trading function. Sometime supplier directories support companies in establishing new business relationships but no actual trade takes place at these platforms. E-markets and supplier directories are also called Business to Business (B2B) Internet platforms. Such platforms include all Internet-based technical solutions that aim at facilitating the establishment of new trading relationships between companies or at supporting existing relationships.[12] Many sharing economy platforms are in fact peer to peer (P2P) marketplaces.

---

[7] Spinello, Richard A. *Cyberethics: Morality and Law in Cyberspace.* Jones & Bartlett Publishers, Massachusetts, 2014.

[8] White House. *The National Strategy to Secure Cyberspace*. 2003.

[9] Crofton, Isaak. *Crypto Anarchy*. Lulu, 2015, p. 84.

[10] "E- market- Definition of E-market in English | Oxford Dictionaries", *Oxford Dictionaries | English*, https://en.oxforddictionaries.com/definition/e-market. Accessed 1 May 2014.

[11] "E-Marketplace Meaning in the Cambridge English Dictionary", http://dictionary.cambridge.org/dictionary/english/e-marketplace. Accessed 1 May 2014.

[12] "What Is an Electronic Marketplace?: Learn How Your Company Can Use E-Markets to Expand Your Business", *eMarket Services*, www.emarketservices.com:80/start/Knowledge/index.html. Accessed 1 May 2014.

Also called "switch" marketplaces, sharing economy platforms' users will characteristically switch between buying and selling services or goods.[13]

In this research the information about activities done in E-market is the object of the studies since many Service Providers collect these data for processing.

4) Personal Data

Personal Data means data[14] or information[15] relating to an identified or identifiable natural person,[16] understanding identifiable natural person is one who can be identified,[17] directly or indirectly,[18] in particular by reference to an identifier such as a name, location data, an online identifier,[19] an identification number or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.[20] Personal Data might be recorded in any form.[21] This definition covers both side of Trans-Atlantic relations, EU and EU-US.

Personally identifiable information (PII), some countries such as USA use the PII as a legal concept,[22] not just a technical concept. Because of the versatility and power of modern

[13] Hamari, Juho et al. "The Sharing Economy: Why People Participate in Collaborative Consumption." *Journal of the Association for Information Science and Technology*, vol. 67, no. 9, 2016, pp. 2047–59

[14] EU-US. *Privacy Shield*. 2016, Overview para. 8(a).

[15] EU. *General Data Protection Regulation*. 2016, Article 4(1); EU. *Directive on Criminal Matters 2016/680*. 2016, Article 3(1); EU-US. *Umbrella Agreement*. 2016, Article 2(1).

[16] EU-US. *Privacy Shield*. 2016, Overview para. 8(a); EU-US. *Umbrella Agreement*. 2016, Article 2(1).

[17] EU. *General Data Protection Regulation*. 2016, Article 4(1); EU. *Directive on Criminal Matters 2016/680*. 2016, Article 3(1); EU-US. *Privacy Shield*. 2016, Overview para. 8(a).

[18] EU. *General Data Protection Regulation*. 2016, Article 4(1); EU. *Directive on Criminal Matters 2016/680*. 2016, Article 3(1); EU-US. *Umbrella Agreement.* 2016, Article 2(1).

[19] EU. *General Data Protection Regulation*. 2016, Article 4(1); EU. *Directive on Criminal Matters 2016/680*. 2016, Article 3(1).

[20] EU. *General Data Protection Regulation*. 2016, Article 4(1); EU. *Directive on Criminal Matters 2016/680*. 2016, Article 3(1); EU-US. *Umbrella Agreement*. 2016, Article 2(1).

[21] EU-US. *Privacy Shield*. 2016, Overview para. 8(a).

[22] De Montjoye, Yves-Alexandre et al. "Unique in the Crowd: The Privacy Bounds of Human Mobility." *Scientific reports*, vol. 3, 2013, p. 1376.

re-identification algorithms,[23] the absence of PII data does not mean that the remaining data does not identify individuals.[24] While some attributes may be uniquely identifying on their own,[25] any attribute can be identifying in combination with others.[26] This definition is important because it reflects the personal data protection law of the US which heavily influence to the study of this research.

5) Data Subject

Data Subject is a living individual to whom personal data relates.[27] Data Subject is an identifiable natural person who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.[28]

6) Data Controller

Data Controller means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data[29]; where the purposes and means of such processing are

[23] Narayanan, Arvind and Vitaly Shmatikov. "Robust De-Anonymization of Large Sparse Datasets." *Security and Privacy, IEEE Symposium,* 2008, pp. 111-125.

[24] Narayanan, Arvind and Vitaly Shmatikov. "De-Anonymizing Social Networks." *Security and Privacy, 2009 30th IEEE Symposium*, 2009, p. 173.

[25] Narayanan, Arvind and Vitaly Shmatikov. "Myths and Fallacies of Personally Identifiable Information." *Communications of the ACM*, vol. 53, no. 6, 2010, p. 24.

[26] Ohm, Paul. "Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization." *UCLA Law Review*, no.197, 2009.

[27] "What Is a Data Subject? // A Definition from the Opt-4 Data Protection Dictionary", www.opt-4.co.uk/dictionary/DataSubject.asp. Accessed 2 May 2014.

[28] EU. *General Data Protection Regulation*. 2016, Article 4(1); EU. *Directive on Criminal Matters 2016/680*. 2016, Article 3(1).

[29] EU. *General Data Protection Regulation*. 2016, Article 4(7); EU. *Directive on Criminal Matters 2016/680*. 2016, Article 3(8); EU-US. *Privacy Shield*. 2016, Overview para. 8(c).

determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.[30]

7) Data Processor

Data Processor means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller. [31]

8) Third Party

Third Party means a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorized to process personal data.[32]

9) Data Collection

Data Collection is the process of gathering and measuring information on variables of interest, in an established systematic fashion that enables one to answer stated research questions, test hypotheses, and evaluate outcomes. The goal for all data collection is to capture quality evidence that then translates to rich data analysis and allows the building of a convincing and credible answer to questions that have been posed.[33]

[30] EU. *General Data Protection Regulation*. 2016, Article 4(7); EU. *Directive on Criminal Matters 2016/680*. 2016, Article 3(8).

[31] EU. *General Data Protection Regulation*. 2016, Article 4(8); EU. *Directive on Criminal Matters 2016/680*. 2016, Article 3(9).

[32] EU. *General Data Protection Regulation*. 2016, Article 4(10);

[33] Lescroël, Amélie et al. "Antarctic Climate Change: Extreme Events Disrupt Plastic Phenotypic Response in Adélie Penguins." *PloS one*, vol. 9, no. 1, 2014, p. e85291.

10) Data Processing

Data Processing means any operation or set of operations[34] which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.[35] Data Processing is involving collection, maintenance, use, alteration, organization or structuring, disclosure or dissemination, or disposition.[36]

11) Automated data processing

Automated Data Processing including Profiling means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.[37]

12) Data Transfer

Data Transfer or 'cross-border processing' means either: (a) processing of personal data which takes place in the context of the activities of establishments in more than one Member State of a controller or processor in the Union where the controller or processor is established in more than one Member State; or (b) processing of personal data which takes place in the context of the activities of a single establishment of a controller or processor in

[34] EU. *General Data Protection Regulation*. 2016, Article 4(2); EU. *Directive on Criminal Matters 2016/680*. 2016, Article 3(2); EU-US. *Privacy Shield*. 2016, Overview para. 8(b); EU-US. *Umbrella Agreement.* 2016, Article 2(2).

[35] EU. *General Data Protection Regulation*. 2016, Article 4(2), Article 4(1); EU. *Directive on Criminal Matters 2016/680*. 2016, Article 3(2); EU-US. *Privacy Shield*. 2016, Overview para. 8(b).

[36] EU-US. *Umbrella Agreement*. 2016, Article 2(2).

[37] EU. *General Data Protection Regulation*. 2016, Article 4(4); EU. *Directive on Criminal Matters 2016/680*. 2016, Article 3(4).

the Union but which substantially affects or is likely to substantially affect data subjects in more than one Member State.[38]

13) Data Surveillance

Data Surveillance is a careful continuous observation of a place, person, group especially of a suspected spy or criminal.[39] It is an ongoing activity in order to gather information[40] especially by the police or army, because of a crime that has happened or is expected. [41]

Data Surveillance is the monitoring of the behavior, activities, or other changing information, usually of people for the purpose of influencing, managing, directing, or protecting them.[42] This can include observation from a distance by means of electronic equipment, or interception of electronically transmitted information (such as Internet traffic or phone calls); and it can include simple, relatively no- or low-technology methods such as human intelligence agents and postal interception. The word surveillance comes from a French phrase for "watching over" ("sur" means "from above" and "veiller" means "to watch"), and is in contrast to more recent developments such as sousveillance.[43]

14) Pseudonymisation

Pseudonymisation means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is

[38] EU. *General Data Protection Regulation*. 2016, Article 4(23)

[39] "Surveillance - Definition of Surveillance in English | Oxford Dictionaries", *Oxford Dictionaries | English*, https://en.oxforddictionaries.com/definition/surveillanc. Accessed 2 May 2014.

[40] "Surveillance | Define Surveillance at Dictionary.com", www.dictionary.com/browse/surveillance. Accessed 2 May 2014.

[41] "Surveillance Meaning in the Cambridge English Dictionary", http://dictionary.cambridge.org/dictionary/english/surveillance. Accessed 2 May 2014.

[42] Lyon, David. *Surveillance Studies: An Overview*. Polity Press, Cambridge, 2007, p. 1.

[43] Clarke, Roger. "Information Technology and Dataveillance." *Communications of the ACM*, vol. 31, no. 5, 1988, pp. 498-512; Michael, Katina et al. "Planetary-Scale Rfid Services in an Age of Uberveillance." *Proceedings of the IEEE*, vol. 98, no. 9, 2010, pp. 1663-1671; Minsky, Marvin et al. "The Society of Intelligent Veillance." *Technology and Society (ISTAS),* IEEE International Symposium, 2013, pp. 13-17.

subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.[44]

15) Data Base

Data Base or 'filing system' means any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis.[45]

16) Cyber Security

Cyber Security or Computer security or IT security is information security as applied to computing devices such as computers and smart-phones, as well as computer networks such as private and public networks,[46] including the Internet as a whole. Data Security is the prevention or protection of personal data against breach or damage. Personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.[47]

Most of the definitions come from the legal concept which is written in various official legal documents; EU instruments, EU-US instruments and the US law, while some definitions are selected from the credible dictionary or well reputation website relating the specific terms. The rest of definitions extracted from the relevant books contain the content related to the concept of particular words. The scope of definition is the personal data protection on Cyberspace of the EU and EU-US legal regime.

---

[44] EU. *General Data Protection Regulation*. 2016, Article 4(5); EU. *Directive on Criminal Matters 2016/680.* 2016. Article 3(5).

[45] EU. *General Data Protection Regulation*. 2016, Article 4(6); EU. *Directive on Criminal Matters 2016/680*. 2016, Article 3(6).

[46] Peters, Sarah. *2009 Csi Computer Crime and Security Survey.* Computer Security Institute, 2009.

[47] EU. *General Data Protection Regulation*. 2016, Article 4(12); EU. *Directive on Criminal Matters 2016/680*. 2016, Article 3(11).

These specific keywords with the definition as given above will be used throughout the research from the start until the end.

1.2. Understanding Cyberspace in Legal Atmosphere

The section is reflected in anxiety. An anxiety is composite of the nature of the cyberspace while realizing the necessity for its regulation. This section will initially elucidate upon the influence actors such a regime must concern, i.e. the protection of data subject's rights by a various entities; State Authority, IT Corporation and International Community. Therefore it will explore any precaution for implementing regulation to different relations or crafting trans-border E-Market regulation. Accordingly, it will critically inquire how the specific characteristics of the cyberspace have impacted any legal atmosphere relate to it. More particularly, it will demonstrate how the counterpart wings of theorists, namely the exceptionist and unexceptionist, have described their contesting intellectual standpoints toward such characteristics. Finally, using diverse perspectives including Political, Economic, Social and Culture Rights perspective, it will review the complicated situations as to how the cyberspace is testing a space for trans-border regulation in terms of right protection, duty bearer obligation and law enforcement.

1) Actors in the Arena and their main interests

During the third wave revolution, there are actors which involve with information technology (IT) are performing via internet medium such as IT Corporations, States, Individual Internet users. The Internet has facilitated increased possibilities for communication and freedom of expression, enabling anonymity, rapid information sharing, and cross-cultural dialogues. At the same time, changes in technologies have also provided new opportunities for State surveillance and intervention into individuals' private lives.[48] Thus the role of each actor and the relations among them should be analyzed under the legal framework.

[48] UN. *A/HRC/23/40*. 2013, para. 11.

1.1) IT Corporation (Legal Person, Service Providers - SPs)

Either IT Corporations or Service Providers are applied to the State's regulation while State Authorities are obliged to respect and fulfill individuals' rights. State Agencies are under the obligation to protect individuals' rights from the abusive actions done by non-State actors including corporation entities.[49] The private sector bears equal responsibility for respecting human rights, particularly given the key role it plays in designing, developing and disseminating technologies; enabling and providing communications; and - where required - cooperating with State surveillance activities. Nevertheless, the scope of the present duties is limited to the obligations of the State[50] which has limited jurisdiction due to the nature of Modern State.

1.2) State

States seeking access to both communications content and communications metadata is rising dramatically, without adequate scrutiny.[51] When accessed and analyzed, communications metadata may create a profile of an individual's life, including medical conditions, political and religious viewpoints, associations, interactions and interests, disclosing as much detail as, or even greater details than would be discernible from the content of communications.[52] Despite the vast potential for intrusion into an individual's life and the chilling effect on political and other associations, legislative and policy instruments often afford communications metadata a lower level of protection and do not place sufficient

[49] La Rue, *Frank. Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression*, 2011.

[50] International Coalition of Civil Organizations on Internet Freedom. *International Principles on the Application of Human Rights to Communications Surveillance*. 2014, Preamble.

[51] For example, in the United Kingdom alone, there are now approximately 500,000 requests for communications metadata every year, currently under a self-authorising regime for law enforcement agencies who are able to authorise their own requests for access to information held by service providers. Meanwhile, data provided by Google's Transparency reports shows that requests for user data from the U.S. alone rose from 8888 in 2010 to 12,271 in 2011. In Korea, there were about 6 million subscriber/poster information requests every year and about 30 million requests for other forms of communications metadata every year in 2011-2012, almost of all of which were granted and executed. 2012 data available at http://www.kcc.go.kr/user.do?mode=view&page=A02060400&dc=K02060400&boardId=1030&cp=1&boardSeq=35586.

[52] Escudero-Pascual, Alberto and Hosein, Ian. "Questioning Lawful Access to Traffic Data." *Communications of the ACM*, vol. 47, no. 3, 2004, pp. 77-82.

restrictions on how they can be subsequently used by agencies, including how they are data-mined, shared, and retained.[53]

In evaluating the invasiveness of State communications surveillance, it is necessary to consider both the potential of the surveillance to reveal protected information, as well as the purpose for which the information is sought by the State.

1.3) Individual (Natural Person)

Communications surveillance that will likely lead to the revelation of protected information that may place a person at risk of investigation, discrimination or violation of human rights will constitute a serious infringement on an individual's right to privacy, and will also undermine the enjoyment of other fundamental rights, including the right to free expression, association, and political participation. This is because these rights require people to be able to communicate free from the chilling effect of government surveillance.[54] A determination of both the character and potential uses of the information sought will thus be necessary in each specific case.

Any measure must not be applied in a manner which discriminates on the basis of race, color, sex, language, religion, political or other opinion, national or social origin, property, birth or other status.[55]

1.4) Relations between relevant actors

The Research will analyze how to design the regime and governance for solving the problems which base on 7 potential relations between State, Corporation and Individual;

a) IT Corporation claim to Individual

The claims from Corporation to Individual are on the basis of Contractual relations; Terms and Conditions, Compulsory Consent. (Unfair contract – instant contract)

[53] International Coalition of Civil Organizations on Internet Freedom. *International Principles on the Application of Human Rights to Communications Surveillance*. 2014, Preamble.

[54] Ibid.

[55] Ibid, Legitimate Aim.

b) Individual claim to IT Corporation

The claims from Individual to Corporate are on the basis of Customer Rights; Consumer Protection on Personal Data, Client Confidential, ISO 27001, Right to Technology, Private property, Right to integrity and privacy on communication and personal domain.

c) State claim to IT Corporation

The claims from State to Corporation are on the basis of Administrative Law on Public Service; Regulation and Governance on Internet Service Providers, Cyber Crime Control, E-Commerce Regulations, Standard, and Right to Regulate both Domestic and International level.

d) IT Corporation claim to State

The claims from Corporation to State are on the basis of Private freedom to conduct business activities in Liberal Legal State; Freedom of access, movement, interconnects, exchange, distribute, provide services in market. States Non-Arbitrary intervene to Market either on Domestic and International level.

e) State claim to Individual

The claims from State to Individual are on the basis of Legitimacy Power to Govern; Surveillance, Command and Control on the activities, communications and movements of criminal or terrorist in the name of "Security". State employs power by creating a reason "Society must be defended" to justify the act of Government.

f) Individual claim to State

The claims from Individual to State are on the basis of Personal Human Rights; Right to Personal Data Protection, Right to Information, Right to enjoy full utility of Technology, Right to basic public service (Communication Infrastructure), and Consumers' Rights.

g) State co-operation with State

The Co-operations between State to State are on the basis of International Security and Criminal Cooperation Agreement; Organized Crime, International Anti-Terrorism, Bi-lateral Secret Intelligence Agreement, Diplomatic Protection. Besides there are some International Economic Agreements or Treaties about E-Trading or E-Services or Trans-border data flows.

The Research will Investigate the positivism evidences of the relations between those actors especially STATE-STATE, STATE-CORPORATION. This Thesis will undertake either on the formal policy and informal practice.

2) Legal issues arising from the distinctive characteristic of Cyberspace

Since the end of the Cold War, the terms 'cyberspace' and 'globalization' have been prevailed. Internet triggered a new world order of interconnection and decentralization. In terms of impacts of Cyberspace on Legal atmosphere, the 'results of technology-ignorance in the legal community can be devastating, with cases being decided and lost based on unsound arguments from the parties and/or unsound reasoning by the courts'.[56] Hence, Judge Frank Easterbrook provocatively stated that studying cyber law as a separate field of study would be no different from studying the 'law of the horse' in the nineteenth century[57]. His statement reflects explicitly that it requires only 'general rules' without the need to invent a new legal regime, without desiring anything called 'cyber law' specifically.

Notwithstanding, the discussions of rights and freedom in Cyberspace are concerned about threats to fundamental rights posed by private power, and not just state as Paul S. Berman mentioned that 'the role of entrenched economic power, the importance of embedded

[56] Svantesson, D J B. "The Times They Are a-Changin'(Every Six Months)--the Challenges of Regulating Developing Technologies." *Forum on public policy: A journal of the Oxford Round Table*, Forum on Public Policy, 2008.

[57] Easterbrook, Frank H. "Cyberspace and the Law of the Horse." *U. Chi. Legal F.*, 1996, p. 207.

legal regimes, the ubiquitous role of the state, the significance of non-state communities to the construction of norms'[58] imply the needs of sensitivity on cyberspace regulation.

In contrast with "Unexceptionalist", it is obvious that online medium creates a new problem depends in large part on what some lawyers have questioned, cyberspace 'exceptionalists' argued that the medium itself created radically new problems requiring new analytical work to be done[59]. Accordingly, new technologies that alter the culture are precisely the sorts of changes that tend to result in *shifts* to well-settled legal principles[60].

From the arguments will be described below, cyberspace impacts take a structural approach, emphasizing large-scale cultural, economic, political and legal forces that are more fundamental than just how particular legal rules will apply to particular sorts of interactions[61] but how would legal community manage this space through transformation.

In addition, there are large numbers of case studies to support the idea that changes and challenges may cause obstacles to Cyberspace Regulating. Since the third wave revolution have been continuing, Nation State and International Community have been concerned whether the universal principle of Law could apply to Cyberspace properly[62], or not. Specifically, it creates impacts on 5 categories of legal atmosphere; which are as follows;

a) Person and Legal Entities

There is mutability on the principle of Person in "Netizen Society" [63] because individuals in Cyberspace can change or undercover their identities to 'create multiple electronic identities which are linked only by their common progenitor, that link, invisible in

[58] Berman, Paul Schiff. "Law and Society Approaches to Cyberspace." *Law and Society Approaches to Cyberspace*, Ashgate Publishing, Aldershot, 2007, p. xiii.

[59] Ibid., p.xiv.

[60] Ibid.

[61] Ibid, p. xv.

[62] Lloyd, Ian J. *Information Technology Law.* Oxford University Press, UK, 2011, p. 182.

[63] Cavanagh, Allison. *Sociology in the Age of the Internet.* Tata McGraw-Hill Education, Delhi, 2010.

the virtual world, is of great significance.'[64] In this respect, state has the duty to assure the traceability of person in case of crime or terrorism.

An effort to create and to enlarge E-Government comes from the anonymity issue, while anonymity[65] is an individual rights, it is a formidable difficulty to manage population.[66] Thus, surveillance-oriented societies have been constructed on the excuse of freedom protection.

In the first case, A Homeland Security Department spokesman was held on charges of sexually preying on 14-year-old girl, which is really an undercover detective, whom he hunting through explicit online conversations related to sexually graphic conversations. He thought the counterpart was a teenage girl, who actually was undercover detective.[67] Hence the pedophile crime case confirms the need of state surveillance on Internet by using undercover agent.

In contrast, the webmaster of Norporchor-USA was found guilty of criminal charges by Thai Computer Crime Act. As well as Joe Gordon,[68]who was famous from his translation on notorious book "The King Never Smile", was distributed as anonymous via above website. These controversial cases bring suspicion on right to be forgotten, to be unknown or unidentifiable or annonymised. Anonymity is required especially during a time of political conflict when confidentiality is important for active citizen who want to express their opinion out loud but still can keep their privacy.

Moreover, the right to privacy and right to know and correct personal data should be corroborated as well.

---

[64] Basu, Subhajit and Jones, Richard. "Regulating Cyberstalking." *Journal of Information Law & Technology*, vol. 22, 2007, p. 10.

[65] Anonymity is one of the characters relating right to data privacy and personal data protection. The legal implication of Anonymity will be further described in chapter 2 and 4.

[66] Ogura, Toshimaru. "Electronic Government and Surveillance-Oriented Society." *Theorizing surveillance*, Willan Publishing, London, 2006, pp. 270-295.

[67] "DHS Press Secretary Arrested on Child Seduction Charges", *Associated Press*, 2006, www.foxnews.com/story/2006/04/05/dhs-press-secretary-arrested-on-child-seduction-charges.html. 2 May 2014.

[68]Ashayagachat, Achara. "Inmates blame UDD for Ah Kong's death", *bangkokpost*, 2012, www.bangkokpost.com/lite/topstories/292704/inmates-blame-udd-for-ah-kong-death. Accessed 21 Nov. 2012.

b) Relationship in Networks: Public or Private sphere?

The relationship in cyberspace seems to be vague when we have to apply law to a virtual line for communication activities whether it is public or private "Sphere".

Cyberspace is suitable for proving the "Governmentality" theory of Michel Foucault which reveals the Modern State's technology of power that penetrates to the self of individual through Public space and activity.[69] Since the state eager to shift the line to the former private space combining with the enlargement of public communication spaces, Legal Society has a duty to answer the problems about whether Social Media is a Public Sphere or truly Private Space.

In an Ashley Cole's astonishing Twitter attack on the Football Association (FA) case, even he then deleted the message and issued a statement apologizing for his outburst but still was fined by FA.[70] It has shown the changing landscape of law and also its consequence, which narrows the gap between private and public life. Furthermore, it should provide choices for constructing legal frameworks to protect and promote the rights of Social Media members[71] in account to handle it to suppress harms and support responsibly freedom of expression. It affirms that power of surveillance is widespread and decentralized to other organization like the FA.

From above cases show the competence of cyberspace as a communication tools which can penetrate to private sphere both by the first party who spread the content and the reflects react by any others in era of digitalization. Consequently, new boundaries should be drawn to make a certainty scope between the public sphere, in which person can express their intimacy with responsibility to others, and private sphere, full capable to speak and be protected on the basis of right to privacy.

---

[69] Loader, Brian. *The Governance of Cyberspace: Politics, Technology and Global Restructuring.* Psychology Press, Brighton, 1997, p. 12-14.

[70] "Ashley Cole Risks England Career with Twitter Rant at FA", *The Sun*, 2012, www.thesun.co.uk/archives/football/968697/cole-twitter-shock/. Accessed 2 May 2014.

[71] Barwick, Hamish. "Social Networking Websites May Face Government Regulation", *Computerworld*, www.computerworld.com.au/article/418730/social_networking_websites_may_face_government_regulation/. Accessed 2 May 2014.

c) Jurisdiction for Legal enforcement

The most predominance shift is Jurisdiction on "place" because activities in cyberspace, which are cross-border or relevant to more than one state[72], could produce many conflicts of laws situations.

In the past, 'well-settled' principles of legal jurisdiction saw jurisdiction as rooted almost exclusively in the territorial power of the sovereign[73] but right now the absolute principle so-called 'effects doctrine' has been difficult to apply to online interaction because material on a website potentially creates effects anywhere[74] regardless state territory.

In this case, online Gamble falls into technically illegal in most of the United States, however the prosecution and conviction of individual players is very difficult because they are gambling from home. Interestingly, most online casinos are located in other countries.[75] There are issues of jurisdiction and sovereignty, which make gambling laws even more paralyzed. These situations require a state measures to combat against organized crime as human trafficking in Internet.

From the changing nature of the countless trans-border transactions, International Community should be considering non-state-based constitutionalism more and recognizing the importance of autonomous social systems apparatus as another one law-making force among many[76]to balance freedom and order in online world.

d) Communication Channels

Internet could provide an opportunity to people but the entitlement to "Medium" is crucial. Additionally, opportunity to compete in a high-technology

[72] Fuchs, Christian. *Internet and Society: Social Theory in the Information Age.* Routledge, London, 2007, pp. 119-120.

[73] Berman, Paul Schiff. "Law and Society Approaches to Cyberspace." *Law and Society Approaches to Cyberspace*, Ashgate Publishing, Aldershot, 2007, p. xvi.

[74] Ibid., p.xv.

[75] "How Online Gambling Works", *HowStuffWorks*, 2005, http://entertainment.howstuffworks.com/online-gambling.htm. Accessed 2 May 2014.

[76] Teubner, Gunther. "Societal Constitutionalism: Alternatives to State-Centred Constitutional Theory?", in Christian Joerges, Inger-Johanne Sand and Gunther Teubner (eds), *International Studies in the Theory of Private Law Transnational Governance and Constitutionalism*, Oxford: Hart Publishing, UK, 2004, pp. 3–28.

communication is an anti-monopoly key[77] on every perspective. Though Internet penetration and digitalization ratio diffuse among different society, they depend on socio-economic conditions: computer skills, literacy, income and regulatory environments[78], which could affect their absorptive capacity.

In Web browser case, EC believes that the company has abused its monopoly by deeply linking Internet Explorer with its operating system,[79] which prevents competitors to access this market. Relatively, in Google case, they offers services and applications to attract Internet traffic to their website/brand so they could collect tons of information and generate revenues from the sponsors by processing users' personal data.[80] These cases imply the power over market and data processing of private corporations.

However, it is impossible to eliminate or block the traffic because the techniques of intermediary controls are generally less effective in small nations[81], and they have a larger array of intermediaries to trace back in super power nations.

e) Property Regimes

With regards to possession of "Technology", the commercialization in products and services into commodities[82] or public goods is the point of cyberspace. Because of right to information, Internet Society should provide individuals the means to participate in the production and distribution of culture.[83] Indeed, freedom of expression sits in an uneasy

[77] Fuchs, Christian. *Internet and Society: Social Theory in the Information Age.* Routledge, London, 2007, pp. 209-212.

[78] Klang, Mathias and Murray, Andrew. "Internet Service Providers and Liability." *Human Rights in the Digital Age.* Psychology Press, Brighton, 2005, p. 88.

[79] Saturday, Aidan M and others. "Europe Revives Claims of Microsoft Web Browser Monopoly", *AppleInsider*, //appleinsider.com/articles/09/01/17/europe_revives_claims_of_microsoft_web_browser_monopoly. Accessed 21 Nov. 2012.

[80] Lopez-Tarruella, Aurelio. "Introduction: Google Pushing the Boundaries of Law." *Google and the Law*, Springer, New York, 2012, pp. 4-5.

[81] Goldsmith, Jack and Wu, Tim. *Who Controls the Internet?: Illusions of a Borderless World.* Oxford University Press, UK, 2006, pp. 81-82.

[82] Fuchs, Christian. *Internet and Society: Social Theory in the Information Age.* Routledge, London, 2007, p. 139.

[83] Balkin, Jack M. "Digital Speech and Democratic Culture: A Theory of Freedom of Expression for the Information Society." *NYUL rev.*, vol. 79, 2004, pp. 1–58.

relationship with copyright law because it effectively censors speech in the name of providing incentives to create[84]. Moreover, it could give a power to the copyrights owner to pursue their goods by detecting devices.

In Creative-Commons case, the Commons will release a software application this fall that permits a work to be copied under certain conditions.[85] As Ginsburg argues that we need to strengthen authorial control over digital distribution of creative works to provide the incentives necessary to give the public access to more material (Unexceptionist)[86]. In contrast, 'untamed anarchic digital sharing' through peer-to-peer networks is a superior distribution mechanism so we ought to encourage the new form rather than use strongly author - based copyright protection, (Exceptionist).[87] It implies that the first owner should own capacity to follow their works but should not have an absolute individual right as tradition Intellectual Property Law stance.

3) Challenges, cyberspace brings to legal atmosphere

The Internet has been a vital communication Technology which is providing facilities to many aspects of human life[88]. Accordingly, there are some features of the challenges that could be described by 4 main perspectives; which are political rights perspectives, economic rights perspectives, social rights perspectives and cultural rights perspectives.

---

[84] Berman, Paul Schiff. "Law and Society Approaches to Cyberspace." *Law and Society Approaches to Cyberspace*, Ashgate Publishing, Aldershot, 2007, p. xvii.

[85] Harrison, Ann. "Creative Commons redefines intellectual property use", *Network World Peer-to-Peer Newsletter,* 29 May 2002, www.networkworld.com/newsletters/fileshare/2002/01366104.html. Accessed on 21 Nov. 2012.

[86] Ginsburg, Jane C. "Copyright and Control over New Technologies of Dissemination." *Columbia Law Review*, 2001, pp. 1613-1647.

[87] Litman, Jessica. "Sharing and Stealing." *Hastings Communications and Entertainment Law Journal*, vol. 27, 2003, pp. 1–50.

[88] Cavanagh, Allison. *Sociology in the Age of the Internet.* Tata McGraw-Hill Education, Delhi, 2010, p. 2.

a) Political Rights Perspective:

The main argument on this respect is the clash between Authority and Power VS Liberation and Resistance[89]. Like China who dominates the "Internet Enemies" list by every measure[90] but In Arab countries, many activists who played crucial roles in the Arab Spring used social networking which have broken the psychological barrier of fear by helping many to connect and share information.[91]

Information Superhighway impacts the world by network accessing, 24-hour medium, two-way communications with multiple-individual participation and non-geographical obstacles.[92] It triggers 'digital democracy' by providing information and full participation, however, the obstacles against internet accession could engender 'information aristocracy'[93] which the minority of wealthy private providers and state could monopolize the Political Arena.

Information and comprehension of public affairs are vital if autonomous and free choices are to be made by individual electors.[94] Hence, the state and privates are able to govern internet by the capacities of: designed codes and applications, guardians of it and develop and implement the decisional principles,[95] in term of facilitating Internet communication.

---

[89] Terranova, Tiziana. *Network Culture: Politics for the Information Age.* Pluto Press, 2004, p. 135.

[90] Abate, Tom. "Net censorship, propaganda on the rise", *GlobalPost*, 30 May 2010, http://www.globalpost.com/dispatch/technology/090407/net-censorship-propaganda-the-rise. Accessed on 21 Nov 2012.

[91] Kassim, Saleem. "Twitter Revolution: How the Arab Spring Was Helped By Social Media", 4 July 2012, https://mic.com/articles/10642/twitter-revolution-how-the-arab-spring-was-helped-by-social-media. Accessed 2 May 2014.

[92] Cathy, Bryan. and James, Tatam. "Political Participation and the Internet." *Liberating Cyberspace: Civil Liberties, Human Rights & the Internet.* Pluto Press, London, 1999, p. 162.

[93] Carter, Dave. "Economic Regeneration and the Information Economy." *The governance of cyberspace: Politics, technology and global restructuring*, vol. 136, 1997, p. 137.

[94] Walker, Clive. "Cyber-Constitutionalism and Digital Democracy." *The Internet, Law and Society,* Longman, London, 2000, p. 127.

[95] Bygrave, Lee A and Michaelsen, Terje. *Governors of Internet.* Oxford University Press, UK, 2009, pp. 93-94.

b) Economic Rights Perspective:

In this sense, it could be described by the confrontation of Monopoly and Dividend VS. Allocation and Accession[96], as Business Model of Google challenges the various Laws, without strictly checked and balanced, in economic fields such as competition, consumer protection and Intellectual Property Law.[97] It deters other marketers to utilize cheap promotional device[98] which SMEs would establish a global presence.

Consequently, Digital Divide or Digital Inequality have a roots from low-quality equipment, incompetence command of use, lack of social support networks, less experience, impotence ICTs using.[99] The incompetence could be diminished by the progressive realization measure supported by State as the right-based approach human development projects. In a Finland case, government has recognized 1Mb Broadband internet access as a legal right[100].

Net Neutrality should be protected by fair competition between service providers[101], however, in some cases ISPs who have power over market could collect a lot of data[102] and imply that direct marketing and mass electronic surveillance have came from those data.

---

[96] Cavanagh, Allison. *Sociology in the Age of the Internet.* Tata McGraw-Hill Education, Delhi, 2010, p. 64.

[97] Lopez-Tarruella, Aurelio. "Introduction: Google Pushing the Boundaries of Law." *Google and the Law*, Springer, New York, 2012, pp. 1-8.

[98] Lloyd, Ian J. *Legal Aspects of the Information Society*. Lexis Law Pub, London, 2000. p. 230.

[99] Klang, Mathias and Murray, Andrew. "Internet Service Providers and Liability", *Human Rights in the Digital Age.* Psychology Press, Brighton, 2005, p. 90.

[100] Reisinger, Don. "Finland Makes 1Mb Broadband Access a Legal Right", *CNET,* 14 Oct. 2009, www.cnet.com/uk/news/finland-makes-1mb-broadband-access-a-legal-right/. Accessed 20 Nov. 2012.

[101] Mahabadi, Ladan. "Price of Monopoly and Democracy, Internet and Democracy Blog", *Price of Monopoly and Democracy*, 19 Aug. 2008, https://blogs.law.harvard.edu/idblog/2008/08/19/price-of-monopoly-and-democracy/. Accessed on 20 Nov. 2012.

[102] Solum, Lawrence B. "Models of Internet governance", *Internet Governance: Infrastructure and Institutions,* Lee A. Bygrave and Jon Bing (eds), Oxford University Press, UK, 2009, pp. 88-89.

c) Social Rights Perspective:

The challenge internet creates to society are the strike between Class fragmented and Exclusion VS Networks and Inclusion[103]. Cyber social life makes it difficult to govern such communities or State should let them exercising their own forms of governance, jurisdiction and sanction[104]. As shown in notorious LambdaMOO, 'cyber-rape' in an early online community, as the group efforts to build fledgling governance structure to address online misbehaviour[105].

However, In outrage prime example: "Social Sanction," a Facebook group recently deleted because it was deemed hate speech, posted phone numbers and addresses of Red Shirt protesters and urged its followers to physically attack one of them[106]. So both state and private have a duty to observe and suppress such hate speech websites. But State should leave social entrepreneur website: they encourage new forms of connection, contribution and participation[107], alone.

d) Cultural Rights Perspective:

Cyberspace creates 'virtual communities' which could have some debate in various cases among Conservative and Domination VS Diversity and Pluralism[108].

Internet could be used by potentially marginalized communities and the increasingly lucrative sphere of multiplayer simulated worlds. On the other hand, it could

[103] Cavanagh, Allison. *Sociology in the Age of the Internet.* Tata McGraw-Hill Education, Delhi, 2010, pp. 112-115.

[104] Berman, Paul Schiff. "Law and Society Approaches to Cyberspace." *Law and Society Approaches to Cyberspace*, Ashgate Publishing, Aldershot, 2007, p. xxiii.

[105] Mnookin, Jennifer L. "Virtual (Ly) Law: The Emergence of Law in Lambdamoo: Mnookin." *Journal of Computer Mediated Communication*, vol. 2, no. 1, 1996, pp. 645–701.

[106] "Thailand's Social Media Battleground", *New Mandala*, 26 Mar 2015, www.newmandala.org/thailands-social-media-battleground/. Accessed 2 May 2015.

[107] "Internet Power Is the New Force for Social Impact", *Social Enterprise,* 7 Dec 2011, www.socialenterpriselive.com/section/comment/community/20111207/internet-power-the-new-force-social-impact. Accessed 20 Nov 2012.

[108] Fuchs, Christian. *Internet and Society: Social Theory in the Information Age.* Routledge, London, 2007, pp. 333-334.

empower of illiberal extremists to find transnational community[109]. This reflects and transforms the social life that migrates there: problem of racism and xenophobia was growing over the Internet[110]. It supports individuals to insulate themselves from competing views will make it more difficult for societies to inculcate shared understandings of reality and ignores the significance of multiculturalism[111]. Somehow, it legitimizes the state surveillance on Cyberspace.

The ability of Internet on increasing racial anonymity, interracial social and destabilize the significance of racial categories[112] should not be deterred by Authority, especially minorities.

These challenges in turn led to the further question of "proper regulation regime". It must be inquired capability of Nation State to apply domestic law to trans-border activities in various perspectives[113]. On the Regional Level, the Assembly of South-East Asian Nations (ASEAN) and European Union (EU) could only provide guidelines[114] but could not oblige member states to implement and enforce it effectively. On International Level, United Nations could not pursue state into specific treaty for harmonizing Cyberspace Regulation Policies as it will be described next.

1.3. Human Rights and the Discourse of Security

This section draws a framework of States' surveillance of communications for the exercises of the human rights to privacy, personal data protection. While considering the impact of significant technological advances in communications, State employ on behalf of state and international security. The research underlines the urgent need to further study new

[109] Berman, Paul Schiff. "Law and Society Approaches to Cyberspace." *Law and Society Approaches to Cyberspace*, Ashgate Publishing, Aldershot, 2007, p. xxii.

[110] Akdeniz, Yaman. "Governing Racist Content on the Internet: National and International Responses." *UNBLJ*, vol. 56, 2007, p. 103.

[111] Chander, Anupam and Sunstein, Cass. "Whose Republic?." *JSTOR*, 2002, pp. 1479–1500.

[112] Kang, Jerry. "Cyber-Race." *Harvard Law Review*, 2000, pp. 1130-1208.

[113] Goldsmith, Jack and Wu, Tim. *Who Controls the Internet?: Illusions of a Borderless World.* Oxford University Press, UK, 2006, p. 179-184.

[114] Lloyd, Ian J. *Information Technology Law*. Oxford University Press, UK, 2011, pp. 443-4.

modalities of surveillance and to revise International Regime and National laws regulating these practices in line with human rights standards.

1) Discourse of Human Rights

As technologies that facilitate State surveillance of communications advance, States are failing to ensure that laws and regulations related to communications surveillance adhere to international human rights and adequately protect the rights to privacy and freedom of expression. This research attempts to explain how international human rights law applies in the current digital environment, particularly in light of the increase in and changes to communications surveillance technologies and techniques.[115] Personal Data Protection can provide civil society groups, industry, States and others with a framework to evaluate whether current or proposed surveillance laws and practices are consistent with human rights.

These principles are the outcome of a global consultation with civil society groups, industry and international experts in communications surveillance law, policy and technology.

a) Right to Privacy

Privacy is a fundamental human right, and is central to the maintenance of democratic societies. It is essential to human dignity and it reinforces other rights, such as freedom of expression and information, and freedom of association, and is recognized under international human rights law.[116] Activities that restrict the right to privacy, including

[115] International Coalition of Civil Organizations on Internet Freedom. *International Principles on the Application of Human Rights to Communications Surveillance*. 2014, Preamble.

[116] Universal Declaration of Human Rights Article 12, United Nations Convention on Migrant Workers Article 14, UN Convention of the Protection of the Child Article 16, International Covenant on Civil and Political Rights Article 17; regional conventions including Article 10 of the African Charter on the Rights and Welfare of the Child, Article 11 of the American Convention on Human Rights, Article 4 of the African Union Principles on Freedom of Expression, Article 5 of the American Declaration of the Rights and Duties of Man, Article 21 of the Arab Charter on Human Rights, and Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms; Johannesburg Principles on National Security, Free Expression and Access to Information, Camden Principles on Freedom of Expression and Equality.

communications surveillance, can only be justified when they are prescribed by law, they are necessary to achieve a legitimate aim, and are proportionate to the aim pursued.[117]

At both the international and regional levels, privacy is also unequivocally recognized as a fundamental human right. The right to privacy is enshrined by the Universal Declaration of Human Rights (art. 12), the International Covenant on Civil and Political Rights (ICCPR, art. 17), the Convention on the Rights of the Child (art. 16), and the International Convention on the Protection of All Migrant Workers and Members of Their Families (art. 14). At the regional level, the right to privacy is protected by the European Convention on Human Rights (art. 8) and the American Convention on Human Rights (art. 11)[118] but there is no provision on right to privacy in the African Charter on Human and Peoples' Rights, while Asia has no regional Human Rights instrument.

b) Right to Personal Data Protection

Before public adoption of the Internet, well-established legal principles and logistical burdens inherent in monitoring communications created limits to State communications surveillance. In recent decades, those logistical barriers to surveillance have decreased and the application of legal principles in new technological contexts has become unclear. The explosion of digital communications content and information about communications, or "communications metadata" -- information about an individual's communications or use of electronic devices -- the falling cost of storing and mining large sets of data, and the provision of personal content through third party service providers make State surveillance possible at an unprecedented scale.[119] Meanwhile, conceptualizations of

[117] Universal Declaration of Human Rights Article 29; *General Comment No. 27*, Adopted by The Human Rights Committee Under Article 40, Para. 4, Of The International Covenant On Civil And Political Rights, *CCPR/C/21/Rev.1/Add.9*, 2 Nov. 1999; see also Scheinin, Martin. "Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism.", *A/HRC/17/34*, 2009.

[118] UN. *A/HRC/23/40*. 2013, para. 20.

[119] Communications metadata may include information about our identities (subscriber information, device information), interactions (origins and destinations of communications, especially those showing websites visited, books and other materials read, people interacted with, friends, family, acquaintances, searches conducted, resources used), and location (places and times, proximities to others); in sum, metadata provides a window into nearly every action in modern life, our mental states, interests, intentions, and our innermost thoughts.

existing human rights law have not kept up with the modern and changing communications surveillance capabilities of the State, the ability of the State to combine and organize information gained from different surveillance techniques, or the increased sensitivity of the information available to be accessed.[120]

State should ascertain whether the information likely to be procured falls within the ambit of "protected information" before seeking it, and should submit to the scrutiny of the judiciary or other democratic oversight mechanism. In considering whether information obtained through communications surveillance rises to the level of "protected information", the form as well as the scope and duration of the surveillance are relevant factors.[121] Because pervasive or systematic monitoring has the capacity to reveal private information far in excess of its constituent parts, it can elevate surveillance of non-protected information to a level of invasiveness that demands strong protection.[122]

c) Freedom of Expression

Innovations in technology have increased the possibilities for communication and protections of free expression and opinion, enabling anonymity, rapid information-sharing and cross-cultural dialogues. Technological changes have concurrently increased opportunities for State surveillance and interventions into individuals' private

[120] International Coalition of Civil Organizations on Internet Freedom. *International Principles on the Application of Human Rights to Communications Surveillance*. 2014, Preamble.

[121] Ibid.

[122] "Prolonged surveillance reveals types of information not revealed by short-term surveillance, such as what a person does repeatedly, what he does not do, and what he does ensemble. These types of information can each reveal more about a person than does any individual trip viewed in isolation. Repeated visits to a church, a gym, a bar, or a bookie tell a story not told by any single visit, as does one's not visiting any of these places over the course of a month. The sequence of a person's movements can reveal still more; a single trip to a gynecologist's office tells little about a woman, but that trip followed a few weeks later by a visit to a baby supply store tells a different story.* A person who knows all of another's travels can deduce whether he is a weekly church goer, a heavy drinker, a regular at the gym, an unfaithful husband, an outpatient receiving medical treatment, an associate of particular individuals or political groups – and not just one such fact about a person, but all such facts." U.S. v. Maynard, 615 F.3d 544 (U.S., D.C. Circ., C.A.)p. 562; U.S. v. Jones, 565 U.S. __, (2012), Alito, Justice, concurring. "Moreover, public information can fall within the scope of private life where it is systematically collected and stored in files held by the authorities. That is all the truer where such information concerns a person's distant past…In the Court's opinion, such information, when systematically collected and stored in a file held by agents of the State, falls within the scope of 'private life' for the purposes of Article 8(1) of the Convention." ECHR. *C-28341/95 Rotaru v. Romania*, 2000, para.43-44.

communications.[123] The research concerns the unprecedented impact of the Internet on expanding the possibilities of individuals to exercise their right to freedom of opinion and expression.

The right to freedom of opinion and expression is guaranteed under articles 19 of the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights, which affirm that everyone has the right to hold opinions without interference, and to seek, receive and impart information and ideas of all kinds through any media and regardless of frontiers. At the regional level, the right is protected by the African Charter on Human and Peoples' Rights (art. 9), the American Convention on Human Rights (art. 13); and the Convention for the Protection of Human Rights and Fundamental Freedoms (art. 10).[124]

d) Right to due process in Justice Procedure

Due process requires that States respect and guarantee individuals' human rights by ensuring that lawful procedures that govern any interference with human rights are properly enumerated in law, consistently practice, and available to the general public. Specifically, in the determination on his or her human rights, everyone is entitled to a fair and public hearing within a reasonable time by an independent, competent and impartial tribunal established by law,[125] except in cases of emergency when there is imminent risk of danger to human life. In such instances, retroactive authorization must be sought within a reasonably practicable time period. Mere risk of flight or destruction of evidence shall never be considered as sufficient to justify retroactive authorization.

State seeks access to or use of protected information obtained through communications surveillance in the context of a criminal investigation, it must establish to the competent, independent, and impartial judicial authority that:[126]

[123] UN. *A/HRC/23/40*. 2013. para. 2.

[124] Ibid, para. 19.

[125] The term "due process" can be used interchangeably with "procedural fairness" and "natural justice", and is well articulated in the European Convention for Human Rights Article 6(1) and Article 8 of the American Convention on Human Rights.

[126] International Coalition of Civil Organizations on Internet Freedom. *International Principles on the Application of Human Rights to Communications Surveillance*. 2014, Preamble.

1) there is a high degree of probability that a serious crime has been or will be committed;

2) evidence of such a crime would be obtained by accessing the protected information sought;

3) other available less invasive investigative techniques have been exhausted;

4) information accessed will be confined to that reasonably relevant to the crime alleged and any excess information collected will be promptly destroyed or returned; and

5) information is accessed only by the specified authority and used for the purpose for which authorization was given.

In order to determine related the legitimacy of authorized communications surveillance, the judicial decision must be made by a competent judicial authority that is impartial and independent. The authority must be:[127]

1) separate from the authorities conducting communications surveillance;

2) conversant in issues related to and competent to make judicial decisions about the legality of communications surveillance, the technologies used and human rights; and

3) have adequate resources in exercising the functions assigned to them.

2) Discourse of Security

The dynamic nature of technology has not only changed how surveillance can be carried out, but also "what" can be monitored**.** In enabling the creation of various opportunities for communication and information-sharing, the Internet has also facilitated the development of large amounts of transactional data by and about individuals. This information, known as communications data or metadata, includes personal information on individuals, their location and online activities, and logs and related information about the e-mails and messages they send or receive. Communications data are storable, accessible and

[127] International Coalition of Civil Organizations on Internet Freedom. *International Principles on the Application of Human Rights to Communications Surveillance*. 2014, Preamble.

searchable, and their disclosure to and use by State authorities are largely unregulated. Analysis of this data can be both highly revelatory and invasive, particularly when data is combined and aggregated. As such, States are increasingly drawing on communications data to support law enforcement or national security investigations. States are also compelling the preservation and retention of communication data to enable them to conduct historical surveillance.[128]

The Sense of "Security" of Western Civilization, especially in the Pact Britannica-Americana, is on the basis of "Preparing for the worst condition" so it constructs the perception of "Collection" or accumulation of capital, information is included. The perception of "Collectivism" is to accumulate everything as the supply ready to be used in crisis.[129] This perception is the foundation logic of Capitalism Society (Neo-Liberalism) which is progressed by Modern State transformation.[130] As well as the way government rule population on behalf of State Security, State Authority use information about population to exercise the power of the ruler over people.[131] The more State collect information the more secure State feel, hence the Superpower Nation enlargement of territory by pushing Globalization via IT revolution is the strategy to extend State power to watch Netizen globally. For understanding security on Cyberspace, the research will analyze the relations between Human Rights and Security in 3 levels; International Community, State and Individual. Further the specific area of information security will be analyzed too.

a) International Community Security

As Internet penetrate through physical boundary, the old school concept of Modern State sovereignty on territory could not smoothly apply to Cyberspace's activity such as International Data Processing and Espionage. Thus International Community must initiate the International Regime or Global Governance to regulate such trans-national activities on Internet.

---

[128] UN, *A/HRC/23/40*. 2013, para.15.

[129] Marx, Karl. *Capital: A Critique of Political Economy*. International, New York, 1867.

[130] Polanyi, Karl. *The Great Transformationthe Political and Economic Origins of Our Time.* Farrar&Rinehart, New York, 1944.

[131] Foucault, Michel. *Security, Territory, Population (Michel Foucault: Lectures at the College De France)*. Burchell, Graham. Trans. Palgrave Macmillan, London, 2007.

The responsible person and any processing service provider must protect the personal data subject to processing with the appropriate technical and organizational measures to ensure, at each time, their integrity, confidentiality and availability. These measures depend on the existing risk, the possible consequences to data subjects, the sensitive nature of the personal data, the state of the art, the context in which the processing is carried out, and where appropriate the obligations contained in the applicable national legislation.[132]

In response to the increased data flows across borders and the fact that majority of communications are stored with foreign third party service providers, a number of States have begun to adopt laws that purport to authorize them to conduct extra-territorial surveillance or to intercept communications in foreign jurisdictions.[133] This raises serious concern with regard to the extra-territorial commission of human rights violations and the inability of individuals to know that they might be subject to foreign surveillance, challenge decisions with respect to foreign surveillance, or seek remedies. In 2012, the European Telecommunications Standards Institute created draft standards for interception of foreign cloud-based services by European Governments.[134] These developments suggest an alarming trend towards the extension of surveillance powers beyond territorial borders, increasing the risk of cooperative agreements between State law enforcement and security agencies to enable the evasion of domestic legal restrictions.

b) State Security

The metadata has been collected, mined and processed as a routine operation. The data Surveillance on targeting suspects were shift to Mass Surveillance on every people without legitimate permission. The abuses of power, State exercise power by compulsory sharing individual data with Corporations, have been disclosed in the case of Super Power State's Security Agency. The arbitrary data sharing among them is illegal. Moreover, the

[132] International Conference of Data Protection and Privacy Commissioners. "International Standards on the Protection of Personal Data and Privacy." *Madrid Resolution*, Vol. 5, 2009.

[133] Republic of South Africa, *General Intelligence Laws Amendment Bill*. 2013, Section 1. c.

[134] ETSITR 101 567 V1.1.1 (2016-01); Cloud/Virtual Services (CLI), http://www.etsi.org/deliver/etsi_tr/101500_101599/101567/01.01.01_60/tr_101567v010101p.pdf. Accessed 2 Oct 2016.

accusation of NSA intercept data, from the middle way of internet traffic, by ISPs is the back-door unlawful spying as well.[135]

State made the "Risk" by creating an image of Horrors; crime, terrorism and chaos, which may threats to society. Then state arbitrary embedded a Panopticon/Governmentality[136] to watch people in the name of "Security". The cooperator is Corporation, who own the technology which adapts to serve consumer in vast majority purpose in everyday-life practice. Corporation, ISPs, share the information of people with State. The Cooperation is constructed on the basis of power of state, law, or on economic benefits which might be the non-transparent pact among them.

Modern surveillance technologies and arrangements that enable States to intrude into an individual's private life threaten to blur the divide between the private and the public spheres. They facilitate invasive and arbitrary monitoring of individuals, who may not be able to even know they have been subjected to such surveillance, let alone challenge it. Technological advancements mean that the State's effectiveness in conducting surveillance is no longer limited by scale or duration. Declining costs of technology and data storage have eradicated financial or practical disincentives to conducting surveillance. As such, the State now has a greater capability to conduct simultaneous, invasive, targeted and broad-scale surveillance than ever before.[137]

The Potentiality of State to panoptical watching on peoples in all space at any time makes the State feels "Secure" to Control and intervene Situations. The ability of Corporate to research on consumers in all space at any time makes the Corporation feels "Secure" to design and launch marketing strategies.

3) Human Security

Internet users can enjoy relative anonymity on the Internet, States and private actors also have access to new technologies to monitor and collect information about individuals'

[135] UN. *A/HRC/23/40*. 2013, para. 59.

[136] Pensador, Ray. "The Surveillance State As Foucault's Panopticon", *Daily Kos*, 11 Sep 2013, www.dailykos.com/story/2013/9/11/1238013/-The-Surveillance-State-As-Foucault-s-Panopticon. Accessed 11 Nov 2013.

[137] UN. *A/HRC/23/40*. 2013, para. 33.

communications and activities. Such technologies have the potential to violate the right to privacy, thereby undermining people's confidence and security on the Internet and impeding the free flow of information and ideas online.[138] The responsible person and those involved at any stage of the processing shall maintain the confidentiality of personal data. This obligation shall remain even after the ending of the relationship with the data subject or, when appropriate, with the responsible person.[139]

Human desires to connect with Info/people. They access/communicate by creating connection channel/device. The issue they would like to engage covers various Technological, Social and Cultural Contents. Internet generates the space for connection then ISPs supply Social Media, Search Engine and Internet Application. Desire to Connect is the demand in Information Market.[140] The Competence to connect to information/people of individual makes them felt "Secure" in different circumstance: from Mega Disaster to minor Everyday-life practice stuffs.[141]

The ownership on mode of production is the basis of Power over Market. The Capital Accumulation is the source of such power. In New Information Market, data is key-bases node of capital since it could turns to valuable information. The collecting, mining and processing of data are the value-added process from internet user information.[142] This phenomenon is necessary for developing E-Commerce Market not only on trading but also marketing and researching. The more people use internet the more data flood in then it enlarges E-Market and create more sophisticate Information Society.[143] The actor who innovate Internet and Construct the data processing is IT Corporation.

These IT Corporations make all Internet services in order to supply those demand from Internet users. However, all markets and society needs certain rules and administrations

---

[138] UN. *A/HRC/17/27*. 2011, para. 22.

[139] International Conference of Data Protection and Privacy Commissioners. "International Standards on the Protection of Personal Data and Privacy." *Madrid Resolution*, vol. 5, 2009, Part V.

[140] UN. *A/HRC/23/40*. 2013, para. 35.

[141] Ibid, para. 34.

[142] International Conference of Data Protection and Privacy Commissioners. "International Standards on the Protection of Personal Data and Privacy." *Madrid Resolution*, vol. 5, 2009, Part VI.

[143] UN, *A/HRC/23/40*. 2013, para. 40.

so the cooperation with Authority is needed. The data sharing between State and Corporate is a form of such cooperative action and policy.[144]

The Strategy of Security Authority to counter the Risk is filling everything into data system. This type of Governmentality is the heritage from Modern State which tries to implant Bio-Power to every single human that they were watching by State.[145] Then watched people will control themselves in order by the feeling of being watched. State also feels secure because they think that tracing back to find the data of everyone is possible since they keep personal data in their data mine.

The most important question is How to balance the "Security" between State, Corporation and Individual. While we are in the phrase of priority on State Security, the Human Security is threatened by the arbitrary sharing of data among state agencies and ISPs. "The security of the State on a state of Human Insecurity"

4) Information security

This Research will offer an overview of what the Personal Data Protection requires in terms of security, and aims to help to decide how to manage the security of the personal data someone hold. This part identifies the main points and information security principle.

The Human Rights Committee analyzed the content of the right to privacy (art. 17) in its General Comment No. 16 (1988), imposes specific obligations relating to the protection of privacy in communications, underlining that "correspondence should be delivered to the addressee without interception and without being opened or otherwise read". "Surveillance, whether electronic or otherwise, interceptions of telephonic, telegraphic and other forms of communication, wire-tapping and recording of conversations, should be prohibited".[146] It also indicates that "the gathering and holding of personal information on computers, data banks and other devices, whether by public authorities or private individuals or bodies, must be

[144] International Conference of Data Protection and Privacy Commissioners. "International Standards on the Protection of Personal Data and Privacy." *Madrid Resolution*, vol. 5, 2009, Part VI.

[145] UN. *A/HRC/23/40*. 2013, para. 39.

[146] UN Human Rights Committee (HRC), *CCPR General Comment No. 16: Article 17 (Right to Privacy), The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation*, 8 April 1988.

regulated by law."[147] The impact of advances in information and communications technologies on the right to privacy was barely understood.[148]

There is the seventh data protection principle.[149] In practice, it means you must have appropriate security to prevent the personal data you hold being accidentally or deliberately compromised. In particular, you will need to:[150]design and organize your security to fit the nature of the personal data you hold and the harm that may result from a security breach; be clear about who in your organization is responsible for ensuring information security; make sure you have the right physical and technical security, backed up by robust policies and procedures and reliable, well-trained staff; and be ready to respond to any breach of security swiftly and effectively.

1.4. Reflection on Data Processing and its Impact on Personal Data Protection

The title of this section is reflected in curiosity. A curiosity is composite of the nature of the data protection while realizing the necessity for its regime. This section will initially critically inquire how the variety economics of the data processing have impacted any legal rights relate to it. More peculiarly, it will demonstrate how the counterpart supporters of political standpoints, namely the Neo-liberal and human rights protector, have described their contesting intellectual evidences toward such characteristics. Secondly, it will review the results as to how the IT Corporation is testing an arena for state regulation in terms of development, freedom and law enforcement. Thirdly, it will indicate why reality manipulates "data of individuals is even more tightly collected", not a monopolized state but a state of monopoly that encourages a fragmented, multi-layered/stakeholder regime of data protection. Finally, it will manifest upon the possible prospects such a policy will accomplished, i.e. the possibility on the participation of peoples and society by a various sphere of multi players, therefore claiming any precarious for risk.

---

[147] Ibid.

[148] UN. *A/HRC/23/40*. 2013, para. 25.

[149] United Kingdom. *Data Protection Act*, 1998, contains 7 Principles. These 7 principles will be the main structure issues for analytical Research in later Chapters. This Law is the Foundation of most Personal Data Protection Law in many States and also International Framework.

[150] United Kingdom. *Data Protection Act*, 1998, the Principle 7. This Principle is high influence to many English using countries and other trade-counterparts.

According to the theme of the above Question, it is important to argue with first four relevant questions which are: Do the Knowledge Economy need a personal data to process and government will save numerous cost from letting it happen and exploiting it at last? Is the attitude of 'Zero Privacy' acceptable? Is the 'fundamental right' an obstacle to the US and EU's Information Society project? and How have the data protection institution done?

Relatively, the essay will introduce the case studies relevant with "Google" to scrutiny the success of EU and US on Data Protection policy and practice in some parts.

1) Does the Knowledge Economy need personal data to process?

At First, not only there are obviously needs of business which prefer a wide open for commercial activities to create a new products in a form of data processing services, but also government whom aroused by private sectors for reforming their efficiency and savings cost for Personal Data Processing. However, there is an argument on the 'unavoidable' economic and social conditions[151] whether it needed to ignore the important of data subjects' protection.

From global economic trend, it leads to data processing reformation in vast majority countries in Western whose economic depend on E-activity more than ever since all manufacturing has been transfer to new major economy countries such as China, Brazil and India. USA, as a leader in ICT business for a long time, is prominently promote the freedom of ICT Corporations but bound itself with Safe Harbor Agreement.[152] The treaty with EU on personal data processing trans-border was constructed as an obligatory manner since US needs to undertake business in EU Market.

However, the globalization of everything include the data transferring, sharing and collecting of personal data, without proper regulation and people-participation, seems to be an violation to abundant data subjects. This concerns leads to the second question about privacy of individual.

---

[151] Ruddick, Graham. "Online Shopping to Grow by £320bn in Three Years", *The Telegraph,* 7 Jun 2015, www.telegraph.co.uk/finance/newsbysector/retailandconsumer/11657830/Online-shopping-to-grow-by-320bn-in-three-years.html. Accessed 2 May 2016.

[152] EU-US. *Safe Harbor Agreement*. 1998.

2) Is the attitude of 'Zero Privacy' acceptable?

On behalf of Privacy, this quote is a controversial one "You have zero privacy. Get over it"[153], since there are many promoters who campaign for integrated global E-Market. This argument could generate effects on the attitude of internet users towards data protection because they try to settle a social norm for accepting "Zero Privacy".

On the contrary, information and comprehension of public affairs are vital if autonomous and free choices are to be made by individual electors.[154] Hence, the state and privates are able to govern internet by the capacities of: designed codes and applications, guardians of it and develop and implement the decisional principles,[155] in term of boosting trust in E-Market.

Nevertheless, it has already been shown of what was government really intents, to promote economic flourishing by any means but lack of protection on data subject's rights. In this respect data collection or data processing without consent of data subjects might lead to massive infringement of Human Rights.

Here withstands, Cyberspace is suitable for proving the "Governmentality" theory of Michel Foucault which reveals the Modern State's technology of power that penetrates to the self of individual through Public space and activity.[156] Since the state eager to shift the line to the former private space combining with the enlargement of public communication spaces, Legal Society has a duty to answer the problems about whether Social Media is a Public Sphere or truly Private Space. With this regards, the data processing system of state authorities and private companies will be used as a powerful Massive Electronic Surveillance device.

---

[153] McNeally, Scott. *SUN Microsystems*. 1999.

[154] Walker, Clive. "Cyber-Constitutionalism and Digital Democracy." *The Internet, Law and Society,* Longman, London, 2000, p. 127.

[155] Bygrave, Lee A and Michaelsen, Terje. *Governors of Internet.* Oxford University Press, UK, 2009, pp. 93-94.

[156] Loader, Brian. *The Governance of Cyberspace: Politics, Technology and Global Restructuring.* Psychology Press, Brighton, 1997, pp. 12-14.

3) Is the 'fundamental right' an obstacle to the Digital Economy Project?

Notwithstanding, the discussions of Human Rights in Cyberspace are concerned about threats to freedom posed by private power, IT Corporation. Not just the threats from the State, as Paul S. Berman mentioned that 'the role of entrenched economic power, the importance of embedded legal regimes, the ubiquitous role of the state, the significance of non-state communities to the construction of norms'[157] imply the needs of sensitivity regulation, cover all influent actors, on cyberspace.

The same old problem on balancing the power of state and individual rights by some conditions; State security, public safety, the monetary interests of the State or the suppression of criminal offences and protecting the rights of others, stills continued. These exceptions are vague and easy to be used as an excuse to interfere the private sphere of individual. Since the competent data collector and processor are the private IT Corporation.[158] While the State Authority are on the edge of dilemma because on one hand State may cooperate with private sectors to gain more power over people, on the other hands they stand still on their position to regulate the misbehaviors of corporation. Due to the low technical capability of State to regulate the data processing, the dreams of people to have a decent state who protect individual by controlling the private company might be naïve.

With regards to EU and EU-US E-Market Harmonization, an intention to create and to enlarge E-Government comes from the concerns on anonymity issue. While anonymity is a part of individual right to privacy, it is a formidable difficulty to manage population[159]of Government. Thus, threats to personal data protection are the surveillance-oriented society which has been constructed on the plea of social order.

4) Does Data Protection need explicit institution to regulate

On the basis of personal data protection implementation, the balance of Individuals freedom and State interference is relevant to characteristics of specific chosen Regulation

---

[157] Berman, Paul Schiff. "Law and Society Approaches to Cyberspace." *Law and Society Approaches to Cyberspace*, Ashgate Publishing, Aldershot, 2007, p. xix.

[158] Koops, Bert-Jaap and Sluijs, Jasper P. "Network Neutrality and Privacy According to Art. 8 Echr." 2011, p. 7.

[159] Ogura, Toshimaru. "Electronic Government and Surveillance-Oriented Society." *Theorizing surveillance*, Willan Publishing, London, 2006, p. 291.

Model. Although the Declaration of Independence of Cyberspace propose the radical independent from state and its legal concepts,[160] which against the eager of governments and corporations mobilized to regulate and control online activities. Even though, the cyberspace could not legitimately regulate by IT Corporation who own technology, or effectively be governed by Centralized-State regulation, there are needs for protection of personal data by some certain of State intervention in combating cybercrime.

For acknowledgement, the legal instruments relating personal data protection were created since 1980's, the time internet was not widespread. So how could International Community apply the old regime to the post-millennium because of the problems caused by Trans-National IT Corporations; Google, Facebook, Yahoo, Microsoft, Apple, etc.. Accordingly, the forthcoming International, Regional and Domestic laws and Data Protection Authority must interpret and apply the law to specific case on dynamism basis but the independent of such institutes should be guaranteed in transparent manner.

In terms of Data Protection Authority (DPA) assessment, this research will show the decisions made by DPAs or the Courts in many cases when there were accusations of cooperation between the National Security Agencies and Information Technology Providers; IT Corporation. The decisions of the Authority could imply some evidence on DPAs efficiency and transparency. The case studies which have been selected are from the EU and USA which will be shown in Chapter 3.

1.5. Object of study and research hypothesis

This Section consists of the object of study, scope of the thesis and lastly the research hypothesis that gives the research questions for studies. These components will illustrate the big picture of the whole research investigation.

Since the object of study is the researches of personal data protection on cyberspace and its limitations in the EU and EU-US E-Market regulation. Thus the limitations in the EU and EU-US legal regime to fulfill right to personal data protection is the matter because such restrictions might put the difficulties to all duty bearers to fulfill data subjects' rights. While

[160] Barlow, John P. "A Declaration of the Independence of Cyberspace, 1996." http://homes. eff. org/~ barlow/Declaration-Final.html. Accessed 3 May 2017.

IT Corporations and State Authorities have an obligation to protect right to personal data of data subjects but those limitations may give the opportunity to State Agencies or IT Corporations to exercise extra interference against those obligations. Moreover, the nature of E-Market, which are dominated by US IT Corporations who transfers and processes personal data of EU citizen across Atlantic, it brings further complicated situations to initiate a common regime to protect personal data between EU and US.

The new proposed regime must deal with 2 main difficult circumstances;

1) Exceptions on the basis of state of emergency; National Security, Public Safety, Morality, etc. to exercise right to personal data especially in the case of Non-US citizen,
2) Enforcing US entities who are obliged with US legal system not the EU in order to implement right to personal data protection in the Single E-Market of EU and EU-US blocs.

This thesis will concentrate on Protection of Personal Data not Privacy, especially on Human Rights purpose, not economic-interest realm. It will focus on the benefit of International Security and Human Rights of internet users around the world not the security of State on the state of human insecurity worldwide.

The Actors and Relations included by the research are the duty bearers of Personal Data Protection law, both State and Private Entity Activities;

1) State Authority who may conduct activities against the integrity of personal data protection; Data Surveillance, Communication Interception of Traffics and Collection of Data.
2) IT Corporation who control and process of data subject's personal data and may fail to fulfill the obligation by undertaking illegitimate Data Collecting, Processing, Mining, Sharing.

The Informal Power Relation between State and Private organization will be brought into account since there is some informal agreement or coordination between State Agency and IT Corporation on data sharing and processing. Hence, the research would find the formal governance of the problem and extend to the informal included regime around the issue.

The time frame of this research is 2001-2016 (After the terrorist's attack in USA on 9/11 until the year the set of EU and EU-US reforms have been launched in 2016). The most critical turning point time that used for separating old regime from new regime is June 5th 2013 since the revelations of Mass Electronic Surveillance was presented on World Wide Web.

The Space of studies covers Cyberspace, Virtual Space on Internet or Online World, especially the E-Market, Internet Traffic in International data transfer. Not only of the EU which have the common regime on Regional Security but also the Trans-Atlantic, EU-US Safe Harbor, Privacy Shield and Umbrella Agreement, which affected and predominated by US Entities. Consequently the Domestic Regulations of USA will be included.

The Research selects 2 Areas for studying; EU and EU-USA E-Market. The research will base on the evidences from practices of each area and others' analysis; documentary reviews and experts' opinions. Moreover, the qualitative information; judgments, resolutions and opinions of the official organization or state authority will be held as the basic proves or interpretations.

There are 3 main issues on personal data protection for the comparative study: Right, Obligation and Implementation. In all 3 issues the study will categorize into 12 subsections; Legal Approval, Definition and Scope of Personal Data Protection, Content of Data Subjects' Rights, Exception to the exercise of Right, Basic Duty of Data Controller and Processor, Condition and Requirement of Data Collection and Processing, Data Security, Data Retention, Transfer of Data to Third Party, Supervisory Authority, Individual Remedy and Enforceability. In each section the analysis will test 3 levels orderly; Universal, Regional and Bi-lateral levels.

Research Hypothesis

International Human Rights Law recognizes a general framework to support and regulate personal data protection on cyberspace realm. Nonetheless, the distinctive characters of cyberspace demand a well designed, at universal level, specific regulation and mechanism to guarantee such fundamental rights relating personal data protection internationally. Accordingly, Research Hypothesis is represented in double issues:

1) Effective personal data protection on cyberspace needs the establishment of an International/Universal legal system treaty-based

2) EU Regime on personal data protection on cyberspace and present EU-US agreements on this issue can be used as a model for initiating such International/Universal Treaty.

Research Questions

From the Hypothesis above, it can be transformed to questions for undertaking research which are:

1) How had the laws of European Union, United States of America and EU-US agreement on personal data protection regulated the E-Market?

2) How the problems had been carried out when there are conflicts between the protecting Human Rights of Individuals and the States' using of IT Corporation's processed data?

3) How did the court decisions relating IT Corporation express? And to what extent does it set precedent for the right to personal data protection?

4) What are the changes that EU and EU-US data protection reforms bring to their E-Market regulation?

5) What should be formulated as the Universal Regime to regulate the data processing of Trans-National IT Corporations and State Authorities for fulfilling right to personal data protection on Domestic, Regional and International levels?

1.6. Research Methods and Methodology

The research applies minor doctrinal legal study on history of data protection law which has been developed to keep up Information technology progress.

However, some of research employs Non-Doctrinal legal study to illustrate the complexity of IT Corporations and State Agencies practice in order to demonstrate the violation on individual rights which was infringed by the ignorance of State Authorities.

In terms of Empirical Research, this research handles both Quantitative and Qualitative style for gathering the data in different case studies in difficult circumstances.

With regards to Quantitative, the static, report and case study numbers will be categorized and represent the operation and cooperation between IT Corporation and State.

On behalf of Qualitative, the literature review on various documents; interviews and press releases from stakeholders, court decisions, official reports and expertise organizations' opinions will be constructed and identify the problems and prospects on personal data protection in different issues.

Aftermath, Critical Legal Study analysis on the political economy among states and corporations will be used as main framework for describing the relationship between them which should be obliged by certain legal data protection regimes.

Ultimately, Prescriptive Research will be employed as a framework to analyze the reforms of EU and EU-US data protection regime. Consequently, the comparative studies to synthesis the prerequisite requirements from EU and EU-US regime for initiating the Universal Regime to support the progressive realization on right to personal data protection of data subjects worldwide.

Researching plan for completing research project consist of

1) Literature Review.
2) Empirical Data will be collected to prove the data processing of IT Corporation and their cooperation with State on data collecting, processing and sharing.
3) Political Economy analysis on the legitimacy of IT Corporation and State relationship from empirical evidence.
4) Socio-Legal analysis on old personal data protection laws and enforcements.
5) Prescriptive Research on Jurisprudence from Court Case Studies; US Courts and Court of Justice of European Union.
6) Normative Research on new personal data protection laws and enforcements.
7) Synthesis the prospects to promote personal data protection regime from research.

For fulfilling the research plan I need to spend time in many places and visit various spaces to access sources of material;

1) Libraries; Facultat de Dret de la Universitat de Barcelona, Facultat de economia i empresa de la Universitat de Barcelona, Faculty of Law Chiangmai University. These libraries not only allow the access to paper books and academic journals but also provide the catalog of digital library will be described below.

2) Internet Portals; Westlaw, Lexis-Nexis, Social Science Research Network (SSRN) and Legal Scholarship Network (LSN).

3) Official Website of Competence Organizations; United Nations, Office of the UN High Commissioner of Human Rights, Internet Governance Forum (IGF), European Union, Court of Justice of European Union, European Commission Justice Mission, European Parliament Committee on Civil Liberties, justice and Home Affairs, US Federal Trade Commission; Safe Harbor, Privacy Shield, Library of Congress, US Courts Gov.

4) International Annual Seminar of United Nation Internet Governance Forum.

1.7. Structure of the thesis

The research divided into 6 Chapters, first Chapter is the research designing and the last is conclusion and recommendation, as Chapter 2, 3, 4 and 5 contain the result of the research on 4 main issues. In this Section the structure of all Research Contents will be illustrated as well as the short introduction to each issue.

a) The old regime on Personal Data Protection

The Chapter 2 analyzes Universal Instruments, EU Laws and EU-US Agreements before 5th June 2013. By starting with the historical background of personal data protection, then the crystallization of personal data protection institutionally or less formally and have variable legal statuses, scope, and substantive provisions. Together they comprise the contemporary international data protection regulatory environment. In this chapter, the research will estimate the STATUS QUO of personal data protection regime which was enacted before the reformation process of EU and Us. Despite the proliferation of international sources of data protection norms, implementation remains at state level. In effect, depending on national restraints, it is up to national governments to decide whether to

introduce data protection legislation, which international model to apply, how to implement it, and how to balance it against other human rights or other considerations; state security, suppress crime and terrorism. Therefore, for the time being, the domestic personal data protection regime of US must be the subject matter, as it will be reviewed this Chapter 2.

b) Hard Cases of Personal Data Protection in practice and in the Court

As The IT Corporations are the leading actors in this dilemma of Data Processing and Data Protection issue, the relationship between Service Providers (SPs) and State Authorities are crucial to analysis. The threats to personal data protection posed by either state agencies or non-state actors, in this case IT Corporation, are amassing huge stores of traceable data they have possessed. Chapter 3 will reflect the problems by picking the policy and practice of US Intelligence Agency which penetrate into the filling systems contained by Trans-National IT Corporation. In order to search for precise interpretation of personal data protection, the court decisions in US domestic courts and the Court of Justice of European Union will be brought to study. The Court cases which applied the Old laws, before the reformation took place, can give the clear precedent on how right to personal data protection was implemented in many scenarios. Subsequently, those precedents the Court made could be used as benchmarks for creating the new regime on personal data protection in different levels; Domestic, Bilateral, Regional and International.

c) Reforms of the EU and EU-US on Personal Data Protection in Cyberspace

In Chapter 4, reviewing of the new EU personal data protection regime and EU-US Bilateral Agreements will be represented as the outputs of reformation since 6th June 2013. Firstly, the study of US domestic regime transition, of personal data protection on cyberspace. US Government had launched a set of laws to reform their surveillance activity and provide Non-US citizen a stronger entitlement to their right to personal data protection in US Court. Thereupon, the comprehensive revision of the new EU and EU-US regimes, EU approves General Data Protection Regulation (GDPR) and Directive on judicial and criminal matters. Then, EU pursued US Government to sign bilateral-agreement to implement those standards; EU-US Privacy Shield for general data protection and EU-US Umbrella Agreement on judicial and criminal matters. However, there has not been such an

International Treaty for Personal Data Protection. But the studies on EU and EU-US regimes will give prospects for the further movement to initiate Universal, Regional personal data protection instruments and Domestic law.

d) The Universal approach for creating new Personal Data Protection Regime

Finally, the 5th Chapter will evaluate the possibility to initiate International Treaty for regulating data using across border. The result of research might show the straightforward balance of control because the politics of law making shift the boundary between State Power and Individual right. This boundary would be beneficial outcome for Governance Model to Regulate IT Corporation and State Authority. The problems here are what State must initiate the changes and what must be done by private company without overwhelming state interfering. For particular action, the initiatives of either international governmental organizations or non-governmental movements will be studied. By extracting the reforms of EU and EU-US regime, there are set of principles in each issue could be imported to create International Regime for protection of personal data.

From the 2nd and 3rd Chapter, the research stripes to narrate the problems, old legal frameworks, hard cases in the Court and reforms of EU and EU-US E-Market chronically. Later, Chapter 4th illustrates the reforms EU and US have taken to handle the problems and the 5th Chapter tries to find probability and propose the prospects to constitute the Universal Personal Data Protection Regime for harmonizing legal standard in Cyberspace.

Chapter 2 Legal Framework on Personal Data Protection before 2013 reform

Information technology converged with telecommunications, creating the current interconnected and internationalized environment of personal data processing, the Internet. Processing of personal information is no longer performed domestically, or even within well-defined physical borders. The original "transborder flows of personal data"[1], which by definition included transmission of data from one jurisdiction to another, were soon replaced by borderless continuous personal data processing, in which personal data are processed somewhere in the "cyberspace", that is, in indistinguishable server-farms installed around the world.

In addition, trans-border personal data processing became individualized. Local data controllers are no longer needed to transmit their data subjects' data across borders to other data controllers in order for trans-border exchanges to occur.[2] Today, Web 3.0 applications enable individuals to upload their personal data to the "social network" or "webpage", going to and from unidentified destination.

Consequently, the need for international governance of data protection is more important than ever. However, the means to achieve this still seem to be missing or at least the ones at hand do not meet with the necessary international consensus. The first point refers to the fact that, the right to data protection is not the same as the right to privacy, and the terms "data privacy" and "information privacy" may have different content in different parts of the world. Even though the goal of this research is to harmonize the provision and implementation of Personal Data Protection, for creating International Regime, but this Chapter will show the overlaps of various instruments; universal, European and bilateral EU-US level, regulating this issue.

Firstly the development of Personal Data Protection will be scrutinized by the running of time through history.

---

[1] *See* the title of the OECD data privacy instrument, "*Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*." 23 Sep. 1980.

[2] De Hert, Paul and Papakonstantinou, Vagelis. "Three Scenarios for International Governance of Data Privacy: Towards an International Data Privacy Organization, Preferably a UN Agency." *ISJLP*, vol. 9, 2013, p. 273.

2.1. The History of General, EU and EU-US legal system on Personal Data Protection

Since the end of Second World War, the concept of a "right to privacy" emerged in international law without obviously mentioned about "personal data protection". This first arose in a rather weak version in Article 12 of the Universal Declaration of Human Rights in 1948. A more substantive protection followed in Article 8 of the European Convention on Human Rights (ECHR) in 1950. According to which everyone has the right to respect for his private sphere. The mentioning of 'home' and 'correspondence' could build on constitutional traditions in many countries around the world, as a common heritage of a long development, sometimes during many centuries, but the focus on 'privacy' and 'private life' was new.[3] It was an obvious reaction to what had happened; secret police, wiretapping and mass surveillance on population, during the time of transition in European Politic Society at the early 1900 until WWII. Thus, the interference with the right to respect for private life, must base on adequate legal basis; clear, accessible and foreseeable, and it was necessary and proportionate for the legitimate interests at stake.

Privacy and Personal Data Protection, to be more precisely: the right to respect for private life and the right to the protection of personal data, have crucial interrelated. They are both fairly recent expressions of a universal thought with strong ethical perspectives: the dignity, autonomy and unique value of every human being. However, there are also important differences. The concept of " personal data protection" was developed in order to provide structural legal protection to individuals against the inappropriate use of information technology for processing information relating to them, regardless of whether that processing would be within the scope of the right to respect for private life or not. The consequence set of safeguards, in essence a system of checks and balances, consisting of substantive conditions, individual rights, procedural provisions and independent supervision, applies in principle to all processing of personal data.[4]

Data protection as a separate topic in legal science discourse and legislative practice arose in the 1970s and 1980s, in the era in which computerized automatic data processing became popular. With technological progress, data has been very valuable and important. Mass volumes of data can be used to provide different services; this was not possible before

[3] Hustinx, Peter. *EU Data Protection Law: The Review of Directive 95/46/EC and the Proposed General Data Protection Regulation*. 2014, p. 3.

[4] Ibid, p. 50.

automated processing. Data exchange and cross-use are important for public and private services based on various data. Still, the nature of data protection should be related to the content of the data and not to their form. In practice, it could mean key differences that the legal system must take into consideration to ensure that the rules are suitable in different situations. With regard to data protection, it must be decided how, if at all, data can be protected to the same extent in the cyberspace as in the "real" world. [5] It is usual that attempts to create a safe online society result in even harder than in an offline environment because the amount of processed data is far greater than the past.

Due to the technology development in early 1970's the Council of Europe concluded that Article 8 ECHR had a number of shortcomings in the light of new developments, particularly in view of the growing use of information technology: the uncertainty as to what was covered by 'private life', the emphasis on protection against interference by 'public authorities', and the lack of a more pro-active approach, also dealing with the possible misuse of personal information by companies or other relevant organizations in the private sector.[6] Since 1997 the European Court of Human Rights has ruled in a number of cases that the protection of personal data is of 'fundamental importance' for a person's enjoyment of the right to respect for private life under Article 8 ECHR, and has derived yardsticks from the Convention for determining the extent to which that right had been infringed.[7] This suggests that the Court is increasingly inclined to assess compliance with the Convention - at any rate for 'sensitive data' - within the context of Article 8 ECHR. This resulted to the Member States to take all necessary steps to give effect to certain principles on the protection of the privacy of individuals in the private and the public sector.[8]

The world's first law on data protection was adopted in Hessen, local government administration in Democratic Republic of Germany, in 1970. Sweden was the first country to

[5] Metcalf, Katrin N. "Legal Aspects of Privacy Law and Data Protection." *The Right to Privacy as a Human Right and Everyday Technologies*, Institute of Human Rights NGO, 2014, p. 83.

[6] Council of Europe. *Explanatory Report to Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*. Strasbourg, 1973, para. 4.

[7] European Court of Human Rights. *ECHR 1997-I Z v Finland, Application 22009/93*, p. 95.

[8] Council of Europe Committee of Ministers. *Resolution (73) 22 on the protection of the privacy of individuals vis-a-vis electronic data banks in the private sector.* 1973; *Resolution (74) 29 on the protection of the privacy of individuals vis-a-vis electronic data banks in the public sector*. 1974.

adopt a national law on data protection in 1973,[9] then it was followed by legislations in a vast majority countries. In December 1983, the Constitutional Court of Germany adopted a decision under which certain aspects of a census were considered to run counter to fundamental liberties due to the inviolability of personal privacy. [10] All of this happened at a time when more computer-based data processing began to be used. Technology showed the importance of data protection, as it was possible to process a very large amount of data to obtain some useful information from them. Technology can be used to glean meaning from a large set of detailed data, various data can be collated so that insignificant data take on importance, and data can be gathered and disseminated worldwide. [11] Information Technology is undisputedly responsible for creating a new context in which personal data protection regime must be implemented.

The first major international document that expressed the main principles of data protection, such as expedience and proportionality, was the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data in 1980.[12] Nevertheless, the first binding instrument on the subject is the product of The Council of Europe which invested time in the preparation of an international agreement. After four years this resulted in the adoption of the Data Protection Convention in 1981 at Strasbourg[13], Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, also known as Convention 108.

During the 1990s, and within the European Communities framework, European Commission therefore submitted a proposal for a Directive in order to harmonize the national laws on data protection in the private and most parts of the public sector.[14] After half-decade of negotiation, this resulted in the adoption of the Directive 95/46/EC32. The consequence is

[9] Fokus, Fraunhofer. (Hoepner, P and Strickand, L and Löhe, M.). *Historical Analysis on European Data Protection Legislation.* 2012, pp. 11-12.

[10] Ibid, p. 12.

[11] Fuster, Gloria González et al. "From Unsolicited Communications to Unsolicited Adjustments." *Data Protection in a Profiled World*, Springer, 2010, pp. 105-117.

[12] The OECD Data Privacy Instrument, "*Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*." 23 Sep. 1980.

[13] Council of Europe. *Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data Convention108.* 1981.

[14] European Commission. *COM (90) 314 final - SYN 287 and 288*. Brussels, 13 Sep. 1990, p. 4.

that the Directive has led to a much greater consistency between Member States, but certainly not to identical or fully consistent solutions.[15]

In 2008 also to Council Framework Decision 2008/977/JHA with general rules on the protection of personal data processed in the context of police and judicial cooperation in criminal matters, including EUROJUST and EUROPOL. It reflects the forthcoming matters in criminal justice that need more and more processed personal data to prevent and suppress crime but the concerns on confidential breached by State Authority has arisen as well.

The EU Directive 95/46/EC has set out rules for transferring personal data from the EU to third countries for two decades. Under these rules, the Commission may decide that a non-EU country ensures an "adequate level of protection". These decisions are commonly referred to as "adequacy decisions" which set standard among EU Member State and between EU and other country since 1995. Until 2000, EU adopted a Decision recognizing the "Safe Harbour Privacy Principles" and "Frequently Asked Questions", issued by the Department of Commerce of the United States,[16] as providing adequate protection for the purposes of personal data transfers from the EU to US. The bilateral data protection agreement had created a significant Bloc of Digital Single Market within liberal democratic regime country.

Due to the rapid progress of ICT in the last two decades, a new situation has now arisen whereby private IT Corporations possess a large amount of data on people – data they have obtained from the individuals themselves – either directly, though the people putting the data in Social Network (e.g. Facebook, Twitter) or people using an Internet service that allows various things to be found out about them (Google, Yahoo, Microsoft Network). Many companies, including major international IT Corporations such as Facebook and Google, have their own "Terms&Conditions" and different structures for implementing the rules. But these are rules the companies have themselves seen fit to establish and are mainly based on the goodwill of the respective IT Corporations. In addition, national legislation is in force regardless of the fact that the companies are multinationals and it may be difficult to establish

[15] Hustinx, Peter. *EU Data Protection Law: The Review of Directive 95/46/EC and the Proposed General Data Protection Regulation*. 2014, p. 9.

[16] European Commission. *Restoring Trust in EU-US data flows - Frequently Asked Questions*. Brussels, 27 Nov. 2013, pp. 2-3.

a direct link to a given jurisdiction in a specific case.[17] Nonetheless, laws could, in fact, prove difficult to apply effectively due to obstacles related to jurisdiction.

The short history of universal data protection has shown the desires in different places to construct Universal, Regional, Bilateral and Domestic norms for protecting the right to personal data of internet users on one hand and to support the enlargement of E-Market on the other hand. As we will analyze in the following section, these old regimes for protecting the right to personal data are not enough to protect internet users in past era. There are obvious needs for creating a harmonized standard for Single E-Market on the basis of liberal democratic society.

2.2. Legal Analysis of the Instruments relating to Personal Data Protection

Apparently a multitude of supranational sources of data protection norms exist, both at an international and at a regional level. The crystallization of data protection may be institutional or less formal and have variable legal statuses, scope, and substantive provisions. Together they comprise the contemporary international data protection regulatory environment. Despite the proliferation of international sources of data protection norms, implementation remains at state level. In effect, depending on national restraints (for instance, participation or not in an international organization), it is up to national governments to decide whether to introduce data protection legislation, which international model to apply (i.e. UN, OECD, Council of Europe, EU, or the Asia-Pacific Economic Cooperation (APEC)), how to implement it, and how to balance it against other human rights or other considerations (state security, finance, etc.). Therefore, for the time being, international governance of personal data protection retains a horizontal character: it sets the agenda and formulates broad principles, but leaves the implementation at the local level.[18] The regulatory regime, as it will be reviewed in Chapter 2 of this research, has reached its limits through contemporary Information Technology applications.

[17] Metcalf, Katrin N. "Legal Aspects of Privacy Law and Data Protection." *The Right to Privacy as a Human Right and Everyday Technologies*, Institute of Human Rights NGO, 2014, p. 85.

[18] De Hert, Paul and Vagelis Papakonstantinou. "Three Scenarios for International Governance of Data Privacy: Towards an International Data Privacy Organization, Preferably a UN Agency." *ISJLP*, vol. 9, 2013, p.275.

In this chapter, the research will analyze the STATUS QUO of personal data protection regime which was enacted before the reformation process of EU and US since 6th June 2013.

2.2.1. Individual's Right to Personal Data Protection

The structure of the content in right to personal data protection of individual will be differentiated into 4 sections. First of all, the research will explore how legal documents recognize personal data protection in various sources; universal, regional and bilateral instruments. Secondly, the crystallization of personal data protection by vast majority instruments in order to illustrate definition and scope of this legal issue. Third, the development of right to personal data protection on behalf of individual, data subjects' right, for evaluating the consistence and overlap between data protection instruments. Ultimately, comparative study on the restrictions to exercise personal data protection from different instruments for framing up the conditions IT Corporation and State Authority may limit the data subjects' right. These are legal issues the research tries to point out as the problems from the old personal data protection regime.

2.2.1.1. Legal Approval of Personal Data Protection

This section will describe the recognition of Personal Data protection in diverse instruments from International Organization to EU Regional Bloc then Bilateral EU-US agreement. Accordingly, the legal binding consequence of each agreement is different because the legal nature of each one is up to the manner of its launching institution.

International human rights law provides the universal framework against which any interventions in individual privacy rights must be assessed. Article 12 of the Universal Declaration of Human Rights (UDHR) provides that "no one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation."[19] Everyone has the right to the protection of the law against such interference or attacks[20] since it is a part of Individual's right to privacy. The rapid and

[19] UN. *UDHR*. 1948, Article 12.

[20] UN. *A/HRC/27/37*, 2014, para. 12.

monumental changes to communications and information technologies experienced in recent decades have also irreversibly affected our understandings of the boundaries between private and public spheres.[21]

The UDHR has been recognized as International Customary Law so the right to privacy and the non-interfere of communication is the fundamental rights of human. Not only it shall apply to any States whether consent has been given or not, but also be the legal basis for any other international instruments relate to personal data protection. UDHR has affirmed the right to privacy of person since 1948 and apply to every States of the world.

The right to privacy is often understood as an essential requirement for the realization of the right to freedom of expression. Undue interference with individuals' privacy can both directly and indirectly limit the free development and exchange of ideas. Restrictions of anonymity in communication, for example, have an evident chilling effect on victims of all forms of violence and abuse, who may be reluctant to report for fear of double victimization.[22]

As freedom of Expression is guaranteed in *Article 19* of UDHR[23], it has reaffirmed the relevance to freedom of expression to hold opinions and access information without interference through any means across frontiers.

Since the Internet is the Technology for human communication, the right to participate in technological development is relevant to activities of the people via Information and Communication Technology. Thus, Article 27of UDHR[24] can be interpreted as a legal baseline for individual to utilize full enjoyment of information technology without arbitrary interference on privacy.

Therefore, the arguments of IT Corporation and State that they told the people, who aware of privacy and data protection on Internet, to avoid using the communication

[21] UN. *A/HRC/23/40*. 2013, para. 21.

[22] Ibid, para. 24.

[23] UN. *UDHR*. 1948, Article 19. *"Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers*"

[24] UN. *UDHR*. Article 27. "(1) Everyone has the right freely to participate in the cultural life of the community, to enjoy the arts and to share in scientific advancement and its benefits.

(2) Everyone has the right to the protection of the moral and material interests resulting from any scientific, literary or artistic production of which he is the author."

technology, is incompatible with the article 27. Since the enjoyment and utilization of the technology are a basic Human Rights of every person. Hence the balance between Data Protection and Technology Participation should be constructed through various forms of legal policy and development practice.

The International Covenant on Civil and Political Rights (ICCPR), ratified by 167 States,[25] provides in article 17 that "no one shall be subjected to arbitrary or unlawful interference with his or her privacy, family, home or correspondence, nor to unlawful attacks on his or her honour and reputation". It further states that "everyone has the right to the protection of the law against such interference or attacks."[26] The ICCPR has obliged member states and protect the rights of person from the violations of any entities.

As well as UDHR, ICCPR recognize the interdependence of right to privacy on communication with freedom of expression. In its General Comment No. 34 (2011) on the right to freedom of expression, the Human Rights Committee indicated that States parties should take account of the extent to which developments in information and communication technologies have substantially changed communication practices. The Committee also called on States parties to take all necessary steps to foster the independence of these new media. The General Comment also analyses the relationship between the protection of privacy and freedom of expression, and recommends that States parties respect that element of the right of freedom of expression that embraces the limited journalistic privilege not to disclose information sources.[27]

International and regional human rights treaty bodies, courts, commissions and independent experts have all provided relevant guidance with regard to the scope and content of the right to privacy, including the meaning of "interference" with an individual's privacy. In its general comment No. 16, the Human Rights Committee underlined that compliance with article 17 of the International Covenant on Civil and Political Rights required that the integrity and confidentiality of correspondence should be guaranteed de jure and de facto.

[25] Update until 19 Feb. 2015, http://indicators.ohchr.org/.

[26] UN. *International Covenant on Civil and Political Right.* 1966, Article 17.

[27] UN. *CCPR General Comment No. 34*. 2011.

"Correspondence should be delivered to the addressee without interception and without being opened or otherwise read".[28]

The United Nations adopted General Assembly resolution 45/95 on December 14, 1990. The resolution, Guidelines for the Regulation of Computerized Personal Data Files, set out Fair Information Practices for the use of personal data. The United Nations General Assembly recommended that governments incorporate the privacy guidelines into legislation and administrative regulations. The UN Guidelines 1990[29] thus form an adequate data protection regulatory Framework.[30]

The UN Guidelines have received undeserved criticism for being of "limited practical relevance,"[31] mostly due to their non-legally binding character. This is probably exaggerated: the OECD Guidelines are non-binding, but there is a general consensus as to their global influence and central importance. Perhaps the root of such criticisms is related to the timing of the UN Guidelines. They came at a time, in 1990, when the OECD Guidelines and Convention 108 had already formed a concrete basis in the data protection field, and the UN Guidelines did not offer much added value. Nevertheless, their greatest advantage was a vastly larger circle, placing them at a unique starting point for becoming the only truly universal instrument[32] for data protection governance.

Even in the International Economic Law under WTO provision, General Agreement on Trade of Services (GATS), recognizes the significance of ensuring privacy of individuals and the protection of sensitive personal data in Article XIV (c) (ii).[33]

---

[28] Official Records of the General Assembly. *Forty-third Session, Supplement No. 40 (A/43/40)*. 1989, annex VI, para. 8.

[29] Regardless of the fact that their elaboration took more than ten years to complete, the UN level took perhaps an unnecessarily long time to complete, something that does not sit well with the contemporary pace of technological developments.

[30] De Hert, Paul and Vagelis Papakonstantinou. "Three Scenarios for International Governance of Data Privacy: Towards an International Data Privacy Organization, Preferably a UN Agency." *ISJLP*, vol. 9, 2013, p.281.

[31] Kuner, Christopher. "An International Legal Framework for Data Protection: Issues and Prospects." *Computer law & security review*, vol. 25, no. 4, 2009, p. 314.

[32] De Hert, Paul and Vagelis Papakonstantinou. "Three Scenarios for International Governance of Data Privacy: Towards an International Data Privacy Organization, Preferably a UN Agency." *ISJLP*, vol. 9, 2013, p. 282.

[33] WTO. *GATS. 1995,* Article XIV: General Exceptions

"Subject to the requirement that such measures are not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination between countries where like conditions prevail, or a disguised

At regional level, the European Convention on Human Rights (ECHR) is the most advance International Human Rights Instrument which describe the advantageous provision on Private Life Protection in the time it was declared in 1950. The detail Article 834 is scoped on protecting everyone's right to respect for his private and family life, his home and his correspondence. Furthermore, the ECHR Article 1035 provide the relationship between right to respect for private and family life and the Freedom of expression as the integrity of communication and confidence in Privacy support freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers. As CJEU decision case 4-73 ensures that fundamental rights are an integral part of the general principles of European Union which every member states and organization must respect and fulfill.[36]Accordingly, all EU Member States' organizations and officers or Council of Europe instruments must incorporate Human Rights, right to privacy;

---

restriction on trade in services, nothing in this Agreement shall be construed to prevent the adoption or enforcement by any Member of measures:…

(c) necessary to secure compliance with laws or regulations which are not inconsistent with the provisions of this Agreement including those relating to:…

(ii) the protection of the privacy of individuals in relation to the processing and dissemination of personal data and the protection of confidentiality of individual records and accounts."…

[34] *ECHR* Article 8 Right to respect for private and family life

"1. Everyone has the right to respect for his private and family life, his home and his correspondence.

2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others."

[35] *ECHR* Article 10 Freedom of expression

"1. Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers. This article shall not prevent States from requiring the licensing of broadcasting, television or cinema enterprises.

2. The exercise of these freedoms, since it carries with it duties and responsibilities, may be subject to such formalities, conditions, restrictions or penalties as are prescribed by law and are necessary in a democratic society, in the interests of national security, territorial integrity or public safety, for the prevention of disorder or crime, for the protection of health or morals, for the protection of the reputation or rights of others, for preventing the disclosure of information received in confidence, or for maintaining the authority and impartiality of the judiciary."

[36] CJEU. *Case 4-73 J. Nold, Kohlen- und Baustoffgroßhandlung v Commission of the European Communities*. 14 May 1974.

data privacy, personal data protection, as a common ground for those provisions and its implementation.

The Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data of the Council of Europe of 1981 (Convention 108) extended the safeguards for everyone's rights and fundamental freedoms, and in particular the right to the respect for privacy, taking account of the increasing flow across frontiers of personal data undergoing automatic processing.[37]

Moreover, Convention 108 is the first Legal-Binding International Instrument in the field of Personal Data Protection on Computerized Data Process and Dominate International Standard since the first Era of Internet Technology across Border and Trans-Atlantic. All members of the Council of Europe have ratified the treaty, except San Marino and Turkey (Turkey signed the Convention in 1981). Uruguay has also ratified the treaty. The Convention 108 had created International Standard since the first Era of Internet Technology across Border and Trans-Atlantic.

At EU level, the EU Directive 95/46/EC encompasses all key elements from article 8 of the European Convention on Human Rights, which states its intention to respect the rights of privacy in personal and family life, as well as in home and in personal correspondence.[38] The Directive is based on the 1980 OECD "Recommendations of the Council concerning guidelines Governing the Protection of Privacy and Trans-Border Flows of Personal Data" [39]. A key purpose of the OECD Guidelines 1980 was to "advance the free flow of information between Member countries and to avoid the creation of unjustified obstacles to the development of economic and social relations among Member countries" they therefore intended to improve international cooperation rather than national law harmonization.[40] The 1995 Data Protection Directive set a milestone in the history of the protection of personal data in the European Union. The Directive reflects two of the

[37] Council of Europe. *Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data Convention108.* 1981, Preamble.

[38] EU. *Directive 95/46/EC.* 1995, Preamble.

[39] Ibid.

[40] Kirby, Michael. "The History, Achievement and Future of the 1980 Oecd Guidelines on Privacy." *International Data Privacy Law,* vol. 1, no. 1, 2011.

important foundation pillars of the European integration process: the protection of fundamental rights and freedoms of individuals and in particular the fundamental right to data protection, on the one hand, and the achievement of the internal market – the free flow of personal data in this case – on the other. The EU data protection Directive 1995 mandated that the member states pass their local data laws by October 25, 1998, but in fact full implementation took several years more.[41]

Directive 2002/58 on Privacy and Electronic Communications, otherwise known as E-Privacy Directive, is an EU directive on data protection and privacy in the digital age. It presents a continuation of earlier efforts, most directly the Data Protection Directive.[42] It deals with the regulation of a number of important issues such as confidentiality of information; treatment of traffic data, spam and cookies, which ensure that the automatic processing of personal data will be regulated on the basis of legal rights protection. This Directive has been minor amended by Directive 2009/136 in 2009, which introduces several changes, especially in what concerns "cookies",[43] that are now subject to prior consent. The EU Cookie Directive (Directive 2009/136/EC of the European Parliament and of the Council) is an amendment of the Directive 2002/58/EC, which concerns the protection of data and privacy on the web.[44]

The entry into force of the Treaty of Lisbon on 1st December 2009 gives place to important novelties as regards personal data protection in the EU. First, a new legal base is introduced in the current article 16 of the Treaty on the Functioning of the EU, [45] recognizing the right of everyone to the protection of personal data concerning them and establishing the

[41] Dowling Jr, Donald C. "Preparing to Resolve Us-Based Employers' Disputes under Europe's New Data Privacy Law." *J. Alt. Disp. Resol.*, vol. 2, 2000, p. 31

[42] EU. *Directive 2002/58/EC.* 2002, Article1.

[43] EU. *Directive 2009/136/EC.* 2009.

[44] Ibid, Preamble.

[45] EU. *Treaty on European Union and the Treaty on the Functioning of the European Union* (TFEU). 2012, Article 16

"1. Everyone has the right to the protection of personal data concerning them.

2. The European Parliament and the Council, acting in accordance with the ordinary legislative procedure, shall lay down the rules relating to the protection of individuals with regard to the processing of personal data by Union institutions, bodies, offices and agencies, and by the Member States when carrying out activities which fall within the scope of Union law, and the rules relating to the free movement of such data. Compliance with these rules shall be subject to the control of independent authorities."

competence of the EU institutions to lay down the rules relating to the protection of individuals with regard to the processing of personal data by Union institutions, bodies, offices and agencies, and by the Member States when carrying out activities which fall within the scope of Union law, and the rules relating to the free movement of such data. The same article requires that compliance with these rules shall be subject to the control of independent authorities. Second, and taking into account article 6 of the Treaty on European Union,[46] those EU rules must comply with the right to the protection of personal data as it is understood in article 8 of the Charter of Fundamental Rights of the EU.[47]

Nevertheless, there were needs for an overarching instrument applying to data processing operations in all sectors and policies of the Union, ensuring an integrated approach as well as seamless, consistent and effective protection. The above challenges require the EU to develop a comprehensive and coherent approach guaranteeing that the fundamental right to data protection for individuals is fully respected within the EU and International Legal Instruments.

At the Bilateral EU-US level, the exchange of personal data for commercial purposes is addressed by the Safe Harbor Decision[48] which provides a legal basis for transfers of personal data from the EU to companies in the U.S. which adhere to the Safe Harbor Principles. US-EU Safe Harbor is a streamlined process for EU and US companies to

[46] EU. The Treaty of European Union (TEU). 2007, Article 6

"1. The Union is founded on the principles of liberty, democracy, respect for human rights and fundamental freedoms, and the rule of law, principles which are common to the Member States.

2. The Union shall respect fundamental rights, as guaranteed by the European Convention for the Protection of Human Rights and Fundamental Freedoms signed in Rome on 4 November 1950 and as they result from the constitutional traditions common to the Member States, as general principles of Community law.

3. The Union shall respect the national identities of its Member States.

4. The Union shall provide itself with the means necessary to attain its objectives and carry through its policies."

[47] EU. *Charter of Fundamental Rights of the European Union*. 2010, Article 8 Protection of personal data

"1. Everyone has the right to the protection of personal data concerning him or her.

2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.

3. Compliance with these rules shall be subject to control by an independent authority."

[48] EU Commission. *2000/520/EC.* 2000, Preamble.

comply with the EU Directive 95/46/EC on the protection of personal data.[49] The process was developed by the US Department of Commerce in consultation with the EU. Intended for organizations within the EU or US that store customer data, the Safe Harbor Principles are designed to prevent accidental information disclosure or loss.

Because safe harbor emerged as a compromise between the EU Commission and the US Department of Commerce very different from what both party had originally wanted, and because safe harbor is a unique-in-the-world arrangement that applies only to the United States, it should not be surprising that safe harbor has attracted criticisms from the beginning.[50]

Personal Data protection has been recognized in diverse instruments from International Organization to EU Regional Bloc then Bilateral EU-US agreement. Accordingly, the legal binding consequence of each agreement is different because the legal nature of each one is up to the manner of its launching institution. Differences in the legal nature of data protection law between cultures and legal systems have made it more difficult to reach an international consensus on the subject.

The characterization of data protection as a human right has important legal implications, since it means that the law may be more difficult to change and a higher value may be placed on the rights of individuals than in jurisdictions where the subject is seen more from the point of view of economic efficiency than human rights. Differences in the legal nature of data protection law between cultures and legal systems have made it more difficult to reach an international consensus on the subject.[51] The Single E-Market Project need the more supranational legal instrument for the sake of harmonized regime to protect personal data and support the progress of flourishing economy.

---

[49] U.S. Department of Commerce. *Welcome to the U.S.-EU & U.S.-Swiss Safe Harbor Frameworks*, 9 Oct. 2015.

[50] Rehder, Jörg and Erika C Collins. "The Legal Transfer of Employment-Related Data to Outside the European Union: Is It Even Still Possible?." *The International Lawyer*, 2005, pp. 150-151.

[51] Kirby, Michael. "The History, Achievement and Future of the 1980 OECD Guidelines on Privacy." *International Data Privacy Law*, vol. 1, no. 1, 2011.

2.2.1.2. Definition and Scope of Personal Data Protection

This section review the particular instruments previously mentioned but now in order to find the commons and differences of definition and scope which are written in those various sources. As the different definition leads to distinctive scope of protection but the same make it easy to compliance. Since there are three levels of instrument; Universal, Regional and Bilateral, the overlaps of scope and definition may bring complicates to the implementation of personal data protection.

Most data protection national legislation is based on the same international documents (such as the UN Framework, OECD Guidelines, Council of Europe Convention 108, the APEC Privacy Framework, etc.), so that the fundamental, high-level principles of the law are similar across regions and national legal systems.[52] However, the differences in the cultural, historical, and legal approaches to data protection mean that once one descends from the highest level of standard settings, there can be significant differences in detail. This is not surprising, since concepts such as 'data protection' and 'privacy' are derived from national legal culture and tradition, and thus vary considerably around the world,[53] even in systems that accept the same fundamental principles.

The United Nations Guidelines for the Regulation of Computerized Personal Data Files lay out the definition and scope in part A.[54] Personal Data is "Information about persons" and Sensitive Personal Data scope is relating to racial or ethnic origin, colour, sex life, political opinions, religious, philosophical and other beliefs as well as membership of an association or trade union. The scope of application extends "to all public and private computerized files" and extends to files on legal persons particularly when they contain some information on individuals.[55] Moreover, it enlarges the scope to apply to personal data files kept by governmental international organizations either files for internal purposes and

[52] Bygrave, Lee A. "Privacy Protection in a Global Context–a Comparative Overview." *Scandinavian Studies in Law*, vol. 47, 2004, p. 347.

[53] International Law Commission. "Report on the Work of its Fifty-Eighth Session (1 May to 9 June and 3 July to 11 August 2006)." *UN Doc A/61/10*, New York, 2006, p. 499.

[54] UN. *A/RES/45/95.* 1990, part A principle 1 and 5.

[55] Ibid, part A principle 10.

external purposes concerning third parties[56] regardless of different jurisdictions[57] and legal traditions.

Another international instrument is WTO agreement, Article XIV (c) (ii) of the GATS[58] mentions data protection rules "in relation to the processing and dissemination of personal data and the protection of confidentiality of individual records and accounts". Looking at this wording, it can hardly be assumed that the full scope of data protection rules is covered. A question mark would be possible for example in respect to registration requirements of data collections.[59]

The Convention 108 has main purpose to secure Individuals with regard to Automatic Processing of Personal Data in the territory of each Party, whatever his nationality or residence, respect for his rights and fundamental freedoms, and in particular his right to personal data, with regard to automatic processing of personal data relating to him ('data protection').[60] The concept of 'personal data' is defined as 'any information relating to an identified or identifiable individual ('data subject')'.[61] Furthermore, Convention 108 set out additional safeguards in order to protect "special categories of data" [62], revealing racial origin, political opinions, religious or other beliefs, as well as personal data concerning health, sexual life or criminal convictions (also known as "sensitive data").

In this context, it should be noted that many activities in the public or the private sector are nowadays connected, in one way or another, with the collection and processing of personal information. The real objective of the Convention is therefore to protect individuals (citizens, consumers, workers, etc.) against unjustified collection, recording, use and dissemination of their personal details. This may also concern their participation in social relations, whether or not in public, and involve protecting freedom of expression, preventing unfair discrimination and promoting 'fair play' in decision-making

[56] Ibid, part B.

[57] Ibid, part A principle 4.

[58] WTO. *GATS.* 1995, Article XIV: General Exceptions

[59] Weber, Rolf H. "Regulatory Autonomy and Privacy Standards under the Gats." *Asian Journal of WTO & International Health Law and Policy*, vol. 7, 2012, p. 26.

[60] Council of Europe. *Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data Convention108*. 1981, Article 1.

[61] Ibid, Article 2 sub a.

[62] Ibid, Article 6.

processes. Finally the Convention also aimed to reconcile the respect for personal data protection and the free flow of information.[63] The key feature of Convention 108 is it applies to every person without discrimination on the basis of nationality or residence, regardless of frontiers.

The most comprehensive and specific instrument for Personal Data Protection is EU Directive 95/46/EC. In the context of the Directive, it gives a definition and scope on:

- Personal data means "any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity".[64]
- Processing is also broadly defined and involves any manual or automatic operation on personal data, including its collection, recording, organization, storage, modification, retrieval, use, transmission, dissemination or publication, and even blocking, erasure or destruction.[65]

The “data protection” is broader than “privacy protection” because it also concerns other fundamental rights and freedoms, and all kinds of data regardless of their relationship with privacy, and at the same time more limited because it merely concerns the processing of personal information, with other aspects of privacy protection being disregarded.[66]

EU Directive 2002/58 on Privacy and Electronic Communications gives main definition of “Data Subject” which the objective of the Directive is to protect the “right to privacy in the electronic communication sector” and free movement of data, communication equipment and services of Individual. It not only protects the right of natural person but also makes it clear that E-Privacy Directive also applies to “Legal Persons”.[67] The scope given by

[63] Ibid, Preamble para. 4.

[64] EU. *Directive 95/46/EC*. 1995, Article 2a.

[65] Ibid, Article 2b.

[66] Hustinx, Peter. *EU Data Protection Law: The Review of Directive 95/46/EC and the Proposed General Data Protection Regulation*. 2014, p. 5.

[67] EU. *Directive 2002/58/EC*. 2002, Articles 1-2.

this Directive is very important since the most powerful actor who control and process personal data is IT Corporation, Multi-National Legal Person indeed.

Article 16 TFEU also signaled the emancipation of the right to data protection from the right to privacy, a development in itself that was probably also long overdue, and included it independently in the fundamental EU human rights list. However, this is not the end of a process that began in some European countries some two decades ago. Far from the goal, the individual right to data protection is not among other fundamental rights that contend themselves into a declaration in a human rights document.[68] The victory point of having harmonized legal definition, to set precise scope for member states, stills need the cooperation from EU States to conclude such initiative.

The EU-US Safe Harbor Principles defined "personal data" or "personal information" as data about an identified or identifiable individual that are within the scope of the Directive (EU Directive 95/46/EC), received by a U.S. organization from the European Union, and recorded in any form.[69] This means US government adopted the same definition as EU did.

The scope of Safe Harbor covers only U.S. organizations registered with the Federal Trade Commission to participate in this voluntary program. This excludes many financial institutions, (such as banks, investment houses, credit unions, and savings & loans institutions – Financial Tech Industry), telecommunication common carriers, including internet service providers, non-profit organizations, online-journalists and most insurances.[70] Although it may include some investment banks by its own volunteer.[71] The USA companies can opt into the program as long as they adhere to the 7 principles and 15 frequently asked questions and answers per the Directive 95/46/EC.[72]

The complicated situations arise when it has to deals with different legal regime base various jurisdiction. As the relationship between EU and US depend heavily on

---

[68] De Hert, Paul. "The Right to Protection of Personal Data. Incapable of Autonomous Standing in the Basic EU Constituting Documents?." *Utrecht Journal of International and European Law*, vol. 1, no. 31, 2015, p. 1.

[69] US Federal Trade Commission. *Safe Harbor Principles*. 2000.

[70] U.S. Department of Commerce. *Welcome to the U.S.-EU & U.S.-Swiss Safe Harbor Frameworks*, 9 Oct. 2015.

[71] U.S. Department of Commerce. *FAQ - Investment banking and audits.* 29 Jan. 2009.

[72] US Federal Trade Commission. *Safe Harbor Principles Annex*. 2000.

the protection of US legal system. The expectation on protection of personal data of EU Nationals may not accomplish since it was out of their reach, in US regime per se. While in the EU Member States case which each State had some flexibility in implementing the Data Protection Directive's requirements into law locally, and they were also permitted to extend the Data Protection Directive's scope (for example, to include the data of non-natural legal persons such as companies).[73] This means there are important national differences in data protection laws within the EU - such as on civil liability, and on penalties for non-compliance with domestic data protection laws. Thus the question of harmonization of legal definition and scope is rising.

The commons and differences of definition and scope written in various sources, brings complicates to the implementation of personal data protection. The most common ground is the concept of 'personal data' and the additional safeguards to protect "special categories of data" , also known as "sensitive data". Many activities in the public or the private sector are under scope of personal data protection instruments which cover large amount of information. But it has brought troubles to individual for exercising their right in other countries. However, the different scopes are on actor and jurisdiction as most powerful actor who control and process personal data, IT Corporation; Multi-National Legal Person, is under the appliance of the Law of specific territory but their activities are trans-border.

2.2.1.3. Content of Data Subjects' Right to Data Protection

The instruments relating to personal data have been creating for decades so there is some out-of date provisions maintain in those legal documents. The more advance in technology the more complexity it brought into legal atmosphere. Accordingly, further affirmation of individual right to personal data protection in detail has been added by many legal instruments. This section finds some common contents of legal right in different personal data protection instruments and some inconsistence may exist because it affects the protection standard either in practice or policy.

[73] Kuner, Christopher. "European Data Protection Law." *Corporate Compliance and Regulation,* Oxford University Press, UK, 2007, ch. 2.37.

The OECD Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data recognize the Rights of Individual in Individual Participation Principle[74] that an individual should have the:

a) Right to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him;

b) Right to have communicated to him, data relating to him

i) within a reasonable time;
ii) at a charge, if any, that is not excessive;
iii) in a reasonable manner; and
iv) in a form that is readily intelligible to him;

c) Right to be given reasons if a request made under subparagraphs (a) and (b) is denied, and to be able to challenge such denial; and

d) Right to challenge data relating to him and, if the challenge is successful to have the data erased, rectified, completed or amended.

Nonetheless, the State Members of OECD are the duty bearers who need to implement above rights into their domestic personal data protection law.

The United Nations Guidelines for the Regulation of Computerized Personal Data Files, *Principle of interested-person access,*[75] approves data subject:

- Right to know whether information concerning him is being processed;
- Right to access and have appropriate rectifications or erasures made in the case of unlawful unnecessary or inaccurate entries;
- Right to gain remedy.

Guidelines not only mention that the cost of any rectification shall be borne by the person responsible for the file. But also emphasize that the principle should apply to everyone, irrespective of nationality or place of residence.

[74] OECD. *Annex to the Recommendation of the Council of Guidelines Governing The Protection of Privacy and Transborder Flows of Personal Data.* 23 Sep. 1980, para. 13.

[75] UN. *A/RES/45/95.* 1990, part B principle 4.

The Convention 108 included the special set of data protection rights for individuals (to information, access and rectification).[76] The Convention 108 is influenced by the OECD Guidelines. The Convention 108 put the strong additional safeguards for the data subject[77]by recognizing that any person shall be entitled:

- Right to know the existence of an automated personal data file, its main purposes, as well as the identity and habitual residence or principal place of business of the controller of the file;
- Right to be informed at reasonable intervals and without excessive delay or expense confirmation of whether personal data relating to him are stored in the automated data file as well as communication to him of such data in an intelligible form;
- Right to access and rectification, as the case may be, rectification or erasure of such data if these have been processed contrary to the provisions of domestic law giving effect to the basic principles set out in Articles 5 and 6 of this convention;
- Right to remedy, to have a remedy if a request for confirmation or, as the case may be, communication, rectification or erasure as referred to in paragraphs b and c of this article is not complied with.

The Convention 108 extended protection[78]by emphasize that None of the provisions of this chapter shall be interpreted as limiting or otherwise affecting the possibility for a Party to grant data subjects a wider measure of protection than that stipulated in this convention.

The EU Data Protection Directive 95/46/EC adopted the inalienable substantive rights (information, access, rectification) and introducing a formal, institutional mechanism for monitoring[79] personal data processing in each Member State.[80] The rights of individuals were affirmed by Directive 95/46/EC that it refers to are: [81]

---

[76] De Hert, Paul and Schreuders, Eric. "The Relevance of Convention 108." *Proceedings of the Council of Europe Conference on Data Protection,* Warsaw, 2001, p. 34.

[77] Council of Europe. *Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data Convention108.* 1981, Article 8.

[78] Ibid, Article 11.

[79] The detail of Supervisory Mechanism will be described later in section 2.2.3.1.

- Right to information about when, where, why and how their data be collected and processed;
- Right of access to a copy of the information comprised in their personal data;
- Right to object to processing that is likely to cause or is causing damage or distress;
- Right to prevent processing for direct marketing;
- Right to object to decisions being taken by automated means;
- Right in certain circumstances to have inaccurate personal data rectified, blocked, erased or destroyed; and
- Right to claim compensation for damages caused by a breach of the Directive.

EU Directive 2002/58 on Privacy and Electronic Communications completes the contents of the Right to Personal Data Protection regulating a number of important issues such as confidentiality of information, treatment of traffic data, spam and cookies. The addressees are Member States, who should prohibit listening, tapping, storage or other kinds of interception or surveillance of communication and "related traffic", unless the users have given their consent or conditions have been fulfilled.[82] Furthermore, Directive 2009/136 in 2009, concerns "cookies",[83] that was subject to prior consent of data subject. The content of data protection is for the confidentiality of information to be maintained, "Negative-Right" base approach must be implemented.

These EU norms are complemented with the "Principles on Internet Governance" adopted by the Council of the European Union on 21 September 2011.[84] The

---

[80] Eberlein, Burkard and Newman, Abraham L. "Escaping the International Governance Dilemma? Incorporated Transgovernmental Networks in the European Union." *Governance*, vol. 21, no. 1, 2008, p.40.

[81] EU. *Directive 95/46/EC*. 1995, Articles 10-12.

[82] EU. *Directive 2002/58/EC*. 2002, Article 5.

[83] EU. *Directive 2009/136/EC*. 2009.

[84] Council of the European Union. *Internet governance principles.* 2011, Preamble.

principles on Internet governance[85] recognize the right to respect for private life which must meet the requirements of international law.[86] Some principle in the declaration could be used as an interpretation of Personal Data Protection on Internet because it has the relevant implication with protection of personal data of internet user.

The EU-US Safe Harbor Principles are designed to protect personal data of Data Subject by urging the EU and USA companies to sign-up into the program as long as they bind to the Rights of Individual below:[87]

- **Right to be Noticed** - Individuals must be informed that their data is being collected and about how it will be used. Organizations must notify individuals about the purposes for which they collect and use information about them. They must provide information about how individuals can contact the organization with any inquiries or complaints, the types of third parties to which it discloses the information and the choices and means the organization offers for limiting its use and disclosure.
- **Right to make a Choice** - Individuals must have the option to opt out of the collection and forward transfer of the data to third parties. Organizations must give individuals the opportunity to choose (opt out) whether their personal information will be disclosed to a third party or used for a purpose incompatible with the purpose for which it was originally collected or subsequently authorized by the individual. For sensitive information, affirmative or explicit (opt in) choice must be given if the information is to be disclosed to a third party or used for a purpose other than its original purpose or the purpose authorized subsequently by the individual.
- **Right to Access and Rectification** - Individuals must be able to access information held about them, and correct or delete it if it is inaccurate. Individuals must have access to personal information about them that an organization holds and be able to correct, amend, or delete that information

[85] Even this Declaration is Non-Legal Binding but the Council of the European Union has supplanted the principles into General Data protection Regulation and Umbrella Agreement with US in 2016, as will see in Chapter 4.

[86] Council of the European Union. *Internet governance principles.* 2011, Principle 9 Open network.

[87] EU Commission. *2000/520/EC.* 2000. Annex 1 Safe Harbor Principles.

> where it is inaccurate, except where the burden or expense of providing access would be disproportionate to the risks to the individual's privacy in the case in question, or where the rights of persons other than the individual would be violated.

Safe Harbor Agreement contains individual's rights which are almost asymmetry with Directive 95/46/EC since it was concluded to satisfy the EU market for harmonizing standard of data protection in both sides of Atlantic counterparts. However, the implementation of Safe Harbor is far more complicated than in EU since the US legal system did not provide a constitutional rights relating to personal data protection remedy to Non-US citizen. So it's all on the burden of US organizations to self-certify themselves without the participation of EU citizen and supervisory mechanism. The only concrete compensation or sanction can be imposed to IT Corporation that breach the provision in Safe Harbor Agreement is "delisting" such organization from the verified list.

The instruments recognizing right to personal data had been creating for decades so there is some out-of date provisions maintain in those legal documents. The more advance in technology the more complexity it brought into legal atmosphere. The implementation of data subjects' right to personal data protection is increasingly complicated because the nature of data which is decentralized to various kinds of organizations. Furthermore, there are some inconveniences: data controller/processor has either formal or informal cooperation with regulators; or the conflict of interest comes from the Self-certified system. Hence, the individual's appeal for right recourse is complex as well as the monitoring of duty bearer, data controller/processor, practice.

2.2.1.4. Exception to the exercise of Right to Personal Data Protection

Like other human rights, the right to personal data protection is not absolute; it can be restricted in certain situations and due to other rights. Most often deal with the relationship between state of emergency and personal data protection. The state authorities and courts must on the one hand weigh up the reasons for accessing certain data and, on the other hand, the potential effect on an individual of such state surveillance. A proportionate solution must be provided, in which state/public interests as well as the interests of the data subject are taken into consideration. In liberal democratic societies, organizations who behold

some public position may employ the measure which has negative impact, information being share relating data subject; examples include address, criminal record, religion, ethnic, etc.

In general, there are exceptions under which states could limit the exercise of Right to Personal Data protection in certain restrictions. Using tensions exist between the right to privacy and the right to freedom of expression, for example, when information considered to be private is disseminated through the media. In ICCPR, article 19 (3) provides for restrictions on freedom of expression and information to protect the rights of others and for the protection of national security or of public order (ordre public), or of public health or morals.[88] However, as it happens for all permissible limitations to the right to freedom of expression, the principle of proportionality must be strictly observed, since there is otherwise danger that freedom of expression would be undermined.[89] Particularly in the political arena, not every attack on the good reputation of politicians must be permitted, since freedom of expression and information would otherwise be stripped of their crucial importance for the process of forming political opinions,[90] advocating for transparency and combating corruption The international jurisprudence at regional level indicates that in situations of conflict between privacy and freedom of expression, reference should be made to the overall public interest on the matters reported.[91]

In this regard, the UN Special Rapporteur takes the position that the right to privacy should be subject to the same permissible limitations test as the right to freedom of movement,[92] as elucidated in General Comment 27.[93] The test as expressed in the comment includes, inter alia, the following elements: [94]

(a) Any restrictions must be provided "by the law" (paras.11-12);

(b) The "essence" of a human right is not subject to restrictions (para.13);

---

[88] UN. *International Covenant on Civil and Political Right.* 1966, Article 19.3.

[89] UN. *A/HRC/23/40*. 2013, para. 27

[90] Nowak, Manfred. *United Nations Covenant on Civil and Political Rights: Ccpr Commentary.* Engel, Lancaster, 1993, p.462

[91] Mendel, Toby et al. *Global Survey on Internet Privacy and Freedom of Expression.* UNESCO, Paris, 2012, pp. 53 and 99.

[92] UN. *A/HRC/23/40*. 2013, para. 29

[93] See also UN. *CCPR General Comment No. 34.* 2011.

[94] See also Ibid, paras.11-15.

(c) Restrictions must be "necessary" in a democratic society (para.11);

(d) Any "discretion" exercised when implementing the restrictions must not be unfettered (para.13);

(e) For a restriction to be permissible, it is not enough that it serves one of the enumerated "legitimate aims". It must be necessary for reaching the legitimate aim (para.14);

(f) Restrictive measures must conform to the "principle of proportionality", they must be appropriate to achieve their protective function, they must be the least intrusive instrument amongst those which might achieve the desired result, and they must be proportionate to the interest to be protected (paras.14-15).

By all means of written ICCPR Article17 and 19 combine with Human Rights Committee on Covenant of Civil and Political Rights (CCPR) General Comments, the Personal Data Protection is a part of basic Human Rights for fulfilling Freedom and Human Dignity. It shall not be interfered nor arbitrary limit by any illegitimate exceptions.

Interference with an individual's right to privacy is only permissible under international human rights law if it is neither arbitrary nor unlawful. In its general comment No. 16, the Human Rights Committee explained that the term "unlawful" implied that no interference could take place "except in cases envisaged by the law. Interference authorized by States can only take place on the basis of law, which itself must comply with the provisions, aims and objectives of the Covenant".[95] In other words, interference that is permissible under national law may nonetheless be "unlawful" if that national law is in conflict with the provisions of the International Covenant on Civil and Political Rights. The expression "arbitrary interference" can also extend to interference provided for under the law. The introduction of this concept, the Committee explained, "is intended to guarantee that even interference provided for by law should be in accordance with the provisions, aims and objectives of the Covenant and should be, in any event, reasonable in the particular circumstances".[96] The Committee interpreted the concept of reasonableness to indicate that

[95] Official Records of the General Assembly. *Forty-third Session, Supplement No. 40 (A/43/40)*. 1989, annex VI, para. 3.

[96] Ibid, annex VI, para. 4.

“any interference with privacy must be proportional to the end sought and be necessary in the circumstances of any given case”.[97]

In specific context, the exceptions to the exercise of Right to Personal Data Protection, the United Nations Guidelines for the Regulation of Computerized Personal Data Files provide exceptions to the protection of personal data. In Principle 5 of part A[98] *Power to make exceptions*: exceptions can be made if "necessary to protect national security, public order, public health or morality . . . [and] the rights and freedoms of others . . ." as well as ". . . within the limits prescribed by the International Bill of Human Rights . . ." or other similar documents.

In addition, the European Convention on Human Rights (ECHR) provide more clear definition on “restrictions” as the prescribe in 2nd paragraph of article 8 that no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of: National security, Public safety or The economic well-being of the country, The prevention of disorder or The prevention of crime, The protection of health or The protection of morals, The protection of the rights and freedoms of others. However, The exercise of Right to Privacy by article 8 and Freedom of Expression in article 10 which are interdependence, since it carries with it duties and responsibilities, may be subject to such formalities, conditions, restrictions or penalties as are prescribed by law as well as restrictions on Right to privacy, for preventing the disclosure of information received in confidence, or for maintaining the authority and impartiality of the judiciary.

The Convention 108 made some conditions for exceptions and restrictions[99] that no exception to the provisions of Quality of data, Special categories of data, and Additional safeguards for the data subject shall be allowed except within the compositions defined below. The Derogation from these principles is allowed in specific circumstances only, provided by national law. Exceptions must also constitute necessary measures in a democratic society, “in the interests of protecting nation security, public safety, monetary

---

[97] Human Rights Committee. *Communication No.488/1992 Toonan v Australia*. 1992, para. 8.3; see also Human Rights Committee. *Communications No.903/1999*. 1999, paras.10.1 and 10.2.

[98] UN. *A/RES/45/95.* 1990, part A.

[99] Council of Europe. *Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data Convention108.* 1981, Article 9.

interests or the suppression of criminal offences or the protection of the data subject or the rights and freedoms of others".[100] The Convention does not contain a general exemption for "National" security which vague and vary by State Parties' domestic law.

While the EU Directive 95/46/EC allows Member States may adopt legislative measures to restrict the scope of the obligations and rights when such a restriction constitutes a necessary measure to safeguard:[101] (a) national security; (b) defence; (c) public security; (d) the prevention, investigation, detection and prosecution of criminal offences, or of breaches of ethics for regulated professions; (e) an important economic or financial interest of a Member State or of the European Union, including monetary, budgetary and taxation matters; (f) a monitoring, inspection or regulatory function connected, even occasionally, with the exercise of official authority in cases referred to in (c), (d) and (e); (g) the protection of the data subject or of the rights and freedoms of others. Furthermore, data, which are processed solely for purposes of scientific research or are kept in personal form for a period and does not exceed the period necessary for the sole purpose of creating statistics, can be kept and processed.[102] These conditions were opened for the benefits of scientific development as well as written in the Convention 108.

The Data Retention Directive, more formally Directive 2006/24/EC, make data controller obligation of data retention bases on the objective for "preventing and suppressing crime and terrorism"[103]. This condition provides an opportunity for legal enforcement authority to seek data, kept by data controller/processor, for tracing back to the convicts. The operations approved by such Data Retention Directive may contrary to the full enjoyment of personal data protection because the interpretation of "terrorism" may prolong the time period of collection of some sensitive groups; ethno religious, migrant, international student from some regions.

The Framework Decision 2008/977/JHA, on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters, contains an exception to the purpose limitation principle: the prevention, investigation, detection or

[100] Galetta, Antonella and De Hert, Paul. *A European perspective on data protection and access rights.* Vrije Universiteit, Brussel, 2013, p. 4.

[101] EU. *Directive 95/46/EC.* 1995, Article 13.1.

[102] Ibid, Article 13.2.

[103] EU. *Directive 2006/24/EC.* 2006, Preamble.

prosecution of criminal offences or the execution of criminal penalties, judicial and administrative proceedings directly related to the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, prevention of an immediate and serious threat to public security;[104] to protect public security; to protect national security; prevention of serious harm to the rights of individuals.[105] These exceptions are too wide and could open the loophole for Mass Electronic Surveillance.

The US-EU Safe Harbor is the streamlined protocol for US companies to comply with the EU Directive 95/46/EC on protecting personal data.[106] The procedure was developed by the US Department of Commerce in consultation with the EU. The framework left domestic organizations within the EU or US to self-monitor the store of customer data. So the Safe Harbor Principles are designed to prevent accidental information disclosure or loss by the hand of the Data Controllers/Processors themselves. The EU and USA Data Controller/Processor must be bind by some other laws which have the limitations to individual rights such as National Security conditions in US Patriot Act.

The Safe Harbor Privacy Principles allows US companies to register their certification if they meet the European Union requirements. However, those companies still a subject under US domestic laws; Patriot Act, homeland Security Act and Foreign Intelligence Surveillance Act.[107] Rights of EU citizen are in the realm of US jurisdiction when such data transfer across Atlantic occurs and it may be compromised by the exercise of security laws mentioned above.

Since the goal of human rights is to protect major fundamental freedoms and rights and to create a system that ensures that individuals cannot infringe upon the rights of others. In the field of personal data protection, the legal instrument has set certain exception. In general, state authority practice mandates that any restriction of human rights must be stipulated in law, proportionate and necessary in a democratic society. Laws that are not proportionate and necessary may infringe on human rights, and situations may occur whereby the necessary laws do not exist or are not implemented properly. Those problems can frame

[104] EU. *Council Framework Decision 2008/977/JHA*. 2008, Article 11.

[105] Ibid, Article 17.

[106] U.S. Department of Commerce. *Welcome to the U.S.-EU & U.S.-Swiss Safe Harbor Frameworks*, 9 Oct. 2015.

[107] The problems arise from this set of security laws will be analyzed in section 2.3.

up in relation to internet and IT Corporations: inappropriate laws or a deficient legal framework.

As well as other human rights, the right to personal data protection is not absolute; it can be restricted in certain situations and due to other rights. Most often deal with the relationship between state of emergency and personal data protection. The state authorities and courts must weigh up the reasons for accessing certain data and the potential effect on an individual of such state surveillance. A necessary precondition and proportionate solution must be provided, in which state/public interests as well as the interests of the data subject are taken into consideration. Nonetheless, US companies, most influence IT Corporations, still a subject under US domestic laws. Hence, the rights of Global Neitizen are in the realm of US regime when their data was transferred to US territory or by US entities, and it may be compromised by the exercise of US Government as will be shown in Chapter 3.

2.2.2. Obligation of the Data Controller and Data Processor

The study on individual right reflects the needs of fulfillment from the duty bearer, in this case the Data Controller and Processor. There are 5 points need to be analyzed in order to understand the obligation of Data Controller/Processor. The basic duty of IT Corporation and State Agency to take care of data subject rights will be the first point. When the organizations collect and process personal data they need to meet the principles and conditions which will be scrutinized in second point. Data Security is the main goal of third point since there many instruments urge Data Controller/Processor to set up measure to guarantee the safety and integrity of data when disaster appears. Data Retention is the next point, the time period and purpose to retain data from different instruments be investigated. The last point is the fragmented standard of data protection in different regimes, when first instance data controller want to send data to processor or other data controller, especially when data across State border. All 5 points associate with the policy and practice of IT Corporation and State Authority, since the legal instruments oblige State to create domestic law and mechanism to regulate Data Controller/Processor.

2.2.2.1. Basic Duty of Data Controller and Processor

The intention of this section is to review and evaluate obligations set out for data controller/processor in order to guarantee the right to personal data protection. The basic duty principles stressing by many forms of legal wording, some are different in vocabulary but have the same legal implication. The comprehensive understanding of basic duty requirement will give a bright path to data subjects' full enjoyment of protection. Not only the common but also the differences obligation in vast majority instruments will be reflected below.

The Data Controller and Processor need to provide measures in order to meet ICCPR standard, individual right to personal data protection. As the General Comment No.16 urged member states to implement ICCPR Article 17 to provide guarantee for the right of every person to be protected against arbitrary or unlawful interference with his privacy concretely, It required the State to adopt legislative and other measures to give effect to the prohibition against such interferences and attacks as well as to the protection of this right.[108] The strong opposition to Surveillance is highlighted, whether electronic or otherwise, interceptions of telephonic, telegraphic and other forms of communication, wire-tapping and recording of conversations should be prohibited[109]since the Article 17 of ICCPR mentions of Non-Interference of communication by any means.

The OECD Guidelines Governing, The Protection of Privacy and Transborder Flows of Personal Data[110], had influenced the Convention 108. Moreover, it has pursued the state party to fulfill its provisions in order to boost up the confidence of Internet users and trigger the enlargement of E-Commerce. These principles emphasize two basic duties of data controller:

1) **Openness Principle**: Data controller should adopt general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the

[108] Official Records of the General Assembly. *Forty-third Session, Supplement No. 40 (A/43/40).* 1989, annex VI, para. 1.

[109] Ibid.

[110] It is a Non-Binding Instruments but many member states adopted the principles for drafting their domestic law in order to harmonize with counter-part trade party.

existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller. [111]

2) **Accountability Principle**: A data controller should be accountable for complying with measures which give effect to the principles stated above.[112]

In the United Nations Guidelines for the Regulation of Computerized Personal Data, it urges that every data controller including governmental international organizations and non-governmental international organizations[113] should guarantee the rights of data subjects. Data Controller must acknowledge to data subject that one's data is being used and also guarantees access to that data in an intelligible form. It requires organizations to supply appropriate remedies to rectify unlawful, unnecessary, or inaccurate data[114] for the victim.

The Convention 108, written in Duties of the Parties,[115] requests all the same burdens approved in OECD Guidelines and emphasize that each State Party shall take the necessary measures in its "domestic law" to give effect to the basic principles for data protection set out in this convention.

EU Directive 2002/58 on Privacy and Electronic Communications, the data controller should prohibit listening, tapping, storage or other kinds of interception or surveillance of communication and "related traffic", unless the users have given their consent or conditions have been fulfilled.[116] Moreover, it has prohibiting the use of email addresses for marketing purposes. The Directive establishes the opt-in regime, where unsolicited emails may be sent only with prior agreement of the recipient.[117] This Directive has been minor amended by Directive 2009/136 in 2009, the important principles in the Directive 2009/136/EC, mentioning the regulations regarding cookies as Member States shall ensure

[111] OECD. *Annex to the Recommendation of the Council of Guidelines Governing The Protection of Privacy and Transborder Flows of Personal Data*. 1980, para. 12.

[112] Ibid, para. 14.

[113] UN. *A/RES/45/95.* 14 Dec. 1990, part B.

[114] Ibid, part A principle 4.

[115] Council of Europe. *Convention108.* 1981, Article 4.

[116] EU. *Directive 2002/58/EC.* 2002, Article5.

[117] Ibid, Article13.

that the storing of personal data or the gaining of access to information already stored, in the terminal equipment of a subscriber.[118]

The Data Retention Directive requires Member States to ensure that communications providers, data controller, retain the necessary data as specified in the Directive for a period of between 6 months and 2 years[119] in order to trace and identify the details of a communication.[120] Data Controller must coordinate with the police and security agencies which may request access to details of data subjects' communication.[121]

In EU Directive 95/46/EC on the principle of lawfulness of processing reaffirms that data controllers must stay in line with other legal obligations, even outside of the Directive, regardless of whether these obligations are general, specific, statutory or contractual.[122] The "7 principles Data Protection" are founded by EU Directive 95/46/EC as basic duties of Data Controller:

1) **Notice**: Data Controller shall give notice of such collection to data subjects whose data is being collected. [123]
2) **Purpose**: Data Controller must ensure that data collected would be used only for stated purpose(s) and for no other purposes. [124]
3) **Consent**: Without consent from its subject(s), Data Controller should not disclose or share personal data with third parties.[125]
4) **Security**: Data Controller should keep personal data safe and secure from potential abuse, theft, or loss. [126]

[118] EU. *Directive 2009/136/EC*. 2009, Article 5(3).

[119] EU. *Directive 2006/24/EC.* 2006, Article 6.

[120] Ibid, Article 5.

[121] Ibid, Article 4.

[122] Van Alsenoy, Brendan et al. "Search Engines After'google Spain': Internet@ Liberty or Privacy@ Peril?." 2013, p. 31.

[123] EU. *Directive 95/46/EC.* 1995, Article 18-21.

[124] Ibid, Article 6.

[125] Ibid, Article 7.

[126] Ibid, Articles 16-17.

5) **Disclosure**: Data Controller should inform subjects, whose personal data is being collected, about the party or parties who collect such data. [127]

6) **Access**: Data Controller should grant data subjects accessing to their personal data and allow them to correct any inaccuracies.[128]

7) **Accountability**: Data Controller should be held accountable for adhering to all of these principles by data subjects. [129]

Supplementary, the Council of the European Union has adopted the Principle on Internet governance which relevance with Personal Data Protection on Internet as mention before. It implies the obligation of Service provider that all public and private actors should recognize and uphold human rights in their operations and activities, in the design of new technologies, services and applications. They should be aware of developments leading to the enhancement of, as well as threats to, fundamental rights and freedoms, and fully participate in efforts aimed at recognizing newly emerging rights.[130] Nevertheless, from the perspective of human rights, it merits further discussion as to whether EU secondary data protection legislation imposes a similar obligation on public authorities and private parties. After all, fundamental human rights primarily aim to limit the actions of public authorities in order to protect the activities of private parties, including the processing of personal data, from state interference.[131]

The EU-US Safe Harbor is a procedure for EU and US Data Controller to comply with the EU Directive 95/46/EC on the protection of personal data.[132] The Safe Harbor Principles are designed to prevent personal data breach. The EU and USA companies can opt into the program as long as they adhere to 7 principles.

---

[127] Ibid, Articles 10-11.

[128] Ibid, Article 12.

[129] Ibid, Articles 22-24.

[130] Council of the European Union. *Internet governance principles.* 2011, Principle 1 Human rights, democracy and the rule of law.

[131] Masing, Johannes. "Herausforderungen Des Datenschutzes." *Neue Juristische Wochenschrift*, vol. 65, no. 33, 2012, pp.2305-2306. ; Grimm, Dieter. “Der Datenschutz vor einer Neuorientierung” *Juristenzeitung*, 2013, p.585. cited in Kokott, Juliane and Sobotta, Christoph. "The Distinction between Privacy and Data Protection in the Jurisprudence of the Cjeu and the Ecthr." *International Data Privacy Law*, vol. 3, no. 4, 2013, p.226.

[132] U.S. Department of Commerce. *Welcome to the U.S.-EU & U.S.-Swiss Safe Harbor Frameworks*, 9 Oct. 2015.

These principles[133] can compare to Directive 95/46/EC as present down here:

1) **Notice** - Data Controller must inform Individuals that their data is being collected and about how it will be used. Compatible with Notice Principle of Directive 95/46/EC.

2) **Choice** - Data Controller must grant Individuals to have the option to opt out of the collection and forward transfer of the data to third parties. For sensitive information, affirmative or explicit (opt in) choice must be given if the information is to be disclosed to a third party. Compatible with Consent Principle and Disclosure principle of Directive 95/46/EC.

3) **Onward Transfer** - Transfers of data to third parties (from data controller to data processor) may only occur to other organizations that follow adequate data protection principles. This principle of Safe Harbor Agreement is completely different from Directive 95/46/EC because it gives data subject right to know when their data is transferred. Data Transfer across border can be made only when it meet standard adequacy principle.

4) **Access** - Data Controller must allow Individuals to access information held about them, and correct or delete it if it is inaccurate. Compatible with Access Principle of Directive 95/46/EC.

5) **Security** - Data Controller must make reasonable efforts to prevent loss of collected information. Compatible with Security Principle of Directive 95/46/EC.

6) **Data Integrity** - Data Controller must ensure that data is reliable for its intended use, accurate, complete, and current. Compatible with Purpose Principle of Directive 95/46/EC.

7) **Enforcement** - Data Controller must provide effective means of enforcing these rules in order to assure compliance with the safe harbor principles. It is slightly different from Accountability principle of Directive 95/46/EC because Safe Harbor has delisting and verification system in order to

[133] EU Commission. *2000/520/EC.* 2000, Annex 1 Safe Harbor Principles.

sanction the non-compliance organizations. But both EU directive and Safe Harbor are relied on domestic court to implement those provisions.

The Safe Harbor Privacy Principles allows US Data Controller to register their organization into the verification list if they meet the European Union requirements then they can transfer data of EU citizen back to US territory.

The effectiveness of measures to prevent persons other than the user from accessing the user's stored personal data may affect whether the data are 'personal data' as regards those persons. Therefore, it seems that a key factor will be the effectiveness of the cloud provider's access control system, which typically only allows authenticated and authorized cloud users to use a particular cloud account. By logging into their data system account, the user gains the ability to access and operate on the full set of any personal data stored.[134] However, the effectiveness of access control of national security exceptions is relevance with the existence of any back doors or other means for a service provider to access unencrypted personal data. The indentified data stored in service provider's server, may affect whether the data are "personal data" in the hands of the provider, even if the provider only has limited incidental access to such data. Yet it is worth to skeptic that the utility infrastructure providers who may not know the nature of the data stored in their infrastructure can be presumed as the controller of "unidentifiable information" or not.[135] If there is no mechanism to supervise the compliance of such data controller/processor, the data protection laws could not be applied in full force or indeed at all.

The key deficiency from the old regime came from the ambiguous status of Data Processor. The old status of data processor is as Third Party, Data Processor has no direct obligations as in new regime such as implementing technical and organizational measures, notifying the controller without undue delay of data breaches. This includes appointing a data protection officer - DPO (if required). The obligation of data processor to protect data subject matters are addressed in supply agreements, which is made between data controller and data processor, but the data processor has no duty to data subject.

The basic duty principles stressing by many forms of legal wording, some are different in vocabulary but have the same legal implication. Most data protection instrument

[134] Hon, W Kuan et al. "The Problem of 'Personal Data'in Cloud Computing: What Information Is Regulated?—the Cloud of Unknowing." *International Data Privacy Law*, vol. 1, no. 4, 2011, p. 36.

[135] Ibid, p. 37.

imposes a similar obligation on public authorities and private parties. After all, fundamental human rights primarily aim to limit the actions of public authorities in order to protect the activities of private parties, including the processing of personal data, from state interference. However, the effectiveness of access control of national security exceptions is relevance with the existence of any back doors or other means for a service provider to access unencrypted personal data. Besides, the lack of Privacy by Design and Privacy by Default principles from obligation of Data Controller/Processor is crucial.

2.2.2.2. Condition and Requirement of Data Collection and Processing

Data collection and Data Processing are the core activity of E-Market but many data protection related instruments draw some baselines for Data Controller/Protector to keep up. The study of condition and requirement of such activity may build the practical map for IT Corporation and State Authority to balance either data controller/processor benefits or data subject rights. In many instruments, previous data protection laws have been influencing to the others as will be seen in the common conditions and requirements they contain. Since the state need to build up the framework for interact in single E-Market, the common rule to protect personal data of consumer is needed. Meanwhile the differences among various instruments are also picked up for further understandings, why do they have loopholes in personal data protection, and how to close the gap.

In General Comment No. 16 to the ICCPR[136] provides Conditions and Requirements on data collection and processing under Article 17. It states, among other things, that: [137]

Condition

1) The collection and storage of personal information on computers, in data bases or other devices, whether by public or private bodies, must be regulated by law;

2) Any "interference" with these rights must only take place on the basis of law which must comply with the Covenant."

[136] It was launched in 1988 after the OECD Guidelines 1980 but before UN Guideline 1990.

[137] Official Records of the General Assembly, *Forty-third Session, Supplement No. 40 (A/43/40)*. 1989, annex VI, para. 10.

Requirement

3) States and Data Controller must take effective measures to ensure that information concerning a person's private life does not reach the hands of persons who are not authorized by law to receive, process and use it;

4) Data Controller must prevent the uses of this information for purposes incompatible with the Covenant;

5) Data Controller must provide individuals the right to determine what information is being held about them and for what purposes and to request rectification or elimination of incorrect information;

These conditions and requirements are supplemented by the storing body's duty of "Transparency" with regard to data processing, in particular as regards the provision of information, rectification and elimination as vital data protection principles.[138] This Transparency Principle will be the main pillar for other instruments agreed thereafter.

The OECD Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data was launched in 1980,[139] it highly dominate the latter instruments such as Convention 108. There are principles for data collection and processing found in Part Two attached in the Annex that give conditions and requirements to data processing:

Condition

1) **Collection Limitation Principle**[140]: There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.

2) **Purpose Specification Principle**[141]: The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfillment of those purposes or such

[138] Ibid.

[139] It is a Non-Binding Instruments but many member states adopted the principles for drafting their domestic law in order to harmonize with counter-part trade party.

[140] OECD. *Annex to the Recommendation of the Council of Guidelines Governing The Protection of Privacy and Transborder Flows of Personal Data*. 23 Sep. 1980, para. 7.

[141] Ibid, para. 9.

others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.

Requirement

3) **Data Quality Principle**[142]: Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.

4) **Use Limitation Principle**[143]: Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with Paragraph 9 except: a) with the consent of the data subject; or b) by the authority of law.

The OECD Guidelines have been the first fundamental ground that affirmed necessary principles to the arena so it was covered by the above General Comment 16.

The UN guidelines 1990, in part A, lay out the following principles to provide minimum guarantees of protection when processing personal data:[144]

Condition

1) **Principle of non-discrimination**: Forbids the collection of data "likely to give rise to unlawful or arbitrary discrimination", safe for the exceptions under principle 6, such as national security or crime prevention. Covered data includes "racial or ethnic origin, colour, sex life, political opinions, religious, philosophical and other beliefs as well as membership of an association or trade union.

2) **Principle of the purpose-specification**: Declares the purpose of the data collection to be transparent in order to ensure the data is used only for the specified purpose and that the data is only kept as long as it is needed to achieve the stated purpose.

[142] Ibid, para. 8.

[143] Ibid, para. 10.

[144] UN. *A/RES/45/95.* 1990, part A principle 1-5.

Requirement

3) **Principle of lawfulness and fairness**: Demands fairness and lawfulness in the collection and processing of personal data.

4) **Principle of accuracy**: Puts responsibility on the persons doing the data collection to ensure the data collected is accurate.

5) **Principle of interested-person access**: Data Controller must guarantee the right to know that one's data is being processed and also guarantees access to that data in an intelligible form. It requires appropriate remedies to rectify unlawful, unnecessary, or inaccurate data.

The UN Guideline 1990 is consistent with General Comment 16 and OECD Guideline since it was adopted to fulfill the appliance of those instruments to activity which has been growing very fast since the 1980s.

At European regional level, the Council of Europe Convention 108 includes the Fair Information Principles[145]. It describes the basic conditions and requirements for data processing which are:

Condition

1) **Special categories of data:**[146] Personal data revealing racial origin, political opinions or religious or other beliefs, as well as personal data concerning health or sexual life, may not be processed automatically unless domestic law provides appropriate safeguards. The same shall apply to personal data relating to criminal convictions.

Requirement

2) **Quality of data:**[147] Personal data undergoing automatic processing shall be:

- obtained and processed fairly and lawfully;

[145] De Hert, Paul and Schreuders, Eric. "The Relevance of Convention 108." *Proceedings of the Council of Europe Conference on Data Protection,* Warsaw, 2001, p. 34.

[146] Council of Europe. *Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data Convention108.* 1981, Article 6.

[147] Ibid, Article 5.

- stored for specified and legitimate purposes and not used in a way incompatible with those purposes;
- adequate, relevant and not excessive in relation to the purposes for which they are stored;
- accurate and, where necessary, kept up to date;
- preserved in a form which permits identification of the data subjects for no longer than is required for the purpose for which those data are stored.

The Convention 108 seems like it contains less conditions and requirements but it takes the same main stances as other instruments focused. The smaller number of principle reflects the scope of Convention 108 which emphasizes only "Automatic Processing of Personal Data".

At EU level, the conditions and requirements of data processing are set by the provision of EU Directive 95/46/EC. The EU Data Protection Directive 1995 adopted the Fair Information Principles.[148] Personal data should not be processed at all, except when certain conditions are met. The first data quality principle provides that personal data must be processed '*fairly and lawfully*' (article 6(1)a) of Data Protection Directive). Fairness of processing is considered an overarching (or 'primary'[149]) principle of data protection law. It is a generic principle which has provided the foundation for other data protection requirements. As such, the fairness principle provides a 'lens' through which the other provisions in the Directive should be interpreted.[150] Directive 95/46/EC fall into three categories: transparency, legitimate purpose, and proportionality:

[148] Eberlein, Burkard and Newman, Abraham L. "Escaping the International Governance Dilemma? Incorporated Transgovernmental Networks in the European Union." *Governance*, vol. 21, no. 1, 2008, p. 40.

[149] Bygrave, Lee A. *Data Protection Law: Approaching Its Rationale, Logic and Limits.* Kluwer Law Intl, 2002, p. 58.

[150] Kuczerawy, Aleksandra and Fanny Coudert. "Privacy Settings in Social Networking Sites: Is It Fair?" *IFIP PrimeLife International Summer School on Privacy and Identity Management for Life*, Springer, 2010, pp. 237–238.

Condition

1) **Transparency**, Data may be processed only if at least one of the following is true: [151]

- when the data subject has given his consent.
- when the processing is necessary for the performance of or the entering into a contract.
- when processing is necessary for compliance with a legal obligation.
- when processing is necessary in order to protect the vital interests of the data subject.
- processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed.
- processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject. The data subject has the right to access all data processed about him. The data subject even has the right to demand the rectification, deletion or blocking of data that is incomplete, inaccurate or isn't being processed in compliance with the data protection rules[152].

The principle of "Transparency" is the fundamental ground of the Directive 95/46/EC as well as other instruments confirmed.

2) **Legitimate purpose**, Personal data can only be processed for specified explicit and legitimate purposes and may not be processed further in a way incompatible with those purposes.[153]

[151] EU. *Directive 95/46/EC.* 1995, Article 7.

[152] Ibid, Article 12.

[153] Ibid, Article 6b.

Requirement

3) **Proportionality**, Personal data may be processed only insofar as it is adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed.

- The data must be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that data which are inaccurate or incomplete, having regard to the purposes for which they were collected or for which they are further processed, are erased or rectified; The data shouldn't be kept in a form which permits identification of data subjects for longer than is necessary for the purposes for which the data were collected or for which they are further processed. Member States shall lay down appropriate safeguards for personal data stored for longer periods for historical, statistical or scientific use. [154]
- When sensitive personal data (can be: religious beliefs, political opinions, health, sexual orientation, race, membership of past organisations) are being processed, extra restrictions apply. [155]
- The data subject may object at any time to the processing of personal data for the purpose of direct marketing. [156]
- A decision which produces legal effects or significantly affects the data subject may not be based solely on automated processing of data.[157] A form of appeal should be provided when automatic decision making processes are used.
- The controller must notify the supervisory authority before he starts to process data.[158]

[154] Ibid, Article 6.

[155] Ibid, Article 8.

[156] Ibid, Article 14.

[157] Ibid, Article 15.

[158] Ibid, Article 19.

The open-ended nature of the fairness principle seems to place a general obligation on controllers to act in a responsible way. This requirement becomes particularly relevant in situations where the extent to which data subjects can exercise control over the processing is limited (e.g., because of a significant power imbalance between controllers and subjects, because of the complexity of processing, etc.).[159]

EU Directive 2002/58 on Privacy and Electronic Communications, It deals with the regulation of data processing issues. When data relating to location of users or other traffic can be processed, only be permitted if such data is anonymized, when users have given consent, or for provision of value-added services. User must be informed beforehand of the character of information collected and have the option to opt out.[160] The EU Cookie Directive "Directive 2009/136/EC" is an amendment of the Directive 2002/58/EC, mentioning the regiulations regarding the purposes of the processing.[161] User consent is the priority condition that the subscriber or controller must concern. This shall not prevent any technical storage or access for the sole purpose of carrying out the transmission of a communication over an electronic communications network, the strict necessary in order for the provider of an information society service explicitly requested by the subscriber or user to provide the service.[162]

At EU-US level, the transfer of processed personal data between the EU and the U.S. for commercial purposes are addressed by the Safe Harbor Decision[163] which provides a legal basis for integrity of personal data from the EU to companies in the U.S. which adhere to the these principles:[164] *Data Integrity*, Data must be relevant and reliable for the purpose it was collected for. Personal information must be relevant for the purposes for which it is to be used. An organization should take reasonable steps to ensure that data is reliable for its intended use, accurate, complete, and current. The Safe Harbor had absorbed the conditions and requirements contained in Directive 95/46/EC due to its original function

[159] Van Alsenoy, Brendan et al. "Search Engines After'google Spain': Internet@ Liberty or Privacy@ Peril?." 2013, p. 31.

[160] EU. *Directive 2002/58/EC.* 2002, Article9.

[161] Ibid, Article5(3).

[162] EU. *Directive 2009/136/EC*. 2009, Article5(3).

[163] EU Commission. *2000/520/EC.* 2000, Preamble.

[164] Ibid, Annex 1 Safe Harbor Principles.

as adequacy decision to meet EU standard but the implementation is upon the US legal system.

The conditions and requirements of data processing are set by the provision of various instruments. There are many coherence requirements and conditions on data processing and collection from diverse instruments. These coherences had been initiated into written legal documents relating to personal data protection for harmonization reason. The Fair Information Principles, Fairness of processing is considered primary principle of data protection law. Personal data should not be processed at all, except when certain conditions are met. The first data quality principle provides that personal data must be processed "*fairly and lawfully*". It is a generic principle which has provided the foundation for other data protection requirements. As such, the fairness principle provides a 'lens' through which the other provisions in the Directive should be interpreted. However, there are some differences make the harmonization unaccomplished especially the differences from preventing and suppressing crime and terrorism which will further analyzed in section 2.2.2.4. Additionally, it is harder to use old data protection regime to regulate the out-paced technology. The up-to-date understanding and the new initiative may give the method to answer customer's trust-concerning question in the near future. Since the creation of Single E-Market needs the harmonized legal framework on personal data protection for assuring customer trust.

2.2.2.3. Data Security

There are needs to secure the data system because processed personal data is collected and transferred in and out of the system all the time. A great numbers of data subjects are involve with the protective measures of the data controller. IT Corporation and State Authority who gather personal data are obliged to the universal, regional and bilateral agreements for maintaining the safety of the data collections. Nevertheless, the instruments can only give principles for State to commit while the front-line defenders are private company or state agency in the field, directly control filing system. Due to the absent of International internet security law or even International Cybercrime treaty, the cooperation among State Parties of Treaty or Member States of legal instruments are very crucial. The consistence of data security standards could affect the efficiency of personal data protection when facing against any threats or risks.

The United Nations adopted General Assembly resolution 45/95 on December 14, 1990. The resolution, Guidelines for the Regulation of Computerized Personal Data Files lay out the following *Principle 7 on security*[165]: Requires protection of the data from natural disasters and human dangers like theft or misuse including unauthorized access, fraudulent misuse of data or contamination by computer viruses. This resolution can be traced back from the OECD Guidelines Governing the Protection of Privacy and Trans-border Flows of Personal Data, on Security Safeguards Principle.[166] The OECD Guidelines was again recognized by UNGA as will be mentioned below. The Guidelines said Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification or disclosure of data.

The United Nations General Assembly adopted a resolution based on the Security Guidelines of OECD at the 78th plenary meeting 20 December 2002.[167] Their principles are a widely recognized international policy standard. The Guidelines were also reflected in various regional organizations such as the Council of the European Union Resolution on a European Approach towards a culture of network and information security and the Asia-Pacific "Strategy to Ensure Trusted, Secure and Sustainable Online Environment".[168] Finally, the Guidelines' principles are annexed to ISO 27001 Information Security Management System standard[169] which "provides a robust model for implementing the principles in those Guidelines".

[165] UN. *A/RES/45/95.* 1990, part A.

[166] OECD. *Annex to the Recommendation of the Council of Guidelines Governing The Protection of Privacy and Transborder Flows of Personal Data*. 23 Sep. 1980, para. 11.

[167] UN. *A/RES/57/239*. 2003.

[168] APEC. *Privacy Framework*. 2005, http://www.apec.org/Groups/Committee-on-Trade-and-Investment/~/media/Files/Groups/ECSG/05_ecsg_privacyframewk.ashx. Accessed 15 Oct. 2015. The APEC Member Economies include Australia; Brunei Darussalam; Canada; Chile; the People's Republic of China; Hong Kong, China; Indonesia; Japan; the Republic of Korea; Malaysia; Mexico; New Zealand; Papua New Guinea; Peru; the Republic of the Philippines; the Russian Federation; Singapore; Chinese Taipei; Thailand; the United States; and Vietnam.

[169] ISO. *ISO/IEC 27001*. 2005, Annex.

The Data Security Principles, which were recognized by both UNGA resolution and OECD Guidelines as mentioned above, are described in Part III. PRINCIPLES which consist of: [170]

1) **Awareness Principle**: In order to foster confidence in information systems, owners, providers and users of information systems and other parties should readily be able, consistent with maintaining security, to gain appropriate knowledge of and be informed about the existence and general extent of measures, practices and procedures for the security of information systems.

2) **Responsibility Principle**: The responsibilities and accountability of owners, providers and users of information systems and other parties concerned with the security of information systems should be explicit.

3**) Response Principle**: Public and private parties, at both national and international levels, should act in a timely coordinated manner to prevent and to respond to breaches of security of information systems.

4) **Ethics Principle**: Information systems and the security of information systems should be provided and used in such a manner that the rights and legitimate interests of others are respected.

5) **Democracy Principle**: The security of information systems should be compatible with the legitimate use and flow of data and information in a democratic society.

6) **Risk Assessment Principle**: Measures, practices and procedures for the security of information systems should encompass key internal and external factors, such as technology, physical and human factors, policies and third-party services with security implications. Because of the growing interconnectivity of information systems, risk assessment should include consideration of the potential harm that may originate from others or be caused to others.

7) **Security Design Principle**: Measures, practices and procedures for the security of information systems should be coordinated and integrated with each other and with other measures, practices and procedures of the organization so as to create a coherent system of security.

---

[170] OECD. *Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security*. OECD Publishing, 2002, pp. 10-12.

8) **Security Management Principle**: Security levels, costs, measures, practices and procedures should be appropriate and proportionate to the value of and degree of reliance on the information systems and to the severity, probability and extent of potential harm, as the requirements for security vary depending upon the particular information systems.

9) **Reassessment Principle**: The security of information systems should be reassessed periodically, as information systems and the requirements for their security vary over time.

At European level, the Council of Europe Convention 108 give a guarantee for Data security[171] by mention that Data Controller/Processor must procure the appropriate security measures for the protection of personal data stored in automated data files against accidental or unauthorized destruction or accidental loss as well as against unauthorized access, alteration or dissemination.[172]

While in EU the EU Directive 95/46/EC urges Member States to secure of data processing by employ guarantee measures:[173]

1) Controller must implement appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

2) Controller must choose only a processor who providing sufficient guarantees in respect of the technical security measures and organizational measures governing the processing to be carried out, and must ensure compliance with those measures.

3) The carrying out of processing by way of a processor must be governed by a contract or legal act binding the processor to the controller.

This provision of Directive 95/46/EC has shown the advantage point as it requires data controller to protect the integrity of personal data to all "Life-Cycle" of data

[171] Council of Europe. *Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data Convention108.* 1981, Article 7.

[172] Galetta, Antonella and De Hert, Paul. *A European perspective on data protection and access rights.* Vrije Universiteit, Brussel, 2013, p. 4.

[173] EU. *Directive 95/46/EC.* 1995, Article 17.

processing. But the data subject still does not entitle to claim their right directly to data processor. Only the data controller can regulate the data processor by using legal binding contract between them.

Due to the security of personal data transfer between the EU and the U.S. for commercial purposes are ensure by the Safe Harbor Decision[174], it complies with the EU Directive 95/46/EC on the protection of personal data.[175] The Safe Harbor Principles are invented, designed and established to prevent accidental information expose or damage. EU and USA Data Controller/Processor can opt into the program as long as they adhere to the *Security Principle*.[176] The Data Controller/Processor must make reasonable efforts to prevent loss of collected information. Organizations must take reasonable precautions to protect personal information from loss, misuse and unauthorized access, disclosure, alteration and destruction.

The challenge to data security comes from the disaster made by the hand of human[177]due to the penetration to data system in pursuance of data surveillance and monitor on the basis of terrorism prevention and crime suppression. The common security challenges will be shifted from national to international level because of the nature of internet. However, the old regime put heavy burden to national data protection authorities to supervise private actors whether they have developed an appropriate precautionary measure to meet the requirement. There is another urgent need to provide preparatory and support advice to national data protection authorities in order to meet these challenges[178] especially when there are wide spread of massive electronic data surveillance worldwide. Whereas the filling system administrator has many burdens to undertake to meet with the security protocol, the incompetence to monitor the act of data controller stills remained. The more solid legal obligation to secure the system is in demand for defending infiltration.

---

[174] EU Commission. *2000/520/EC.* 2000, Preamble.

[175] U.S. Department of Commerce. *Welcome to the U.S.-EU & U.S.-Swiss Safe Harbor Frameworks*, 9 Oct. 2015.

[176] EU Commission. *2000/520/EC.* 2000, Annex 1 Safe Harbor Principles.

[177] The data breach destroy the security of data system will be discussed in Chapter3.

[178] Boehm, Franziska. "Confusing Fundamental Rights Protection in Europe: Loopholes in Europe's Fundamental Rights Protection Exemplified on European Data Protection Rules." *University of Luxembourg, Law Working Paper Series, Paper no. 2009-01,* 2009., p. 17.

2.2.2.4. Data Retention

There are needs of personal data collection to create data base that can trace back to individual who may be convicted as a criminal or a terrorist. The demand of legal enforcement authority, to pursuit personal data to fulfill their duty, reflects in the cooperation with IT Corporation. From the flourishing of internet, as the popular medium for communicating and spreading ideas, the governmental agency put their request in a form of data retention clause. This section will investigate the instruments in domestic, regional and international levels as provision of data retention is a part of many data protection instruments. Since the time period, purpose and conditions of collecting the personal data are the main issue of data controller/processor obligation. The bigger collection and longer period to be kept the more risky of data breach it may happen. Thus, the study on the scope and condition of data retention may elucidate the vulnerable point which might occur from arbitrary and unnecessary retention of data. The most important characteristic of data retention functions in a form of relationship between state authority and data controller/processor regardless their legal status; private organizations, public agencies, or level of relations; domestic, regional and international. The solid scope and condition of data retention will balance the full enjoyment of right to personal data and the effectiveness of legal enforcement.

In practice, data retention, involves the storage of information, whether personally identifiable or not, for specified or unspecified "periods of time". Data Retention is a form of surveillance and depends on the technologies they involve; these types include watching, listening, locating, detecting, and personal data monitoring ("dataveillance").[179]

Data retention is intrinsically involved with surveillance, more precisely to data surveillance, since it enables states to collect data related to their citizens' activities and to use these data to understand and control or assist the subjects of monitoring.[180] The retention of traffic and location data perfectly meets the definition of surveillance as presented by David Lyon: "a focused, systematic, and routine attention to personal details in

[179] Raab, Charles D and Jones, Richard. *A report presenting a review of the key features raised by the political perspectives of surveillance and democracy*. 2013, p. 38.

[180] Roberts, Hal and John Palfrey. "The Eu Data Retention Directive in an Era of Internet Surveillance." *Access controlled: The shaping of power, rights, and rule in cyberspace*, 2010, p. 35.

the end to individuals for the purposes of influencing and protecting those whose data have been garnered".[181]

The observation of Internet activities represents a uniquely powerful form of surveillance, since the web provides multiple spaces for individuals to be engaged in personal activities: contacting each other, sharing personal ideas, engaging in business transactions, shopping, etc.[182] European data retention law does not allow the retention of the content of communications,[183] and "only" location records and traffic data are to be stored;[184] these can be used for creating clear tracking profiles of targeted persons.[185]

There are no specific universal instruments which contain the provision of data retention not even UDHR and ICCPR. Unless, there are negative clauses contain in the UN Guidelines for the Regulation of Computerized Personal Data Files which allow state authority to limit the full enjoyment of personal data protection in emergency situations; national security, public safety, morality…or protect others' rights etc.. The most likely provision is the basic duties of data controllers to collect data for legitimate purposes.

In regional level, the ECHR has the same standard as mentioned above in international level. Whereas, the Convention 108 give more concrete provision relating to data retention but does not extend *Quality of Data* principle[186] beyond the "specified and legitimate purposes" clause. Moreover, state authority must give reasonable claim that meet the conditions of restriction lay down in *Restrictions and Exceptions* principle[187] such as state

[181] Lyon, David. *Surveillance Studies: An Overview*. Polity Press, Cambridge, 2007, p. 14.

[182] Huey, Laura and Richard Rosenberg. "Watching the Web: Thoughts on Expanding Police Surveillance Opportunities under the Cyber-Crime Convention." *Canadian Journal of Criminology and Criminal Justice*, vol. 46, no. 5, 2004, p. 603.

[183] Mitrou, Lilian. "The Impact of Communications Data Retention on Fundamental Rights and Democracy: The Case of the Eu Data Retention Directive." *Haggerty/Samatas*, 2010, p. 129.

[184] Rauhofer, Judith. "Just Because You're Paranoid, Doesn't Mean They're Not after You: Legislative Developments in Relation to the Mandatory Retention of Communications Data in the European Union." *SCRIPTed*, vol. 3, 2006, pp. 323-4.

[185] Farrell, Maria. "Communications data retention in the UK." *E-commerce Law and Policy*, Vol. 3, 2001, p. 11.

[186] Council of Europe. *Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data Convention108*. 1981, Article 5.

[187] Ibid, Article 9.

security or the suppression of criminal offences. In addition, those restrictions, for retention the personal data, need to be provided by the law.

On the contrary, at EU level data retention has been specifically regulated. The first mention can be found in EU Directive 2002/58 on Privacy and Electronic Communications. The directive obliges the providers of services to erase or anonymise the traffic data processed when no longer needed, unless the conditions have been fulfilled. Retention is allowed for billing purposes but only as long as the statute of limitations allows the payment to be lawfully pursued. Data may be retained upon a user's consent for marketing and value-added services. For both previous uses, the data subject must be informed why and for how long the data is being processed.[188]

Later, a very different perspective has been introduced in the Data Retention Directive, more formally "Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC" was a Directive issued by the European Union and related to telecommunications data retention.[189]

Directive requires Member States to ensure that communications providers retain the necessary data as specified in the Directive for a period of between 6 months and 2 years[190] in order to:[191]

- Trace and identify the source of a communication;
- Trace and identify the destination of a communication;
- Identify the date, time, and duration of a communication;
- Identify the type of communication;
- Identify the communication device;
- Identify the location of mobile communication equipment.

[188] EU. *Directive 2002/58/EC.* 2002, Article 15.

[189] Ibid, Preamble.

[190] Ibid, Article 6.

[191] Ibid, Article 5.

Under the directive the police and security agencies will be able to request access to details such as IP address and time of use of every email, phone call and text message sent or received.[192] A permission to access the information will be monitored by Supervisory Authority.[193]

Given the wide scale of data surveillance tools existing today in the EU surveillance regime, the Data Retention Directive of 2006 has given rise to the most intense controversy. Until 2004 the issue of a common approach for countering organized crime and terrorism did not gain prominence on the EU policy agenda.[194]

The EU was reluctant to harmonize the diverging data retention regimes until 2004 despite external pressure. The radical change was triggered by the terrorist bombing attacks in Madrid and London that directed lawmakers' attention to EU mechanisms for the intensification of the collection, storage and exchange of personal data.[195] Adopting the Directive in 2006 was a direct legal manifestation of this attempt. The main point of its adoption was the standardization of national regulations of the way in which traffic data are stored by Communication Service providers (CSPs). By choosing the form of a Directive from the range of possible legally binding instruments, lawmakers provided considerable leeway for Member States in implementing the mandatory data retention requirements. The Directive obliges telephony suppliers and Internet Service Providers (ISPs) to retain, for up to 2 years, communication traffic and location data, and information about subscribers, for the purposes of investigating, detecting and prosecuting serious crime.[196]

The traffic and location records might be quite important in law enforcement procedures by providing key information both for detecting organized crime activities and for granting evidences of guilt (or even innocence) before the courts. Indeed, it is without doubt

[192] EU. *Directive 2006/24/EC.* 2006, Article 4.

[193] Ibid, Article 9.

[194] Flynn, Cathal. "Data Retention, the Separation of Power in the Eu and the Right to Privacy: A Critical Analysis of the Legal Validity of the 2006 Directive on the Retention of Data." *UC Dublin L. Rev.*, vol. 8, 2008, p. 1.

[195] Konstadinides, Theodore. "Destroying Democracy on the Ground of Defending It? The Data Retention Directive, the Surveillance State and Our Constitutional Ecosystem." *European Law Review*, vol. 36, 2011, pp. 722-4.

[196] Raab, Charles D and Jones, Richard. *A report presenting a review of the key features raised by the political perspectives of surveillance and democracy*. 2013, p. 41.

that these records might play an especially important role in identifying criminals, especially those who use screen names or pseudonyms on the Internet.[197] Nonetheless, there are massive doubts have been raised about the reliability of the retained data by non-oversight authority or company.

The EU instrument for the protection of personal data in the areas of police and judicial cooperation in criminal matters is the Framework Decision 2008/977/JHA. The Framework Decision is an important step forward in a field where common standards for data protection were very much needed. However, further work needs to be done until meeting on 27-29 November 2008[198] and the final text was published on the Official Journal as the Council Framework Decision 2008/977/JHA.

The Framework Decision only applies to the cross-border exchange of personal data within the EU and not to domestic processing operations in the Member States. This distinction is difficult to make in practice and can complicate the actual implementation and application of the Framework Decision.[199]

Also, the Framework Decision 2008/977/JHA contains too wide an exception to the purpose limitation principle.[200] Another shortcoming is the lack of provisions that different categories of data should be distinguished in accordance with their degree of accuracy and reliability, that data based on facts should be distinguished from data based on opinions or personal assessments,[201] and that a distinction should be made between different categories of data subjects (criminals, suspects, victims, witnesses, etc.), with specific guarantees laid down for data relating to non-suspects.[202]

---

[197] Solove, Daniel J. "Reconstructing Electronic Surveillance Law." *Geo. Wash. L. Rev.*, vol. 72, 2003, p. 1284.

[198] EU. *Council Framework Decision 2008/977/JHA*. 2008, p. 60.

The Framework Decision only envisages minimum harmonisation of data protection standards.

[199] This distinction does not exist in the relevant Council of Europe instruments such as: Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (CETS No.: 108), its Additional Protocol regarding supervisory authorities and transborder data flows (ETS No.: 181) and Recommendation No R (87) 15 of the Committee of Ministers to Member States regulating the use of personal data in the police sector, adopted on 17 September 1987.

[200] As mention in section 2.2.1.4.

[201] As required by Principle 3.2 of Recommendation No R (87) 15.

[202] Contrary to Principle 2 of Recommendation No R (87) 15 and its evaluation reports.

In addition the Framework Decision does not replace the various sector-specific legislative instruments for police and judicial co-operation in criminal matters adopted at EU level[203], in particular those governing the functioning of Europol, Eurojust, the Schengen Information System (SIS) and the Customs Information System (CIS)[204], which either contain particular data protection regimes, and/or which usually refer to the data protection instruments of the Council of Europe. For activities within the area of police and judicial cooperation all Member States have subscribed to the Council of Europe Recommendation No R (87) 15, which sets out the principles of Convention 108 for the police sector. However, this is not a legally binding instrument.

This situation may directly affect the possibilities for individuals to exercise their data protection rights in this area (e.g. to know what personal data are processed and exchanged about them, by whom and for what purpose, and on how to exercise their rights, such as the right to access their data).

The Framework Decision is thus applicable to cross-border exchanges of personal data within the framework of police and judicial cooperation. The instrument contains rules applicable to onward transfers of personal data to third countries and to the transmission to private parties in Member States. The decision also allows the EU states to have higher-level safeguards for protecting personal data than those established in this act.

The outcome of the introduction of data retention rules in terms of their intended and unintended costs has led to widespread European criticism from many different groups and for many different reasons. Central to these criticisms, the questions of necessity and proportionality of the mandatory storage of all traffic and location data relating all EU individuals in the European Union especially for such a long time that is prescribed by the Data Retention Directive (6-24 months).[205]

---

[203] See an overview of such instruments in the Commission Communication 'Overview of information management in the area of freedom, security and justice' - COM(2010) 385.

[204] Joint Supervisory Authorities have been set up by the relevant instruments to ensure data protection supervision, in addition to the general supervisory powers of the European Data Protection Supervisor (EDPS) over Union institutions, bodies, offices and agencies based on Regulation (EC) No 45/2001.

[205] Raab, Charles D and Jones, Richard. *A report presenting a review of the key features raised by the political perspectives of surveillance and democracy*. 2013, p. 43.

The pervasive surveillance performed by data retention changes individuals' social behaviour, jeopardizes their autonomous decision-making, discourages their participating in public debate, and chills their personal activities. Data retention may result in all the potential harms that are associated with privacy invasive tools in general in the academic literature.[206] The practical experience of the implementation of the Directive led even the European Data Protection Supervisor itself to conclude that the Directive is "the most privacy invasive instrument ever adopted by the European Union."[207]

The negative impacts of data retention on freedoms of expression and the press are also suggested. Traffic data can easily be misused to spy on journalists and to expose their sources and whistleblowers. What makes matters worse from this perspective is the lack of guarantees of high data security in order to guard against misuses.[208]

The Data Retention Directive 2006 may negatively impact upon competition and other economic policies in the EU by leading consumers to use international webmail services (that is, non-EU providers), and new (and even existing) market participants to take their businesses elsewhere. In all, Maria-Helen Maras found the Directive a disproportionate measure.[209] On 8 April 2014, the Court of Justice of the European Union declared the Directive "invalid" in response to a case brought by Digital Rights Ireland against the Irish authorities and others.[210] Afterward, the EU needs to re-initiate a new Directive of Data Retention since the old one was invalidated by Court decision. The progression of drafting new directive will be described in the Chapter 4 on "New Umbrella Agreement 2016"[211] which has been launched in 2016.

At EU-US level, in 23 November 2009, the EU and US High Level Contact Group (HLCG) have agreed to launch Report on information sharing and privacy and

[206] Newland, Erica and Wong, Cynthia. "Data Retention Mandates: A Threat to Privacy, Free Expression, and Business Development." *Center for Democracy & Technology*, Washington, DC, 2011.

[207] Hustinx, Peter. "The Moment of Truth for the Data Retention Directive." Presentation at The 'Taking on the Data Retention Directive'Conference, Brussels, 2010.

[208] Institute, Forsa. "Opinions of citizens on data retention." 2 Jun. 2008, www.vorratsdatenspeicherung.de/content/view/228/79/. Accessed 21 Apr. 2014.

[209] Maras, Marie-Helen. "The Economic Costs and Consequences of Mass Communications Data Retention: Is the Data Retention Directive a Proportionate Measure?" *European Journal of Law and Economics*, vol. 33, no. 2, 2012, pp. 447-472.

[210] This case will be further discussed and analyzed in Chapter 3.

[211] EU. *The Umbrella Agreement*. 2016.

personal data protection. The Report consist of 12 principles relate to EU Directive on Data Protection 1995, the principles' text of which is attached as an annex to this report, define the following privacy and personal data protection requirements in 12 issues: [212]

1) Purpose Specification/Purpose Limitation;
2) Integrity/Data Quality;
3) Relevant and Necessary/Proportionality;
4) Information Security;
5) Special Categories of Personal Information (sensitive data);
6) Accountability;
7) Independent and Effective Oversight;
8) Individual Access and Rectification;
9) Transparency and Notice;
10) Redress[213];
11) Automated Individual Decisions;
12) Restrictions on Onward Transfers to Third Countries.

In response to the final report from the High-Level Contact Group, the European Data Protection Supervisor suggested a number of principles that should guide an EU–US sharing agreement. Most were at least partially included in the European Commission negotiating mandate, but some remain controversial with the US government:[214]

[212] EU-US HLCG. *Annex to Final Report by EU-US High Level Contact Group on information sharing and privacy and personal data protection.* 2009.

[213] However, both EU and U.S. made a reservation on the principle 10 Redress until very last minute of negotiation, and this reservation give impact on the negotiation on New Umbrella Agreement Since both parties have spent long time to find a common ground on International Dispute Resolution Unit and procedure.

[214] EU-US HLCG. *Opinion of the European Data Protection Supervisor on the Final Report by the EU-US High Level Contact Group on information sharing and privacy and personal data protection.* 8 Nov. 2011.

- Clarification as to the nature of the instrument, which should be legally binding in order to provide sufficient legal certainty;
- A thorough adequacy finding, based on essential requirements addressing the substance, specificity and oversight aspects of the scheme. The EDPS considers that the adequacy of the general instrument could only be acknowledged if combined with adequate specific agreements on a case by case basis.
- A circumscribed scope of application, with a clear and common definition of law enforcement purposes at stake;
- Precisions as to the modalities according to which private entities might be involved in data transfer schemes;
- Compliance with the proportionality principle, implying exchange of data on a case by case basis where there is a concrete need;
- Strong oversight mechanisms, and redress mechanisms available to data subjects, including administrative and judicial remedies;
- Effective measures guaranteeing the exercise of their rights to all data subjects, irrespective of their nationality;
- Involvement of independent data protection authorities, in relation especially to oversight and assistance to data subjects.

While Private companies and State Authorities must comply with security maintaining obligation, State Parties in these treaties must guarantee, through the police, courts, criminal law, etc., the adequate implementation of those treaties.

As the analysis throughout this section shows, there are controversial arguments from either side of the debates. The legal enforcement authority demands greater capacity to detain and trace back the data, while human rights advocates appeal for strict condition and tighten scope. Furthermore, the requirement of power to manipulate data controller organization from the State Authority brings some concerns to many personal data protection organization so they urge for independent oversight on relationship between state authority and data controller/processor. Another problem comes from the practical situation

that most of IT Corporations are American organization and under the mandate US State Authorities.[215] The old regime has not provided durable shield to protect the full enjoyment of data subject rights. To achieve the full integrity of data protection, the solid legal instrument which contain enough preventive measure, supervisory mechanism and stricter restrictive clause, are required.

2.2.2.5. Data Transfer

Internet creates prominent effects to Modern Law because of its transcendence nature, one action across different jurisdictions produce multiple legal consequences. Harmonizing data transfer standard is necessary for constructing Single E-Market space as the priority step. To achieve this goal, many International Economic Organizations, Regional organization and Bilateral Inter-Parties agreements have adopted data transfer principle base on different legal theories. The Adequacy principle and Accountability principle are legal menifestions which were adapted into instruments. The Adequacy principle requires States to lift up their domestic law to meet the standard otherwise they may face countermeasure. While Accountability principle urges States to monitor their legal entities, whether they comply national law of their head quarter, when act aboard. The contrasting approaches can pursue peculiar state implementation so the design of data transfer laws can determine the progression of Single E-market project.

In General Comment No. 16 to the ICCPR, it provides specification on data protection requirements under Article 17. The Comment longs for taking care of the possible violation by Third-party, the Private entities. States parties are under a duty themselves not to engage in interferences inconsistent with article 17 of the Covenant and to provide the legislative framework prohibiting such acts by natural or legal persons.[216] As the rise of Data Processing has been developing by Transnational IT Corporation so the vulnerable groups, whose personal data may be breached, are not just a people under Totalitarian State Regime but also the customers of those Private Actor. Then United Nations adopted General Assembly resolution 45/95 in 1990. This resolution, Guidelines for the Regulation of Computerized Personal Data Files, guarantees of protection for personal data. In part A**,**

[215] The problems come from US system will be described later in section 2.3.

[216] Official Records of the General Assembly, *Forty-third Session, Supplement No. 40 (A/43/40)*. 1989, annex VI, para. 9.

Trans-border data flows, only allowed for free circulation between countries when those countries have "comparable safeguards for the protection of privacy."[217]

The fundamental right to personal data protection recognized by the General Agreement on Trade of Services (GATS) of WTO. It provides the protection of personal data of individuals in relation to the processing and dissemination of personal data that remain governed by Article XIV of the GATS. The trade and investment in Service Sectors especially the Telecommunication and Financial services might be confronted with certain national requirements realizing a specific degree of confidentiality; in particular, the technical security of communications is an indispensable element of any transaction.[218] Otherwise the Service Providers from non-adequate criterion State may face non-tariff measure against them such as restrict of market access. The absent of compliance by State or IT Corporation lead to the prohibition of data transfer to such territory. However, it stresses that member party data protection legislation cannot be deemed an 'arbitrary or unjustifiable discrimination' in the application of Article XIV of the GATS. So the domestic data protection law must base on the standard of relevant data protection instruments; OECD, UN Guidelines etc.

The first global instrument that influenced later international laws is OECD Guideline 1980 Part Five listed a series of recommendations to member countries (for instance, to make known among them details of their observance of the Guidelines, to introduce simple procedures for trans-border data flows, etc.), which aimed to facilitate transnational information exchanges but from a national law point of view[219] by making cooperation among state members. At the time the OECD Guidelines were approved, trans-border data flows were typically understood to refer to point-to-point transfers such as the 'exchange of internal company administrative information, response to requests for service by customers, and maintenance of records concerning or describing customers or subjects'[220]. By contrast, many trans-border data flows today involve multiple computers communicating

[217] UN. *A/RES/45/95.* 1990, part A.

[218] WTO. *GATS.* 1995, Article XIV: General Exceptions.

[219] Wright, David et al. "Are the Oecd Guidelines at 30 Showing Their Age?" *Communications of the ACM,* vol. 54, no. 2, 2011, pp. 119-127.

[220] Carroll, J M. "The Problem of Transnational Data Flows." *Policy issues in data protection and privacy, Proceedings of the OECD seminar,* vol. 24, 1974, p. 201.

through a network in a distributed fashion[221] (As known as 'Web 2.0', online social networking, search engines, and cloud computing).

At European regional apparatus, the Council of Europe Convention 108 lead the world by launching the first Legal-Binding International Instrument, regulates data transfer across border of state party and a baseline for Trans-Atlantic data transfer. The Convention has an important role to protect Trans-border flows of personal data and propose an implementation to state member domestic law[222]. The Protection of transfer across national borders obliges whatever medium, of personal data undergoing automatic processing or collected with a view to their being automatically processed. By employing Accountability Principle, a Party shall not prohibit or subject to special authorization trans-border flows of personal data going to the territory of another Party. Party shall be entitled to derogate from the above obligation unless:[223]

1) its legislation includes specific regulations for certain categories of personal data or of automated personal data files except where the regulations of the other Party provide an equivalent protection;

2) when the transfer is made from its territory to the territory of a non-Contracting State through the intermediary of the territory of another Party.

These exceptions are up-to-date because the communication via internet, across border right away and massively, makes it hard to prepare for each transfer. Moreover, the regulation on . Nevertheless, there are many territories involve in one single communication as data controller may send the personal data to data processor in Non-State Party territory so the guarantee of protection in all step of data life cycle might be impossible.

In the EU, the EU Directive 95/46/EC created International Standard through its *adequacy* criterion.[224] In this way, the EU has triggered the introduction of data protection legislation to several third countries that wish to do business with it. [225]

---

[221] Kuner, Christopher. "Regulation of Transborder Data Flows under Data Protection and Privacy Law: Past, Present, and Future." *TILT Law & Technology Working Paper No. 016/2010*, 2010, p. 10.

[222] Council of Europe. *Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data Convention108.* 1981, Article 12.

[223] Ibid.

[224] Eberlein, Burkard and Newman, Abraham L. "Escaping the International Governance Dilemma? Incorporated Transgovernmental Networks in the European Union." *Governance*, vol. 21, no. 1, 2008, p. 40.

In the EU Directive 95/46/EC "Third countries" is the term used in legislation to designate countries outside the European Union. Personal data may only be transferred to third countries if that country provides an adequate level of protection. [226] Some exceptions to this rule are provided, for instance when the controller himself can guarantee that the recipient will comply with the data protection rules. The Directive's Article 29 created the "Working party on the Protection of Individuals with regard to the Processing of Personal Data", commonly known as the "Article 29 Working Party".[227] The Working Party gives advice about the level of protection in the European Union and third countries. [228] The Working Party negotiated with United States representatives about the protection of personal data, the Safe Harbor Principles were the result. According to critics the Safe Harbor Principles do not provide for an adequate level of protection, because they contain fewer obligations for the controller and allow the contractual waiver of certain rights.

The Flows of Trans-border Personal Data to a third country, which are undergoing processing or are intended for processing after transfer, may take place if only the third country ensures an adequate level of protection.[229] This Directive is the most influence legal instruments on Personal Data Protection for nearly two decades, not only in EU member state, but also word wide counter-parts around the globe, since it constructs the standard for Personal Data Protection to any Actors who transfer data across EU border.

Indeed, the EU Directive has influenced the works in the Council of Europe and has been the frame for bilateral agreements EU-US:

The Council of Europe furthered its Convention 108 (1981) through the 2001 release of an additional protocol regarding supervisory authorities and trans-border data flows (significantly influenced by the EU Data Protection Directive).[230] A potentially significant development in international governance is the fact that the Council of Europe opened up the

---

[225] De Hert, Paul and Vagelis Papakonstantinou. "Three Scenarios for International Governance of Data Privacy: Towards an International Data Privacy Organization, Preferably a UN Agency." *ISJLP*, vol. 9, 2013, p. 288.

[226] EU. *Directive 95/46/EC*. 1995, Article 26.

[227] Ibid, Article 29.

[228] Ibid, Article 25.

[229] Ibid, Articles 25-26.

[230] De Hert, Paul and Schreuders, Eric. "The Relevance of Convention 108." *Proceedings of the Council of Europe Conference on Data Protection*, Warsaw, 2001, p. 43.

ratification process of its Convention 108 to nonmembers. This supposedly will pave way for the Convention 108 to replace a still-missing international treaty on data protection, [231] though with 38 countries having ratified the Convention to date, remarkable progress would be needed.

In the scope of the thesis, the US has applied this Directive by adopted Safe Harbor Agreement guarantee Personal Data Protection of EU citizen which are transferring to US territory or US subjects companies.

The Exchange of personal data between the EU and the US for commercial purposes are addressed by the Safe Harbor Decision[232] which provides a legal basis for transfers of personal data from the EU to companies in the U.S. which adhere to the Safe Harbor Principles. The Safe Harbor is a streamlined process for EU and US companies to comply with the EU Directive 95/46/EC on the protection of personal data.[233] Intended for organizations within the EU or US that store customer data, the Safe Harbor Principles are designed to prevent accidental information disclosure or loss. EU and USA companies can opt into the program as long as they adhere to the principle of onward transfer**.**

Onward Transfer, principle of Safe Harbor, has written that transfers of data to third parties may only occur to other organizations that follow adequate data protection principles. To disclose information to a third party, organizations must apply the notice and choice principles. When an organization wishes to transfer information to a third party that is acting as an agent, it may do so if it makes sure that the third party subscribes to the Safe Harbor Privacy Principles or is subject to the Directive or another adequacy finding. As an alternative, the organization can enter into a written agreement with such third party requiring that the third party provide at least the same level of privacy protection as is required by the relevant principles.[234]

From the Safe Harbor Agreement, Companies operating in the European Union are not allowed to send personal data to countries outside the European Economic

---

[231] De Hert, Paul and Vagelis Papakonstantinou. "Three Scenarios for International Governance of Data Privacy: Towards an International Data Privacy Organization, Preferably a UN Agency." *ISJLP*, vol. 9, 2013, p. 287.

[232] EU Commission. *2000/520/EC.* 2000, Preamble.

[233] U.S. Department of Commerce. *Welcome to the U.S.-EU & U.S.-Swiss Safe Harbor Frameworks*, 9 Oct. 2015.

[234] EU Commission. *2000/520/EC.* 2000, Annex 1 Safe Harbor Principles.

Area unless there is a guarantee that it will receive adequate levels of protection. Such protection can either be at a country level (if the country's laws are considered to offer equal protection) or at an organizational level (where a multinational organization produces and documents its internal controls on personal data).

The Safe Harbor Privacy Principles allows US companies to register their verification-list if they meet the European Union requirements.

As we have seen the regulation of transborder data flows has gradually evolved over the last several decades. The first such laws enacted in the 1970s tended to make transborder data flows contingent on strict conditions being fulfilled, such as that the transfer was approved by the local data protection authority.[235] Later instruments added further options for legalizing transborder data flows (such as the use of standard contractual clauses). Recently more sophisticated instruments have been developed to provide protection for transborder data flows across organizations, such as binding corporate rules (BCRs) in the European Union.

Some important regional data protection instruments (such as the EU Data Protection Directive) are currently being renewed, with a view to making the legal regime for transborder data flows under them more effective and efficient.[236] Discussions are also ongoing between data protection regulators, civil society groups, international organizations, and multinational companies about how the principle of accountability could be used as a way both to facilitate data flows in a globalised world and to protect the personal data and privacy of individuals.

Moreover, the very word 'accountability' seems to have no precise translation in many languages, so that its legal status in non Anglo-American legal systems remains uncertain.[237] But it seems that the concept of accountability may prove useful in helping to bridge the various approaches to the governance of transborder data flows.[238]

---

[235] Kuner, Christopher. "Regulation of Transborder Data Flows under Data Protection and Privacy Law: Past, Present, and Future." *TILT Law & Technology Working Paper No. 016/2010*, 2010, p. 24.

[236] Reding, Viviane. "The Upcoming Data Protection Reform for the European Union." *International Data Privacy Law*, vol. 1, 2011.

[237] Article 29 Working Party. *Opinion 3/2010 on the principle of accountability*. WP 173, 13 Jul. 2010, p. 8.

[238] Kuner, Christopher. "Regulation of Transborder Data Flows under Data Protection and Privacy Law: Past, Present, and Future." *TILT Law & Technology Working Paper No. 016/2010*, 2010, p. 25.

Regulation of transborder data flows focuses on policies such as preventing circumvention of the law and guarding against data processing risks where the data are received, and if these policies are not implicated (for example, because the law of the countries of export and import have been harmonised), then the necessity of regulating transborder data flows is lessened or eliminated. Such regulation thus performs a protective function designed to prevent the fundamental principles of data protection and privacy law from being circumvented, but regulation of transborder data flows is not itself a fundamental principle of the law.[239]

The laws and instruments also differ in the 'default position' that they take regarding transborder data flows. Some instruments (such as the OECD Guidelines and Convention 108) presume that data flows should generally be allowed, but give regulators the power to block or limit them in certain circumstances, while others (most notably the EU Directive) proceed from the assumption that personal data may not flow outside the jurisdiction[240] unless a particular legal basis is present. However, the number of national data protection laws has increased dramatically, thus reducing the chances that data can be transferred to a jurisdiction where no privacy protection applies, and so far there has been little hard evidence of a widespread transfer of data processing to 'data havens' without data protection legislation.[241] Accordingly, the "Default Position" is deficient because OECD Guidelines and Convention 108 were thinking of data transfer between State parties while EU Directive 95/46/EC approach emphasize on data transfer from an EU State, with strong national data protection laws, to a Third Party in Non EU Member State.

Many instruments on transborder data flows show the influence of multiple approaches, and even those as seemingly divergent as the EU's 'adequacy' approach and the 'accountability' approach used in the OECD member countries are likely to grow closer over time. For example, the Article 29 Working Party, established by the EU Directive 95/46/EC, has called for the principle of accountability to be explicitly incorporated into EU data protection law,[242] and some national Data Protection Authority (DPAs) in Europe has also

[239] Ibid, pp. 27-28.

[240] Ibid, p. 30.

[241] Bennett, Colin J and Raab, Charles D. *The Governance of Privacy: Policy Instruments in Global Perspective.* 2006, p. 279.

[242] Article 29 Working Party. *The Future of Privacy.* p. 3.

expressed interest in it. Some jurisdictions using the accountability approach also recognize that the flow of personal data across national borders may raise concerns about the level of privacy protection.

In practice, the subjects of transborder data flow regulation and applicable law are often intertwined, and countries may use rules on applicable law to protect data transferred beyond their borders. In EU, personal data may generally not be transferred outside the geographic boundaries of the EU without a legal basis, which may require the continued application of EU law to the processing of the data in other countries. Thus, under EU law, certain legal bases for international data transfers (e.g., signature of EU-approved standard contractual clauses between data exporter and data importer that impose data processing obligations based on EU law) result in the application of EU data protection standards in other countries where personal data are processed.[243] Moreover, EU standards are then also applied to further transfers from the data importer to third parties (so-called 'onward transfers') as presented in EU-US Safe Harbor Agreement.

2.2.3. Implementation of Personal Data Protection

This section will reflect how personal data protection law in old regime have transformed itself into action by implanting the mechanism to monitor, remedy and sanction the legal provision. In the first part, Supervisory mechanism, there are some oversight bodies in a form of quasi-judiciary or judicial institution. For individual's remedy, it has shown that not only adjudicative tribunal but also independent reparation unit is created to restore the damage of data subject. On sanctions, there were certain administrative measures or civil compensations or criminal penalties awarded as the enforcement of written law in some cases.

2.2.3.1. Monitoring Body and Supervisory Authority

To supervising personal data protection implementation, Data protection Authority is required in every levels; International, Regional, Bilateral and domestic. The

[243] EU, *2004/915/EC*: Commission Decision of 27 December 2004 amending Decision 2001/497/EC as regards the introduction of an alternative set of standard contractual clauses for the transfer of personal data to third countries, OJ L385/74, Clauses II(i) and III; Safe Harbor Onward Transfer Principle, 2004 , <http://www.export.gov/safeharbor/eu/eg_main_018475.asp>.

estimation of supervisory mechanism is required under right to personal data protection implementation. In order to provide a legal basis and supervisory body for regulating data processing or trans-border data flows. Some countries, particularly those subject to the EU Directive, require that bureaucratic formalities be observed before the transfer takes place, such as that the transfer be registered with the data protection regulator before personal data may be transferred.[244] Other countries that do not specifically restrict trans-border data flows may impose compliance responsibilities on entities that transfer personal data outside the country's borders.

At universal level, monitoring and control mechanisms over States compliance of the right to Personal Data Protection rely on the UN system, specifically on Human Rights Committee (CCPR) and the Universal Periodic Report (UPR).

The implement measures of United Nations are General Assembly Resolutions by the recommendation of Human Rights Council, Universal Periodic Report procedure and National Report of ICCPR member states. The strongest measure is of presenting national report for undermining and having some feedback recommendations.[245] The Committee mentioned that State party reports should also contain information on complaints lodged in respect of arbitrary or unlawful interference, and the number of any findings in that regard, as well as the remedies provided in such cases.[246] The Human Rights Committee (CCPR) can take only a review with the friendly resolutions for asking States to fulfill the obligation of Covenant.

In general, United Nations has Universal Periodic Report (UPR) procedure to call up the State Members to present their national report in every 4.5 years.[247] The Right to Privacy, personal data protection issue, will be covered for review by other UN Member States, Expertise Organizations and NGOs. The State who submitted the UPR report must pledge their intent to develop its domestic implementation in specific problem then come back with the response in the next UPR round.

---

[244] RAND Europe. *Review of the European Data Protection Directive*. 2009, pp. 34-35.

[245] UN. *International Covenant on Civil and Political Right.* 1966. Article 40.

[246] Official Records of the General Assembly, *Forty-third Session, Supplement No. 40 (A/43/40).* 1989, annex VI, para. 6.

[247] UN. *A/HRC/RES/5/1.* 2007.

In General, There is no specific International sanction to enforce Right to Personal Data protection on Natural Person or Legal Persons; IT Corporation and State Authority. The implement measures of United Nations are General Assembly Resolutions which cannot directly compel individual person or private company. The strongest sanction is of presenting national report for undermining and having some feedback recommendations.[248] Even The Human Rights Committee (CCPR) can take only a review with the friendly resolutions for urging States to fulfill the obligation of Covenant but nothing at all to compel individual or private organizations. Some State Parties may send the communication to the Human Rights Committee (CCPR) that the specific State Party is not fulfilling its obligations under the present Covenant.[249] Then Committee shall hold closed meetings to examine the practice of the complained State. When examining result is out the committee will provide friendly resolutions for State to fulfill the obligation of Covenant.

Besides those mechanisms, main international guidelines and documents highlight the need of national monitoring bodies and authorities. So, the United Nations Guidelines for the Regulation of Computerized Personal Data Files lays out the principle on *Supervision and Sanctions* in part A.[250] It requires the designation of an authority responsible for supervising observance of the principles set forth above. The authority shall offer guarantees of impartiality, independence vis-a-vis persons or agencies responsible for processing and establishing data, and technical competence.

Since the quantity of internet using is rising, there is also a growing need for international data protection authority to regulate the data processing of IT Corporations. More importantly, the monitoring of data exchange among State Authorities for the purposes of preventing and combating transnational crime and terrorism become the requirement. In this context, clear and consistent rules on data protection at EU level will help fostering co-operation between such authorities.

The EU Directive 95/46/EC require each member state to set up a supervisory authority, an independent body that will monitor the data protection level in that member state, give advice to the government about administrative measures and regulations, and start

[248] UN. *International Covenant on Civil and Political Right.* 1966, Article 40.

[249] Ibid, Article 41.

[250] UN. *A/RES/45/95.* 1990, part A.

legal proceedings when data protection regulation has been violated. [251] The Directive also set up the organization called "Article 29 Data Protection Working Party"[252] which has an advisory status and acts independently in adhere with all provisions of the Directive.

The Article 29 Data Protection Working Party is composed of:

- a representative of the supervisory authority(ies) designated by each EU country;
- a representative of the authority(ies) established for the EU institutions and bodies;
- a representative of the European Commission.

The Working Party elects its chairman and vice-chairmen. The chairman's and vice chairmen's term of office is two years. Their appointment is renewable. The Working Party's secretariat is provided by the Commission.

The EU Data Protection Directive 1995 requires the establishment of institutional mechanism for monitoring personal data processing in each Member State. [253] In practice, the data controller must notify the supervisory authority before he starts to process data. The notification contains at least the following information: [254]

- the name and address of the controller and of his representative, if any;
- the purpose or purposes of the processing;
- a description of the category or categories of data subject and of the data or categories of data relating to them;
- the recipients or categories of recipient to whom the data might be disclosed;
- proposed transfers of data to third countries;
- a general description of the measures taken to ensure security of processing.

This information is kept in a public register.

[251] Ibid, Article 28.

[252] Ibid, Article 29.

[253] Eberlein, Burkard and Newman, Abraham L. "Escaping the International Governance Dilemma? Incorporated Transgovernmental Networks in the European Union." *Governance*, vol. 21, no. 1, 2008, p. 40.

[254] EU. *Directive 95/46/EC*. 1995, Article 19.

The Data Retention Directive gives State authority permission to access the information but will be monitored by national supervisory authority.[255] The dismissal of such permission by national court remains question as there are different domestic laws of member states.

The European Union's **Article 29 Working Party** is the most influential organization of DPAs, both because it has a formal role under the European Data Protection Directive and because of the quality and diversity of its Opinions On data privacy issues. Its membership is coextensive with that of the EU, but is separately reflected in the Table. It may increasingly have a rival for influence in the Council of Europe Convention 108, Consultative Committee (to be renamed 'Convention Committee'), as an outcome of the Convention's 'modernization' process.[256] However, this is technically not a committee of data protection authority, it is one of the representatives of State Parties to the Convention,[257] although nearly half of the State Representatives are DPAs.

A larger and also influential body is the Conference of European Data Protection Authorities (**EDPAs**),[258] which holds a 'Spring Conference' almost every year, resolutions are usually passed.[259] From Charles Raab's analysis, the conference is significant to the development of data protection policies in Europe.[260] According to one of its member DPAs, 'one of the most important tasks of the European Data Protection Authorities Consists in advising the authorities involved in legislative matters on data protection issues, by pointing out the risks that legislative initiatives might entail and by proposing alternatives which would be more respectful of individual's rights with regard to the processing of their

[255] EU. *Directive 2006/24/EC*. 2006, Article 9.

[256] Greenleaf, Graham. "'Modernising'data Protection Convention 108: A Safe Basis for a Global Privacy Treaty?" *Computer law & security review*, vol. 29, no. 4, 2013, pp. 430-436.

[257] Greenleaf, Graham. "Sheherezade and the 101 Data Privacy Laws: Origins, Significance and Global Trajectories." *Journal Of Law, Information & Science*, 2013, p. 23.

[258] The Conference of National Data Protection Authorities from European States which are member of either Convention 108 or Directive 95/46/EC.

[259] "Resolutions since 2004 are listed on the European Data Protection Supervisor website." *European Conference*, www.edps.europa.eu/EDPSWEB/edps/Cooperation/Eurconference. Accessed 12 May 2015.

[260] Raab, Charles D. "Information Privacy: Networks of Regulation at the Subglobal Level." *Global Policy*, vol. 1, no. 3, 2010.

personal data'.[261] EDPA Has quite strict accreditation rules, requiring its members to operate under a law of a State Implementing either Council Of Europe Convention 108 Or the EU Data protection Directive, And having independence and appropriate functions and powers.[262]

From the perspective of the Safe Harbor Decision, USA private organization can opt into the program as long as they have competent self-monitor system.[263] The Self-Regulate system means registered companies must employ data protection officers or agency to monitor the data leaks and breaches. There must be effective means of enforcing these rules in order to ensure compliance with the safe harbor principles.

As Safe Harbor Agreement is a self-certification system, it has no mandatory independent verification of what a business actually does. Safe harbor companies can have an independent body check their compliance up front and annually thereafter, but independent-body checkups are not required, and few companies seem to do them. The fact that safe-harbor enforcement tends to be complaint-driven, rather than overseen by regulators, and the fact that US enforcement agencies seem rarely if ever to initiate proceedings to enforce safe harbor on the US side, make Europeans nervous—especially in light of Europeans' fear that US data processors are less concern about complaints coming from across the Atlantic.[264] The Safe Harbor registered companies must employ data protection officers or agency to monitor the data leaks and breaches[265] where the applicable law or private sector initiatives so provide.

To the bottom line, the judicial procedure and domestic court of the State Party or Member State is the last available resort for appealing. The court can dismiss the illegitimate orders which could violate the protection of personal data if the violator is National Entity. Despite, the competence of domestic court, adjudicative authority at national level, to compel the organization out of their jurisdiction is low. Likewise, the National Data

[261] Office of the Information and Data Protection Commissioner, Malta, <http://idpc.gov.mt/article.aspx?art=163>.

[262] Conference of European Data Protection Authorities. *Report of the Accreditation Committee.* Lisbon, 16-17 May 2013, <http://www.tietosuoja.fi/uploads/xpit2ond8o6_1.pdf >.

[263] EU Commission. *2000/520/EC.* 2000, Annex 1 Safe Harbor Principles.

[264] Dowling Jr, Donald C. "International Data Protection and Privacy Law." *Practising Law Institute treatise International Corporate Practice*, 2009., p.16.

[265] EU Commission. *2000/520/EC.* 2000, Annex 1 Safe Harbor Principles.

Protection Authority who has the same scope of power as the domestic court is available for oversight or supervisory mission but the limitation of jurisdiction stills remain.

In many cases the supervisory authorities may not have sufficient resources or personnel to properly monitor compliance with trans-border data flow regulation. For example, one study found that eleven out of twenty-seven national data protection authorities in the EU Member States were unable to carry out the entirety of their tasks because of a lack of financial and human resources.[266] This suggests that the authorities are only able to enforce data transfer requirements on a piecemeal basis.

2.2.3.2. Redress Mechanism and Individual Remedy

The tough affair of personal data protection implementation is individual's remedy. As this right is not an absolute right but wide spread breaches may occur internationally. Proportionately, the architecture of complaint and remedy channel lay out by different treaties may arrange vary paths for data subjects. The next complexity is to pursuit remedy from the organization located outside the victim's territory. The exploration of possible way to gain the remedy is the vital part to succeed the full enjoyment of right to personal data protection.

Usually the remedy of individual's damage must start at the most local point of state service body then file a suitcase to the local and national court as such State provided. After the sufferer has been through all of domestic remedy system he may bring the court to higher level mechanism. The principle "Exhaustion of Domestic Remedy" must be the baseline and spring board for victims who want to bring their case to the Regional or International level.

Start with Universal Individual' remedy, due to the breaches on right to personal data protection, Member States of International Covenant on Civil and Political Rights (ICCPR) can take appropriate action immediately, including court action, against the breach of their sovereignty, and thereby the violation of general public international law, perpetrated through the mass surveillance programmes; calls further on Member States to

[266] European Union Agency for Fundamental Rights. *Data Protection in the European Union: the Role of National Data Protection Authorities*. 2010, http://fra.europa.eu/fraWebsite/attachments/Dataprotection_ en.pdf. p. 42.

make use of all available international measures to defend EU citizens' fundamental rights, notably by triggering the inter-state complaint procedure under Article 41 of ICCPR.

Next, the Optional Protocol to the International Covenant on Civil and Political Rights 1996 (ICCPR Optional Protocol 1)[267] , ratified by 115 state parties[268], has the international remedy channel for individuals, who have exhausted all available domestic remedies, to file their complaints directly to the Human Right Committee.[269] Individuals who were violated will be undercover anonymously[270] throughout the process

More specific remedy on Personal Data Protection, the United Nations Guidelines for the Regulation of Computerized Personal Data Files In part A, principle 8 *Supervision and sanctions*,[271] it requires every country to create system for the event of violation of the provisions of the national law to accuse criminal offences and provide with the appropriate remedies for data breach victim.

Come down to European regional level, the Convention 108 put the strong additional safeguard for the data subject[272] by recognizing that any person shall be enabled to have a remedy if a request for confirmation or, as the case may be, communication, rectification or erasure as referred to in paragraphs b and c of this article is not complied with.

To find the closer remedy channel for individual, the EU Directive 95/46/EC provides a right for Individuals to lodge complaints about violations to the supervisory authority[273] or in a court of law for compensations from the suffered. However, the controller may be exempted from this liability, in whole or in part, if he proves that he is not responsible for the event giving rise to the damage.[274]

---

[267] UN. *Optional Protocol to the International Covenant on Civil and Political Rights*. 1966, Article 2.

[268] Update on 30/9/2016. <http://indicators.ohchr.org/>

[269] UN. *Optional Protocol to the International Covenant on Civil and Political Rights*. 1966, Article 4.

[270] Ibid, Article 3.

[271] UN. *A/RES/45/95*. 1990, part A.

[272] Council of Europe. *Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data Convention108*. 1981, Article 8.

[273] EU. *Directive 95/46/EC*. 1995, Article 22.

[274] Ibid, Article 23.

The protection of personal data is closely linked in the jurisprudence of the European Court of Human Rights and the Court of Justice of the European Union, but they should not be considered to be identical.[275]

While there are the EU data processing dispute resolution procedures in general but there has not been any international redress organization in the Safe Harbor Agreement for EU Nationals.[276]

The effectiveness of the enforcement regimes in various countries even EU members is on the extent of judicial interpretation of these laws and on other comparative aspects of data privacy laws.[277] All of this requires an accurate account of the incidence, growth and distribution of the Global data protection regime.

In the case of EU Data Retention Directive, EU citizens brought their cases to domestic constitutional system. The highest judicial authorities of several Member States have ruled that the implementation of the Directive in domestic law was unconstitutional, such as the Constitutional Court of Romania, Germany, the Czech Republic, as well as the Irish High Court.[278] All these courts concluded that the relevant national laws did not ensure adequate safeguards in order to balance between the serious infringement of the right to privacy and other freedoms affected, on the one hand, and the legitimate purpose of combating crime, on the other.[279] The Data Retention gives state authority permission to access the information but the national court may dismiss such permission.[280] However, the different domestic laws of member states will give individual a non-harmonized standard in disparate jurisdictions. Later, the illegitimate Data Retention Directive 'case that EU citizen

[275] Kokott, Juliane and Sobotta, Christoph. "The Distinction between Privacy and Data Protection in the Jurisprudence of the Cjeu and the Ecthr." *International Data Privacy Law*, vol. 3, no. 4, 2013, p. 228.

[276] Dowling Jr, Donald C. "Preparing to Resolve Us-Based Employers' Disputes under Europe's New Data Privacy Law." *J. Alt. Disp. Resol.*, vol. 2, 2000, p. 31

[277] Greenleaf, Graham. "Sheherezade and the 101 Data Privacy Laws: Origins, Significance and Global Trajectories." *Journal Of Law, Information & Science*, 2013, p. 26.

[278] Konstadinides, Theodore. "Destroying Democracy on the Ground of Defending It? The Data Retention Directive, the Surveillance State and Our Constitutional Ecosystem." *European Law Review*, vol. 36, 2011, pp. 727-733.

[279] Raab, Charles D and Jones, Richard. *A report presenting a review of the key features raised by the political perspectives of surveillance and democracy*. 2013, p. 44.

[280] EU. *Directive 2006/24/EC.* 2006, Article 9.

appealed was brought European Court of Justice and Court has disapproved the Directive in 2014.

Maria-Helen Maras shows that the Directive may negatively impact upon competition and other economic policies in the EU by leading consumers to use international webmail services (that is, non-EU providers), and new (and even existing) market participants to take their businesses elsewhere. In all, she found the Directive a disproportionate measure.[281]

An effective remedy is a fundamental right under the EU Charter and the ECHR, awarded to all persons, regardless of their nationality, also applicable to cases where data protection rights have been violated. The ECJ has also established, as a basic principle, that remedies must be available in all cases of breach of EU law. All these EU safeguards are in direct contrast to the legal framework in the US which reciprocally denies European citizens, who are not resident in the US, the right to an effective remedy. If EU citizens are under surveillance for any lawful reason they must have the right to challenge the information by intelligence authorities. Given the mass international transfer of data of EU citizens to US companies and authorities, the lack of appropriate redress mechanism for European citizens is an issue of extreme concern. [282]

The Safe Harbor Decision which provides a legal right for personal data subject from the EU to companies in the U.S. which adhere to the Safe Harbor Principles. [283] The US-EU Safe Harbor provides procedure for individual's remedy due to comply with the EU Directive 95/46/EC on the protection of personal data.[284] The Safe Harbor Procedures are developed to prevent accidental information disclosure or loss. The US

[281] Maras, Marie-Helen. "The Economic Costs and Consequences of Mass Communications Data Retention: Is the Data Retention Directive a Proportionate Measure?" *European Journal of Law and Economics*, vol. 33, no. 2, 2012, pp. 447-472.

[282] Moraes, Claude. "Working Document on the US and EU Surveillance programmes and their impact on EU citizens fundamental rights." *LIBE Committee Inquiry on electronic mass surveillance of EU citizens*, Justice and Home Affairs, 2013, p. 72.

[283] EU Commission. *2000/520/EC.* 2000, Preamble.

[284] U.S. Department of Commerce. *Welcome to the U.S.-EU & U.S.-Swiss Safe Harbor Frameworks*, 9 Oct. 2015.

private organization can opt into the program as long as they have effective remedy procedure. These principles urge IT Corporation to respect and fulfill these issues: [285]

- **Notice** - Individuals must be provided information about how individuals can contact the organization with any inquiries or complaints.
- **Enforcement** - There must be effective means of enforcing these rules. In order to ensure compliance with the safe harbor principles, there must be procedures for verifying that the commitments companies make to adhere to the safe harbor principles have been implemented.

Data subject must have ready access to affordable procedures for safeguarding his rights under safe harbor.[286] Therefore, safe harbor companies must build dispute-resolution machinery, and offer it to European data subjects who have grievances.[287] At a minimum, this machinery must be included but there has no existence organization.

As Safe Harbor Agreement is a self-certification system but the safe harbor enforcement tends to be complaint-driven.[288] The Safe Harbor organization must employ data protection officers or agency, readily available and affordable independent recourse mechanisms, so that each individual's complaints and disputes can be investigated and resolved and damages awarded[289] where the applicable law or private sector initiatives so provide.

The channels for data subjects to file complaints, which the safe harbor company then actually investigates and resolves, awarding damages or other real remedies if there was a violation (these procedures should not be a "show trial"—a widespread perception in Europe sees the chief failing of safe harbor as American data processors too often sweeping European data subjects' complaints under the rug).[290]

---

[285] EU Commission. *2000/520/EC.* 2000, Annex 1 Safe Harbor Principles.

[286] EU-US. *Safe Harbor Agreement.* 1998, Annex II, FAQ 11, p. 22.

[287] Ibid, Annex I, p. 12.

[288] Dowling Jr, Donald C. "International Data Protection and Privacy Law." *Practising Law Institute treatise International Corporate Practice*, 2009., p. 16.

[289] EU Commission. *2000/520/EC.* 2000, Annex 1 Safe Harbor Principles.

[290] EU-US. *Safe Harbor Agreement.* 1998, Annex I, p. 13.

Data protection authorities have received complaints from individuals and non-governmental organizations (NGO) regarding data transfers abroad, though the number does not seem to be large.[291] The increasing complexity of data processing on the Internet caused by phenomena such as cloud computing and outsourcing can make it difficult for individuals to obtain information as to where their personal data are being processed and stored, which may lead to a loss of confidence. On the other hand, some studies demonstrate a lack of interest by individuals in the regulation of trans-border data flows.[292]

The enforcement of right to personal data protection is increasingly based on formal or informal cooperation between regulators outside of traditional legal assistance. There is also ever-increasing use of internal dispute resolution mechanisms in both the private and public sectors, [293] which may enhance the ability of individuals to assert their rights in other countries.

Even though, the Safe Harbor gives a right to access for Individuals to their personal information that an organization holds and be able to correct, amend, or delete that information where it is inaccurate, except where the burden or expense of providing access would be disproportionate to the risks to the data subjects in the case in question, or where the rights of persons other than the individual would be violated. However, it is not easy to undertake for example in the case of normal internet users in EU claim their right to the IT Corporation located in Texas. It is even harder if the Non-EU citizen want to appeal for reparation from US company when they are surfing online market in EU territory.

2.2.3.3. Enforceability of Rights

Enforceability of right to personal data protection is the hardest feature of implementation because many case studies comprehend different jurisdiction. The compatible sanction and the solution for conflict of laws induced by vast majority legal apparatus will be shown. Most enforcements sanctioned by domestic court but there is some measures can be

[291] OECD. *Report on the Cross-Border Enforcement of Privacy Laws*. 2006, p. 9.

[292] European Commission. *Data Protection in the European Union Citizens' perceptions: Analytical Report*. 2008, p. 33.

[293] Kuner, Christopher. "Regulation of Transborder Data Flows under Data Protection and Privacy Law: Past, Present, and Future." *TILT Law & Technology Working Paper No. 016/2010*, 2010, p. 33.

imposed internationally. Consequently, the survey for available sanction in numerous data protection laws would be useful to the sufferer.

The point of departure for the specific Personal Data Protection enforceability can be found in the United Nations Guidelines for the Regulation of Computerized Personal Data Files In part A, principle 8 *Supervision and sanctions*,[294] as far as it requires every country to prepare for the event of violation of the provisions of the national law. State must be able to enforce criminal or other penalties and should be envisaged together with the appropriate individual remedies.

That requirement has been developed by the Convention 108 which pursues each party to establish appropriate sanctions and remedies for violations of provisions of domestic law giving effect to the basic principles for data protection set out in this chapter.[295]

Specifically within the EU framework, two norms are of interest. First, the EU Directive 95/46/EC urges that Member States shall adopt suitable measures to ensure the full implementation of the provisions of this Directive and shall in particular lay down the sanctions to be imposed in case of infringement of the provisions adopted pursuant to this Directive.[296]

Second, under the Data Retention Directive, it depends on national court power to dismiss the permission to access. Nonetheless, the procedure and conditions of provoking the permission, remedy the damage or punishment the violator will be diverse due to the different domestic laws of member states.[297]

As a step towards reciprocity, the US must explore the most appropriate mechanisms to extend at least the legal protection afforded to persons within the US also to Global citizens outside the US, in order to provide an effective legal redress mechanism for Global citizens whose data has been held or accessed by the US authorities and companies. Most importantly, the reparation to victim violated by US entities especially the US public authorities such as National Security Agency or National Intelligence Agency.

---

[294] UN. *A/RES/45/95.* 1990, part A.

[295] Council of Europe. *Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data Convention108.* 1981, Article 10.

[296] EU. *Directive 95/46/EC.* 1995, Article 24.

[297] EU. *Directive 2006/24/EC.* 2006, Article 9.

In between relationship of EU and US, the Safe Harbor Decision, provides procedure for individual's remedy due to the eager to comply with the EU Directive 95/46/EC on the protection of personal data.[298] The Safe Harbor Procedures are developed to prevent accidental information disclosure or loss. The EU and US private organization can opt into the program as long as they provide effective redress measures.

The Safe Harbor registered Corporation must prepare:

- follow-up procedures, conducted either by self-assessment or outside compliance review, verifying that what the safe harbor company claims about its privacy practices is accurate and in place;[299] and
- methods to fix problems, and, for violations, sanctions with teeth.[300]

  There are two options a safe harbor company can build this machinery which are: [301]

- to buy a prepackaged privacy enforcement program that incorporates the safe harbor principles, or
- submit to legal/regulatory supervisory authorities, such as European data protection authorities (DPAs), that have dispute-resolution machinery already in place.

The enforcement principle urges organization to have effective means of enforcing the rules of Safe Harbor. In order to ensure compliance with the safe harbor provisions, there must be obligations to remedy problems arising out of a failure to comply with the principles. Sanctions must be sufficiently rigorous to ensure compliance by the organization.[302] The Safe Harbor organization must employ data protection officers or agency to investigate

[298] U.S. Department of Commerce. *Welcome to the U.S.-EU & U.S.-Swiss Safe Harbor Frameworks*, 9 Oct. 2015.

[299] EU-US. *Safe Harbor Agreement*. 1998, Annex II, FAQ 7, at 16. For detail on how self-assessment works, see *id*. Annex II, FAQ 7, pp. 16–17.

[300] Ibid, Annex I, at 12. On EU data processing dispute resolution procedures generally, albeit not in the safe harbor context.

[301] Ibid, Annex II, FAQ 5 and 11, pp. 14, 21.

[302] EU Commission. *2000/520/EC*. 2000, Annex 1 Safe Harbor Principles.

individual's complaints and disputes so that can be resolved and sanctioned compensation.[303] Organizations that fail to provide annual self certification letters will no longer appear in the list of participants and safe harbor benefits will no longer be assured.

The complexities of implementation to Safe Harbor Agreement by company discussed above can obscure the fact that, procedurally, safe harbor status is amazingly easy to get.[304] All a company need do is log onto the Department of Commerce website and fill out a one-page form, or send a letter self-certifying that it has adequate procedures and protections up and running.[305] Specifically, this self-certification merely needs only basic details to disclose but SMEs or Start-up business may found this is hard to follow since they might have not had system to support data protection policy yet.[306] Due to the Red-Tape that the Agreement had putted in front of the data transfer across border, some SME companies may loss their opportunity to access EU market. But if SMEs need to prepare for accession, the cost of transaction and set up system might make them less competitive when compare with Multi-national Corporation.

State Members that export personal data across national borders may also not comprehend the ubiquity of trans-border data flows: for example, in a study by the European Commission published in 2008, only a small percentage (10%) of data controllers stated that their companies transferred personal data outside the European Union,[307] a figure that must be too low given the widespread use by companies of e-mail and the Internet.

In addition, rules on applicable law and jurisdiction with regard to data protection and privacy law are notoriously unclear,[308] which can create problems in particular for individuals, who often may not be able to determine which law applies to the processing

---

[303] Ibid.

[304] Bender, David and Larry Ponemon. "Binding Corporate Rules for Cross-Border Data Transfer." *Rutgers JL & Urb. Pol'y*, vol. 3, 2006, p. 154.

[305] EU-US. *Safe Harbor Agreement*. 1998, Annex II, FAQ 6, p. 15.

[306] Dowling Jr, Donald C. "International Data Protection and Privacy Law." *Practising Law Institute treatise International Corporate Practice*, 2009., p. 15.

[307] European Commission. *Data Protection in the European Union Citizens' perceptions: Analytical Report*. 2008, p. 7.

[308] European Commission. "Comparative Study on Different Approaches to New Privacy Challenges in Particular in the Light of Technological Developments." *Final Report*, 2010, p. 24.

of their personal data, and to which national regulatory authorities they may turn if a problem arises.

Despite the large number of laws regulating trans-border data flows, it is questionable how widely such regulation is enforced because 'many unauthorised and possibly illegal transfers are being made to destinations or recipients not guaranteeing adequate protection. Yet there is little or no sign of enforcement action by the supervisory authorities'.[309] The fact that some of the largest economies in the world (such as China and Japan) have not been the subject of a formal EU adequacy decision means that there must be substantial non-compliance at least with regard to data flows from the EU to those countries.[310]

2.3. Failures due to limitations of US Domestic System relate to Personal Data Protection

The legal system of US for protecting personal data is the real matters because the most of prominent trans-national IT Corporations are subjected to the obligation of US jurisdiction. Most of IT Corporations' servers are located in US territory or the personal data of users is transfer to US territory. Consequently, the US regime on personal data protection is the regulation, governs the acts of US IT Corporations and State Authorities, which may effect to the personal data protection standard of internet users in other States. Accordingly, there were the limitations on rights of global internet user arising from the exercise of US entities. The power of US State Authority over the US IT Corporation, or the cooperation between both actors, might put the obstacles to the full enjoyment of right to personal data protection of Internet Citizen worldwide.

Unlike the EU, however, the United States does not have a single, overarching personal data protection framework. [311] The fundamental law to protect personal data in

[309] European Commission. *First report on the implementation of the Data Protection Directive (95/46/EC): COM(2003) 265 final*. Brussels, 15 May 2003, p. 19.

[310] Kuner, Christopher. "Regulation of Transborder Data Flows under Data Protection and Privacy Law: Past, Present, and Future." *TILT Law & Technology Working Paper No. 016/2010*, 2010, p. 29.

[311] Weiss, Martin A and Archick, Kristin. "US-EU Data Privacy: From Safe Harbor to Privacy Shield." *Congressional Research Service*, 2016, p. 4.

United States has a decentralized and multi-layers legal framework for personal data protection:

- **Constitutional protections.** The U.S. Constitution, above all the Fourth Amendment (protecting against government "searches and seizures")[312], and well-settled U.S. Supreme Court law grounded in the Bill of Rights provide strong baseline protection for personal data.
- **Federal statutes.** Several federal privacy laws regulate the collection, use and disclosure of information on a sectoral basis, including information in the finance and information related to consumer credit and commercial email. Additionally, the Privacy Act of 1974 protects against the improper use of personal data by government agencies[313], the Electronic Communications Privacy Act (ECPA) regulates the interception of electronic communications[314], and the Computer Fraud and Abuse Act (CFAA) imposes criminal penalties on unauthorized access to information stored on computers.
- **Federal Enforcement Authority.** The Federal Trade Commission (FTC) has broad authority under the FTC Act to address "unfair or deceptive acts or practices in or affecting Commerce", and it has used this authority in a variety of privacy and data security contexts to protect consumers by bringing enforcement actions against companies engaging in unfair practices harmful to consumers regarding the collection, use and disclosure of information. [315]
- **State law protections.** There are numerous additional data protections under U.S. state law providing an expanded scope of data protections[316], including explicit provisions relating to a right to data protection in several state constitutions, and laws to protect individuals' personal data in various areas, including requiring

[312] Bignami, Francesca. "The Us Legal System on Data Protection in the Field of Law Enforcement. Safeguards, Rights and Remedies for EU Citizens." 2015., p. 10.

[313] Ibid, p. 11.

[314] Ibid, pp. 17-18.

[315] ITI. *The U.S. Privacy and Data Protection Framework: Basic Characteristics and Recent Reforms.* 18 Jan. 2016.

[316] European Commission. *Restoring Trust in EU-US data flows - Frequently Asked Questions*. Brussels, 27 Nov. 2013.

companies to disclose details of their data sharing with third parties, limiting unauthorized access to network accounts, and security breach notification laws requiring companies to disclose any computer breaches resulting in unauthorized access to consumers' personal data. [317]

On the contrary, there is the **Executive Order 12333**, an Executive Order intended to extend powers and responsibilities of U.S. intelligence agencies and direct the leaders of U.S. federal agencies to co-operate fully with CIA requests for information.[318] This executive order entitled United States Intelligence Activities; government surveillance, including mass electronic surveillance activities. As Professor Francesca Bignami has explained, "the National Security Agency - NSA's original mandate was considerably elaborated and extended in Executive Order 12333, promulgated by President Reagan in 1981."[319] the government's reliance on EO 12333, particularly the reliance on Section 1:12(b)(13), which authorizes the NSA to provide "such administrative and technical support activities within and outside the United States as are necessary to perform the functions described in sections (1) through (12) above, including procurement." [320] This provision appears to have opened the door for the NSA's broad and unwarranted surveillance of U.S. and foreign citizens.

Moreover, the further bulk collection of intelligence information is allowed under **Section 215 of the PATRIOT Act** since 2001 right after the 9/11 attack. This section 215 of the USA PATRIOT Act is controversial because the order may be granted *ex parte* (without notice to the other party – surveillance target), and once it is granted, in order to avoid jeopardizing the investigation[321], the order may not disclose the reasons behind why the order was granted.

Nonetheless, Personal Data Protections, extend to surveillance by law enforcement and national intelligence/security authorities, are regulated by:

---

[317] Ignami, Francesca. "European Versus American Liberty: A Comparative Privacy Analysis of Antiterrorism Data Mining." *BCL Rev*, vol. 48, 2007, pp. 624–635.

[318] Reagan, Ronald. "Executive Order 12333—United States Intelligence Activities." *Public Papers of the Presidents: Ronald Reagan*, 1981.

[319] Ignami, Francesca. "European Versus American Liberty: A Comparative Privacy Analysis of Antiterrorism Data Mining." *BCL Rev*, vol. 48, 2007, pp. 624–635.

[320] Bignami, Francesca. "The Us Legal System on Data Protection in the Field of Law Enforcement. Safeguards, Rights and Remedies for EU Citizens." 2015, p. 27.

[321] Ibid, p. 21.

- **Foreign Intelligence Surveillance Act (FISA).** Congress passed FISA in 1978 to govern surveillance activities, including to: (1) establish a Foreign Intelligence Surveillance Court (FISC) (Staffed with independent judges with life tenure); (2) require a warrant issued by aFISC judge for electronic surveillance, to ensure high-level approval of narrowly-tailored and targeted requests; and (3) create the Senate and House Intelligence Committees, to provide oversight of the Executive Branch.[322]
- **Section 702 of FISA provides additional protections regarding surveillance of non-U.S. persons.** Section 702 contains important limitations, oversight, and accountability provisions, including FISC approval of surveillance requests only after several safeguards have been met, including that the government: (1) have a valid "foreign intelligence purpose;" (2) follow FISC targeting procedures; (3) use specific identifiers to limit collections and avoid overly broad queries; and (4) employ minimization procedures to destroy raw data between two and five years after collection.[323]
- **Protections under U.S. federal case law.** Courts have routinely interpreted the Fourth Amendment and other legal provisions to: (1) restrict the scope and circumstances of law enforcement wiretaps; (2) require a warrant before a national security wiretap; (3) exclude evidence obtained from illegal police searches; and (4) require a warrant before police may search cell phones or use tracking devices[324], among other protections.

However, there are some critiques from what have happened in US system when the protection of personal data versus the power of State to surveillance on matters of National Security or Public Safety: [325]

[322] Ibid, pp. 22-26.

[323] Shane, Peter M. "Foreword: The Nsa and the Legal Regime for Foreign Intelligence Surveillance." 2013, pp. 10-12.

[324] ITI. *The U.S. Privacy and Data Protection Framework: Basic Characteristics and Recent Reforms.* 18 Jan. 2016.

[325] Look at Council of the European Union. *Report on the findings by the EU Co-chairs of the ad hoc EU-US Working Group on Data Protection 16987/13*, Brussels, 27 Nov. 2013, p.26-27.; Bignami, Francesca. "The Us Legal System on Data Protection in the Field of Law Enforcement. Safeguards, Rights and Remedies for Eu Citizens." 2015., p.33-34.; European Commission. *Restoring Trust in EU-US data flows - Frequently Asked Questions*. Brussels, 27 Nov. 2013; Shane, Peter M. "Foreword: The Nsa and the Legal Regime for Foreign Intelligence Surveillance." 2013, p. 40-42.

1) Under US law, a number of legal bases allow large-scale collection and processing, for foreign intelligence purposes, including counter-terrorism, of personal data that has been transferred to the US or is processed by US companies. The US has confirmed the existence and the main elements of certain aspects of these programmes, under which data collection and processing is done with a basis in US law that lays down specific conditions and safeguards. Other elements remain unclear, including the number of EU citizens affected by these surveillance programmes and the geographical scope of surveillance programmes under Section 702. [326]

2) There are differences in the safeguards applicable to EU data subjects compared to US data subjects, namely: [327]

- Collection of data pertaining to US persons is, in principle, not authorised under Section 702. Where it is authorised, data of US persons is considered to be "foreign intelligence" only if *necessary* to the specified purpose. This necessity requirement does not apply to data of EU citizens which is considered to be "foreign intelligence" if it *relates* to the purposes pursued. This results in lower threshold being applied for the collection of personal data of EU citizens.
- The targeting and minimisation procedures approved by FISC under Section 702 are aimed at reducing the collection, retention and dissemination of personal data of or concerning US persons. These procedures do not impose specific requirements or restrictions with regard to the collection, processing or retention of personal data of individuals in the EU, even when they have no connection with terrorism, crime or any other unlawful or dangerous activity. Oversight of the surveillance programmes aims primarily at protecting US persons.
- Under both Section 215 of Patriot Act and Section 702 of FISA, US persons benefit from constitutional protections (respectively, First and Fourth Amendments) that do not apply to EU citizens not residing in the US.

[326] Council of the European Union. *Report on the findings by the EU Co-chairs of the ad hoc EU-US Working Group on Data Protection 16987/13.* Brussels, 27 Nov. 2013, pp. 8-10.

[327] Ibid, pp. 10-11.

3) Moreover, under US surveillance programmes, different levels of data protection safeguards apply to different types of data (meta-data vs. content data) and different stages of data processing (initial acquisition vs. further processing/analysis). [328]

4) A lack of clarity remains as to the use of other available legal bases, the existence of other surveillance programmes as well as limitative conditions applicable to these programmes. This is especially relevant regarding Executive Order 12333[329] which may occur even after the reforms in 2014.

5) Since the orders of the FISC are classified and companies are required to maintain secrecy with regard to the assistance they are required to provide, there are no avenues, judicial or administrative, for either EU or US data subjects to be informed of whether their personal data is being collected or further processed. There are no opportunities for individuals to obtain access, rectification or erasure of data, or administrative or judicial redress. [330]

6) Various layers of oversight by the three branches of Government apply to activities on the base of Section 215 of Patriot Act and Section 702 of FISA. There is judicial oversight for activities that imply a capacity to compel information, including FISC orders for the collection under Section 215 and annual certifications that provide the basis for collection under Section 702. There is no judicial approval of individual selectors to query the data collected under Section 215 of Patriot Act or tasked for collection under Section 702 of FISA. The FISC operates *ex parte* and *in camera*. Its orders and opinions are classified, unless they are declassified. There is no judicial oversight of the collection of foreign intelligence outside the US under Executive Order 12333, which are conducted under the sole competence of the Executive Branch. [331]

Many U.S. officials and industry representatives maintain that the U.S. approach to data protection is more nimble than what they view as the EU's "one-size-fits-all" approach. They also contend that the U.S. approach helps to promote and sustain U.S. technological

[328] Ibid, p. 13.

[329] Ibid, pp. 12-13.

[330] Ibid, pp. 22-23.

[331] Ibid, pp. 24-25.

innovation.[332] Nevertheless, some U.S. privacy advocates argue that there are significant gaps in this "patchwork" approach, especially in terms of data collection online, and have long urged Congress to enact comprehensive data protection legislation.[333]

The discontents US system brought to the personal data protection recourse came from the directly clash with the State intelligence operation in National Security realm. The intention of US government to conduct mass electronic surveillance on activities relate to terrorism, especially on foreigner who is out of the full constitutional protection, may put further complicated situation for internet users around the world. Since most of prominent IT Corporations have US nationality status or transfer personal data to the servers in US territory, the different standard would be the main threat to Non-US citizen internet users therefore.

2.4. Lesson Learnt from the Old Regime

After the end of WWII, the concept of a "right to privacy" emerged in international law but there is no solid universal legal instrument about "personal data protection". These rights have the sense of Negative Rights, interference with the right to respect for private life, must base on adequate legal basis; clear, accessible and foreseeable. As well as the prerequisite of necessary and proportionate for the legitimate ground to intervene at baseline.

The right to respect for private life and the right to the protection of personal data, not only have connections but also differences. The concept of " personal data protection" was developed in order to provide structural legal protection to individuals against the inappropriate use of information technology for processing information relating to them, regardless of whether that processing would be within the scope of the right to respect for private life or not.

Data protection as a specific issue in legal policy and legislative practice arose since the 1970's, in the era in which computerized automatic data processing became widespread. In practice, it could mean key differences that the legal system must take into consideration to ensure that the rules are suitable in different situations. However, the deliberation to create a

[332] Singer, Natasha. "Data Protection Laws, an Ocean Apart." *New York Times*, 2013.

[333] Weiss, Martin A and Archick, Kristin. "US-EU Data Privacy: From Safe Harbor to Privacy Shield." *Congressional Research Service*, 2016, p. 5.

safer online society is even harder than in an offline world because the overwhelming of data processing is heavier than the paper document era.

In 1980's, the first binding international instrument on personal data protection was launched with regard to automatic processing of personal data across border. Later, the proliferation of data sharing in the area of criminal and judicial matters reflects result in needs to protect personal data in the case of criminal procedure undertaken by State Agency.

The eager to construct International regime to protect right to personal data of data subjects to support the development of Single E-Market on the basis of liberal democratic society are the goal. Notwithstanding, the old personal data protection regime, has shown that there are incompetence conditions, need reforms in order to create more harmonize standard.

A range of potential trans-border personal data protection standards have been developed by various initiatives and organizations, courts and civil societies such as the European Data Protection Supervisor. These cover data processing, sharing of private entities and the oversight of surveillance activities by State intelligence agencies. The principal opportunities for implementing them are in EU and EU–US negotiations over a data sharing privacy agreement and the further Transatlantic Trade and Investment Partnership in the future. The Council of Europe and state–state negotiations over intelligence sharing are also possible venues.

Even at that time (Mid-2013) trans-border flows of personal data were taking place at an increasing pace. International business cooperation became difficult; the need for some regulations on automated personal data processing was felt, but not everybody shared the same enthusiasm for the introduction of formal data privacy acts.[334] The institutional internationalization of the data protection law-making process became necessary to encourage and formalize a possibly broad adoption of the new field of law.

Beyond this, there are opportunities to introduce new standards through the Council of Europe's data protection convention, and encourage ratification by non-European states, as well as introducing new personal data protections in the General Data Protection Regulation and Data Protection Directive on criminal procedure.[335] More difficult will be efforts to make intergovernmental intelligence sharing agreements transparent. Outside the USA and EU,

[334] Schwartz, Paul M. "Preemption and Privacy." *The Yale Law Journal*, 2009, p. 118.

[335] Will be described with more details in Chapter 4.

forums at the UN, OECD, Privacy Commissioners' Conference, WTO and WIPO could also play a role, although they present challenges of scope and enforcement.

Despite, the difficulties come from the failure of US legal system for protecting personal data of data subjects around the world. Since most of prominent trans-national IT Corporations are under the obligation of US jurisdiction and there are plenty of personal data had been transferring to servers located in US territory. Accordingly, the US regime on personal data protection became the main regulation to govern the acts of US IT Corporations and State Authorities. The limitations to full enjoyment of right to personal data due to the exercise of State Authority's power over the IT Corporation or the cooperation between both sectors are the risky threats to data subjects worldwide. The inadequacy of US system brought deteriorates to the personal data protection. The program of US government to conduct mass electronic surveillance on activities relate to terrorism, especially on foreigner who is out of the full US constitutional protection, may put further obscure scenario for internet users globally.

Following a review by an independent panel appointed by President Obama[336], the US executive branch has recently made significant changes to improve the compliance of its foreign intelligence practices with international human rights law. These include more specific definitions of the purposes for which surveillance can be undertaken, and—significantly—greater protections for non-US citizens and residents.[337] There remains an opportunity for democratic states to further improve and entrench human rights protections for their citizens through the implementation of the standards[338] which will be described in Chapter 4 and 5.

The deficiencies of personal data protection instruments on universal and EU regional level are:[339]

[336] The US reform will be discussed in detail at the early stage of Chapter 4.

[337] Obama, Barack. *US Presidential Policy Directive 28 – Signals Intelligence Activities*. The White House Office of the Press Secretary, 17 Jan. 2014.

[338] Brown, Ian. "The Feasibility of Transatlantic Privacy-Protective Standards for Surveillance." *International Journal of Law and Information Technology*, vol. 23, no. 1, 2015, pp. 23-40.

[339] Blackmer, WS. "Gdpr: Getting Ready for the New EU General Data Protection Regulation." *Information Law Group, InfoLawGroup LLP, Retrieved*, vol. 22, no. 08, 2016.

- the inconsistencies in national laws;
- the unbalanced standard to provide better privacy protection for individuals;
- outdated-law to address contemporary personal data challenges, such as those posed by the Internet, Social media, mobile apps, cloud computing, "Big data," and State Agency data sharing, that were in their infancy when the Data Protection Instruments were drafted;
- Costly administrative burdens for companies dealing with multiple data protection authorities.
- Incompetence oversight and supervisory mechanism when deal with trans-border problems.
- Almost impossible for common data subjects to lodge their complaint and gain feasible remedy in the multi-national case.

In the European Union, various legal instruments and obligations provide individuals and regulators with a framework that allows the assertion of rights with regard to EU-based data processing. Thus, EU data protection authorities are obliged to cooperate with each other,[340] and often do so in practice.[341] Court decisions from one EU Member State can also be enforced in another Member State with relative ease.[342] However, the same legal instruments do not apply to situations where a non-EU country is involved, meaning that such enhanced regulatory cooperation and ease of enforcement are not possible to fulfill. [343] The difficulty of asserting legal rights abroad is not unique to data protection and privacy law, but results from the fact that there is no global legal framework for the assertion of consumer rights, or for the recognition and enforcement of court decisions in other countries.

The Critique on Safe Harbor Agreement from multinationals' point of view is that it insulates only EU-to-US data transfers, and as such is useless when a conglomerate wants to roll out a globally accessible data base, such as a global information system, or else to

[340] EU Data Protection Directive, Article 28(6).

[341] For example, a DPA of an EU Member State informed the author that it receives 20 to 30 cooperation requests annually from other EU DPAs.

[342] EU. *Regulation (EC) 44/2001*. 2001.

[343] Kuner, Christopher. "Regulation of Transborder Data Flows under Data Protection and Privacy Law: Past, Present, and Future." *TILT Law & Technology Working Paper No. 016/2010*, 2010, p. 32.

transfer data beyond the United States. Quite apart from that data-controller-perspective shortcoming, however, are the criticisms of safe harbor as ineffective in safeguarding the rights of EU data subjects[344] or any other Non-US Citizen data subjects.

One of the problems around personal data protection on E-Market comes from an obvious paradox: Internet is an issue/object with an exclusive and unique international nature. Nonetheless, it is submitted to national regulations and, specifically, to the US national rules because of the physical location of most enterprises providing internet services.

While data protection legislation has a cross-border dimension, its subsequent development acquired distinct national and regional characteristics. Perhaps most importantly, in European countries a new field of law emerged, data protection, which gained in depth and width and claimed its independence from the traditional right to privacy.[345] However, the European approach was not shared elsewhere in the world—perhaps most notably in the US Given, however, the globalization of transactions, as well as the national security imperatives, personal data need to travel across borders now more than ever. In order to accommodate the international cooperation of fundamentally different data protection legal systems,[346] a series of initiatives have been undertaken, particularly during the last decade.

As with new information technologies, it is quite complicate to see if and how a certain activity can be impacted with laws and other rules due to nature of jurisdiction, the fact that it is difficult to implement existing legislation to new and complicated technologies, or for national security reasons. There are many scenarios in which public feel that certain situation must be regulated, that something should be banned, that it should be possible to impede a certain activity and so on, even though the legal system actually does not have the necessary regime to success this. In liberal democratic state, respect human rights and human dignity, it is still important to permit everything that is not specifically prohibited by legislation. Otherwise the concrete legislation, which gives precise scope of what activities are illegal and when such limitation may employ, is needed.

---

[344] Dowling Jr, Donald C. "International Data Protection and Privacy Law." *Practising Law Institute treatise International Corporate Practice*, 2009, p. 16.

[345] Rodotà, Stefano. "Data Protection as a Fundamental Right." *Reinventing Data Protection?*, Springer, 2009, pp. 77-79.

[346] De Hert, Paul and Papakonstantinou, Vagelis. "Three Scenarios for International Governance of Data Privacy: Towards an International Data Privacy Organization, Preferably a UN Agency." *ISJLP*, vol. 9, 2013, p. 293.

The likelihood that a legally-binding data protection instrument of global application will be enacted in the foreseeable future appears insufficient for a variety of reasons, in particular because of the difficulty of agreeing on the form of the legal framework, selecting the standards on which such an instrument would be based, determining the scope of the instrument, and agreeing on an international organization to coordinate the work.[347] Some other tactics to proliferate the recognition of personal data protection may be desired.

In the next Chapter 3, various cases will show the practice and interpretation of EU and EU-US regime, when it has to handle the Trans-National IT Corporations and National Intelligence Agencies. Thus, theses problems are needed to be tackled by proposing the new set of data protection laws. As reforms have been launching since Mid-2013, it has triggered changes not only to EU regime but also EU-US regime. The results of such reforms will be discussed in Chapter 4.

[347] Kuner, Christopher. "An International Legal Framework for Data Protection: Issues and Prospects." *Computer law & security review*, vol. 25, no. 4, 2009, p. 307.

Chapter 3 Personal Data Protection analysis in Hard Case Study

In this chapter, IT Corporation and State National Security Authority will be brought into highlight as the case study to understand the operation of Personal Data Protection Regime prior reforms. Both IT Corporation Policy and Practice in their own regulate realm and the External relationship with society and State Agency is on the radar of scrutiny. Moreover, the Chapter also investigates into cases which were decided by various courts, Regional and Domestic in EU and USA, in order to reflect shifting paradigms from arbitrary interference to more transparency. As Right to Personal Data Protection is a mainstream attention of International Community since the most notorious revelations of the Century in June 2013, the recognition of vast majority judicial/oversight mechanism will be the hard evidences to draw the line between legitimate data processing and illegal penetration in data collection on cyberspace. The most controversial issue the chapter will discuss is the complicated argument on Human Rights in one hand and National Security on the other.

3.1. The Nature of Information Technology Corporation relate to Personal Data Protection

The prominent Information Technology (IT) Corporation has launched the vast majority of inventive products and services into the information market. Thus, IT Corporation has encountered legal concerns since some applications such as the search engine, web browser, and visual map have a critical impact on individual rights directly and indirectly. These applications were invented and developed by ongoing data processing of users' personal data; however, they outspokenly have claimed that "Corporate does no evil". Furthermore, IT Corporation is the mega power in information-based society which could provide various services to world-wide internet surfers then turn users into their products by data processing. Howbeit, the efficiency of governance models on Internet Service Providers (ISPs) is relevant with diverse conditions. For implement the data protection regime, the penetration and collection of personal data by IT Corporation is unpredictably high and extensive in the long run and must be taken into account.

IT Corporation is increasing clout as the ultimate arbiter of commercial success ("to exist is to be indexed by a search engine"[1]) and as a central database for users' personal information, not only logging their search queries but also storing their e-mail, map (Street View), web browser, operating system, calendars, photos storage, videos port website, blogs, documents saving, social networks, news feeds, credit card information, in short, the "entire digital lives".

IT Corporation's access to and storage of vast amounts of personal data create a serious privacy problem, as Edward Felten recently called "perhaps the most difficult privacy [problem] in all of human history."[2] Every day, millions upon millions of users provide IT Corporation with unfettered access to their interests, needs, desires, fears, pleasures and intentions.[3] The information is logged and maintained in a form which may facilitate the identification of specific users for various purposes, including not only their targeting with effective advertising but also prosecution by the government or pursuit by private litigants.[4] The "Database of Users' Intentions" in the description of John Battelle, "link by link, click by click, search is building possibly the most lasting, ponderous, and significant cultural artifact in the history of humankind: the Database of Intentions."[5] It constructs a honey pot for various actors, not only State Agencies such as NSA and FBI which spent billions dollars on online surveillance, to penetrate in, IT Corporation 's information treasure mine, but also hackers and data thieves, who deliberately try to sneak information security systems no matter how tight.

How did IT Corporation evolve from being a benevolent giant seeking to "do no evil" into a privacy menace, an unruly private sector "big brother" reviled by human rights advocates worldwide?[6] Is the skeptic of IT Corporation's dominant presence justified or

---

[1] Introna, Lucas D and Nissenbaum, Helen. "Shaping the Web: Why the Politics of Search Engines Matters." *The information society*, vol. 16, no. 3, 2000, pp. 169, 171.

[2] '"Inside the Googleplex." *The Economist*, 30 August 2007, www.economist.com/node/9719610. Accessed 10 May 2017.

[3] Tene, Omer. "What Google Knows: Privacy and Internet Search Engines." *Utah Law Review*, Forthcoming, 2007, p. 1432.

[4] Ibid, pp. 1435.

[5] Battelle, John. *The Search: How Google and Its Rivals Rewrote the Rules of Business and Transformed Our Culture*. Penguin, 2005, p.6.

[6] Avet, Traci. "Who's Afraid of Google?." *Library Journal*, vol. 131, no. 10, 2006, p. 154.

overstated? What personal data should IT Corporation allowed to control and process? What rules should regulate access to IT Corporation's data mine? What were the court cases take place and were they sufficient to represent the personal data protection crisis? These are the main issues mentioned in this Chapter.

3.1.1. The impact of Internet Services on the user's right to personal data protection

At First, there are obviously needs of business to improve their capacity to operate in New Informative Market, E-Commerce Society. Furthermore, The Corporate prefers a wide open Market Society for freedom on commercial activities. For accomplish their goal, the Private Sector has been proposing for less State intervention in order to boost the creativity to invent new products. The new products and services in forthcoming market are Information and Communication Technology (ICT)'s off springs which have been invented by employing various forms of data processing services. Moreover, Governments have been stimulated by private sectors to reform their efficiency and save corporate cost on processing Personal Data. Hence, there is an evident on the 'unavoidable' economic and social conditions which could be proved by the economic figures[7] that Western States must support their private sector to generate more productivity in a time of Economic Regression.

IT Corporation is the recently new mega power in information-based society which could provide various services to a vast majority of internet surfers and turn users into their products[8] by data processing. However, the penetration and collection of personal data by IT Corporation are unpredictable high and deep in long run.

IT Corporation's success was built on the commercial surveillance of civilians through "services": web search, email, social networking, et cetera. But IT Corporation's development in recent years has seen it expand its surveillance enterprise by controlling

[7] Ruddick, Graham. "Online Shopping to Grow by £320bn in Three Years." *The Telegraph,* 7 Jun 2015, www.telegraph.co.uk/finance/newsbysector/retailandconsumer/11657830/Online-shopping-to-grow-by-320bn-in-three-years.html. Accessed 2 May 2016.

[8] Vaidhyanathan, Siva. *The Googlization of Everything: (and Why We Should Worry)*. Univ of California Press, 2012, p. 3.

mobile phones and tablets. The Overshadow of IT Corporation on Internet users is enormous because surfers make some applications as the default web-browser or search engine. [9]

Moreover, IT Corporation has a dominant smart phone operation system (IOS of Apple, Android and Microsoft) to promote their web browser. The success of Google's mobile operating system, Android, launched in 2008, has given Google an 80 percent share of the smart-phone market. Google claims that over a billion Android devices have registered themselves, at a rate now of more than a million new devices a day.[10] Through Android, Google controls devices people carry on their daily routine and use to connect to the internet. Each device feeds back usage statistics, location, and other data to Google. This gives the IT company unprecedented power to surveil and influence the activities of its user base, both over the network and as they go about their lives extending IT Corporation's surveillance capabilities farther into the space around their users.[11]

The prominent book 'Google and the Law; Empirical Approaches to legal aspects of knowledge-economy business models'[12] addresses various effects IT Corporation brings to legal atmosphere. Nonetheless, the vital issue on data processing and data mining are missed out. Howbeit, the efficiency of governance models on Internet Service Providers (ISPs) is relevant with diverse conditions. In different States and Regions, The design and implementation of regulatory regime are significant conditions.

Due to various human rights defenders reports, Privacy International, recently ranked IT Corporation 's privacy practices including Google, Microsoft, Yahoo, Amazon and eBay are merely meet Personal Data protection standard set by legal frameworks.[13] Privacy

[9] "Why Google Pays 10 Billion USD to Its Competitor Mozilla?." *Pubarticles*, http://articles.pubarticles.com/why-google-pays-10-billion-usd-to-its-competitor-mozilla-1324916942,640235.html. Accessed 31/10/2012.

[10] "Q1 2014 Smartphone OS Results: Android Dominates High Growth Developing Markets." *ABIresearch*, 6 May 2014, www.abiresearch.com/press/q1-2014-smartphone-os-results-android-dominates-hi/. Accessed 2 Apr. 2015.

[11] Yarow, Jay. "This Chart Shows Google's Incredible Domination of the World's Computing Platforms." *Retrieved April*, vol. 23, 2014.

[12] Lopez-Tarruella, Aurelio. "Introduction: Google Pushing the Boundaries of Law." *Google and the Law*, Springer, 2012, pp. 4-5.

[13] Simpson, Gemma. "Google Scores Lowest in Privacy Rankings." *ZDNet*, www.zdnet.com/article/google-scores-lowest-in-privacy-rankings/. Accessed 29 Jun. 2015.

International describes some IT Corporations as "an endemic threat to privacy."[14] It criticized IT Corporation's "aggressive use of invasive or potentially invasive technologies and techniques" and claimed the company "fails to follow generally accepted privacy practices such as the OECD Privacy Guidelines and elements of EU data protection law."[15] The EU data protection regulators had launched an investigation into Google's data retention and privacy practices,[16] which was extended to cover other search engines as well.[17] Moreover, the Electronic Privacy Information Center (EPIC), a leading right to privacy advocate, filed a complaint with the Federal Trade Commission, arguing Google's contemplated merger with long-time privacy nemesis Double-Click must be blocked.[18] In 2012 the EPIC appealed to the United States District Court for the District of Columbia seeking disclosure of any communications between NSA and Google Inc. regarding encryption and cyber security.[19] The case may lead to the revelation of the cooperation between NSA and IT Corporation which impact to Personal Data Protection will be discussed in this Chapter.

3.1.2. Big IT corporation's Policy and Practice on Personal Data Protection

IT Corporation records all search queries linked to a specific Internet Protocol (IP) address.[20] Thus the Policy and Practice of IT Corporation will definitely influence the right to personal data protection of millions people in cyberspace.

In IT Corporations' privacy policy, the company usually states: Our servers automatically record information that your browser sends whenever you visit a web site.

[14] "A Race to the Bottom: Privacy Ranking of Internet Service Companies." *The Citizen Lab*, 13 Jun. 2007, https://citizenlab.org/2007/06/a-race-to-the-bottom-privacy-ranking-of-internet-service-companies/. Accessed 29 Jun. 2015.

[15] Ibid.

[16] Global Privacy Counsel. *Article 29 Working Party Letter to Mr. Peter Fleischer on Google*. 16 May 2007.

[17] Article 29 Working Party. *Press Release*. Brussels, 21 June 2007.

[18] "Complaint and Request for Injunction, Request for Investigation and for Other Relief." Federal Trade Commission, 20 Apr. 2007, www.epic.org/privacy/ftc/google/epic_complaint.pdf. Accessed 29 Jun. 2015.

[19] United States District Court for the District of Columbia. *Case 11-5233 EPIC vs. NSA*. 05/11/2012.

[20] Sookman, Barry B. *Computer, Internet and Electronic Commerce Terms: Judicial, Legislative and Technical Definitions*. Carswell, 2001, pp. 301–302.

These server logs may include information such as your web request, Internet Protocol address, browser type, browser language, the date and time of your request and one or more cookies that may uniquely identify your browser.[21]

IT Corporations cumulate Big Data by using the 'Compulsory Consent terms and Conditions' model. This contract of application form is usually used by ISPs to address issues of data privacy. Nonetheless users are given 'freedom of choice' to opt in to or opt out of data collection activities[22]without reading the Terms and Conditions for using such services carefully.

IT Corporation has been criticized both for disclosing too much information to governments too quickly and for not disclosing information that governments need to enforce their laws. In April 2010, Google the most prominent IT Corporation, for the first time, released details about how often countries around the world ask it to hand over user data or to censor information.[23] Online tools make the updated data available to everyone.[24]

Most IT Corporations also analyzes search-query logs for revenue-generating purposes, particularly for targeting and maximizing the effectiveness of advertisements, such as Google, after all, is an advertising company.[25] The predominant business model for search engines is contextual advertising, in which, alongside organic search results, users are displayed advertisements, most commonly textual, that are relevant to their search.[26] The name of the game in online advertising, which is dominated by the pay-per-click (PPC) method of billing,[27] is maximizing click-through rate (CTR), that is, the number of times

[21] "Privacy Policy – Privacy & Terms – Google." *Google*, www.google.com/policies/privacy/. Accessed 7 Nov. 2015.

[22] Cohen, Julie E. "Examined Lives: Informational Privacy and the Subject as Object." *Stanford Law Review*, 2000, pp. 1373-1438.

[23] Shields, Maggie. "Google Reveals Government Data Requests and Censorship." *BBC News*, 20 Apr. 2010.

[24] "Government Requests." *Google Transparency Report*, www.google.com/transparencyreport/removals/government/. Accessed 6 Nov. 2015.

[25] Hansell, Saul. "Google Wants to Dominate Madison Avenue, Too." *The New York Times*, 30 Oct. 2005, www.nytimes.com/2005/10/30/business/yourmoney/google-wants-to-dominate-madison-avenue-too.html. Accessed 7 Nov. 2015.

[26] Grimmelmann, James. "The Structure of Search Engine Law." *Iowa L. Rev.*, vol. 93, 2007, p. 1.

[27] Vangie, Beal. "What Is Pay per Click (PPC)?." *Webopedia Definition* www.webopedia.com/TERM/P/PPC.html. Accessed 7 Nov. 2015.

users who visit a web page featuring an advertisement actually click the ads.[28] And in order to maximize CTR, search engines gauge user tastes, preferences, interests and needs. Google CEO Eric Schmidt stated: "If we target the right ad to the right person at the right time and they click it, we win."[29] Targeting "the right ad to the right person at the right time"[30] requires knowing the users; and knowing the users means analyzing their search history,[31] given the increasingly small costs of data warehousing,[32] and makes data processing more profitable.

Even Google may said the "search engines do not sell users' personally identifiable information to third parties,[33] However, Search engines do share user data with subsidiaries, affiliated companies, and other "trusted" business partners for the purpose of data processing and the provision of services.[34] In addition, they retain the right to transfer data to a third party in case of a merger or consolidation.[35]

The transparent of IT Corporations can be reflected by their report of Transparency, in Google Report, which describes the cooperation with Governments around the world. Between July and December 2009, Brazil topped the list for user data requests with 3,663, while the US made 3,580, the UK 1,166, and India 1,061. Brazil also made the largest number of requests to remove content with 291, followed by Germany with 188, India with 142, and the US with 123. Google, who stopped offering search services in China a month

[28] Ibid.

[29] Hansell, Saul. "Google Wants to Dominate Madison Avenue, Too." *The New York Times*, 30 Oct. 2005, www.nytimes.com/2005/10/30/business/yourmoney/google-wants-to-dominate-madison-avenue-too.html. Accessed 7 Nov. 2015.

[30] "Google PPC Online Advertising." *Google AdWords – Google*, https://adwords.google.com/home/. Accessed 7 Nov. 2015.

[31] "Make Money Online through Website Monetization." *Google AdSense*, www.google.com/adsense/start/#/?modal_active=none. Accessed 7 Nov. 2015.

[32] Markoff, John. "Redefining the Architecture of Memory." *The New York Times*, 11 Sep. 2007. www.nytimes.com/2007/09/11/technology/11storage.html. Accessed 7 Nov. 2015.

[33] "Privacy Policy – Privacy & Terms – Google." www.google.com/policies/privacy/. Accessed 7 Nov.2015.

[34] The term "trusted" is not defined in the Google and Yahoo privacy policies.

[35] "Yahoo Privacy Center." *Yahoo*, https://policies.yahoo.com/us/en/yahoo/privacy/index.htm. Accessed 7 Nov. 2015.

before the data was released, said it could not release information on requests from the Chinese government because such information is regarded as a state secret.[36]

Google's chief legal officer said, "The vast majority of these requests are valid and the information needed is for legitimate criminal investigations or for the removal of child pornography"[37]. The main problem of cooperation with State Authority is whether all coordination is reported or announced only the cases which are in the line of the law.

3.1.3. How have IT corporation done their duty as the Data Controller and Processor

This section brings the 6 basic principles of Data Controller and Processor included in EU Directive and relating instruments as a framework to analyze the practice and policy of IT Corporation. For easier understanding, IT Corporation's service which will be used as example is Search Engine, either solo search engine or hybrid browser-search engine, since it is popular and gain plenty personal data form internet users.

Principle 1 – purpose and manner of collection of personal data

The prohibition against secret databases is one of the doctrinal foundations of European data protection law, survived following decades of totalitarian regimes that used information in secret databases to police and terrorize citizens into conformity and submission.[38] Data aggregation is the "gathering together of information about a person."[39] Solove explains that "combining information creates synergies". When analyzed, aggregated information can reveal new facts about a person that she did not expect would be known about her when the original, isolated data was collected."[40] User search-query logs aggregate vast amounts of data from tiny bits of information revealed by user click by click search by

[36] Shields, Maggie. "Google Reveals Government Data Requests and Censorship." *BBC News*, 20 Apr. 2010.

[37] Ibid.

[38] Simitis, Spiros. "Reviewing Privacy in an Information Society." *University of Pennsylvania Law Review*, vol. 135, no. 3, 1987, pp. 707, 715–17.

[39] Solove, Daniel J. "A Taxonomy of Privacy." *University of Pennsylvania Law Review*, 2006, pp. 477, 479–487, 507.

[40] Ibid.

search history.[41] This evident gave the wealth and depth of information collected in search query logs that contain vast majority of searches aggregated over a period of uses. Even the few users who are aware of search engines' data compilation practices probably underestimate the impact of search-query logs on their privacy, effectively making their lives "transparent" over time.[42]

Data log or Big Data collection concentrated is the nature of the search-engine industry. There are voluminous data being compiled by search engine controller and then processor. Furthermore, Government, private litigants, and hackers alike know that IT Corporations store this personal information. It creates new type of risk and insecure by gather Mega Data Mine and even worse when collects data more than the legitimate purpose. The more it collects the more devastate result it could affect to the protection of personal data.

Principle 2 – accuracy and duration of retention of personal data

This section concern of the distortion of information, which is "the manipulation of the way a person is perceived and judged by others, and involves the victim being inaccurately exposed to the public."[43] Recognizing the potentially harmful effects of inaccurate information, the EU Data Protection Directive provides that personally identifiable information must be "accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that data which are inaccurate or incomplete, having regard to the purposes for which they were collected or for which they are further processed, are erased or rectified."[44] In addition, individuals in the EU enjoy the right to access their personally identifiable information without delay, and to rectify, erase, or block data that are inaccurate or incomplete.[45] The combination of inaccurate and misleading data, ease of government

[41] Tene, Omer. "What Google Knows: Privacy and Internet Search Engines." *Utah Law Review*, Forthcoming, 2007, p. 1458.

[42] Battelle, John. *The Search: How Google and Its Rivals Rewrote the Rules of Business and Transformed Our Culture*. Penguin, London, 2005, pp. 181-94.

[43] Solove, Daniel J. "A Taxonomy of Privacy." *University of Pennsylvania Law Review*, 2006, pp. 477, 479–87, 550.

[44] EU. *Directive 95/45/EC*. 1995, Article 6(1)(d).

[45] Ibid, Article 12.

access, and lack of transparency and accountability to users, makes user search-query logs highly problematic from a privacy perspective.

Moreover, after many cases in Court of Justice of European Union (CJEU) which will describe later, the right to be forgotten is the direct reflection from this kind of search engine effect. Since anything pop-up on internet once it almost has never been erased, the wrong searchable information could lead to misunderstanding to target people. Even sometime the fault story has been rectified in real world but the information is still online somewhere ready for searched.

Similarly, Information in search-query logs may be highly misleading, with potentially troubling results for users.[46] A user searching for "Death of King or President" is not necessarily a terrorist or criminal intention; instead, it might be a researcher finding for a history evident or primary school students did their homework. As well as, a user searching for "how to plant opium" is not absolutely considering an agricultural endeavor; it may be a social worker concerned with growing drug use in neighborhood or it's a part of PhD thesis.

Principle 3 – use of personal data

EU Data Protection Directive includes the principle of purpose specification.[47] Under the purpose specification principle, personally identifiable information obtained for one purpose must not be used or made available for another purpose without the affected individual's prior informed consent.[48] Because secondary use of personally identifiable information "creates a dignitary harm . . . emerging from denying people control over the future use of their data, which can be used in ways that have significant effects on their lives."[49] Solve points out that "secondary use resembles breach of confidentiality, in that there is a betrayal of the person's expectations when giving out information."[50]

[46] Tene, Omer. "What Google Knows: Privacy and Internet Search Engines." *Utah Law Review*, Forthcoming, 2007, p. 1459.

[47] Council of Europe. *Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data*. 1981, Article (5)(b); EU. *Directive 95/46/EC*. 1995, Article 6(1)(b).

[48] Ibid, Article 6(1)(b); Ibid, Article 2(a).

[49] Solove, Daniel J. "A Taxonomy of Privacy." *University of Pennsylvania Law Review*, 2006, pp. 521-522.

[50] Ibid, p. 522.

In case of user search-query logs, users may expect that information to be used by IT Corporation to respond to your query only and users most certainly do not expect IT Corporation to disburse this information to the government or private parties engaged in litigation against you.[51] When IT Corporation uses the information in your search-query log for purposes diverging from those you reasonably envisaged, it breaches your trust, your "reasonable expectation of privacy",[52] as well as the purpose specification principle.

In reality, IT Corporation not only aggregate your current query with all of your past searches and mine the data in order to improve its service but also make use of this information to target you with effective advertising or analyze your ad-viewing behavior.[53] The consent of user is needed, implicitly at least, to all of these uses, since they are specified in IT Corporation's privacy policy but not many users may notice the terms and conditions that written in instant contract. Nevertheless, implicit consent argument is tenuous at fundamental as a clause to invoke an unfair instant contract.

First, consent is based in this case on a browse-wrap agreement,[54] which must be assembled from several distinct web pages[55] and is hard to comprehend. Second, Search Engine Corporation's privacy policy remains constructively opaque concerning the *primary* use of search-query logs, rendering secondary use all the more difficult to accept.[56]

IT Corporation's use of search data for secondary purposes and the privacy issues it raises expose a broad rift between U.S. and European privacy law. The purpose specification principle, so deeply ingrained in EU law,[57] is not at all evident in the United States, where the underlying assumption has traditionally been that as between any individual and a company

[51] Tene, Omer. "What Google Knows: Privacy and Internet Search Engines." *Utah Law Review*, Forthcoming, 2007, p. 1462.

[52] Concurring, Harlan J. *Case 389 U.S. 347 Katz v. United States*. 1967, pp. 360–61.

[53] "Privacy Policy – Privacy & Terms – Google." www.google.com/policies/privacy/. Accessed 7 Nov.2015.

[54] US Second Circuit Court. *Case 306 F.3d 17 Specht v. Netscape Communications Corp.* 2002, para. 22.

[55] "Google Privacy Chief Talks." www.out-law.com/page-8285. Accessed 7 Nov. 2015.

[56] Tene, Omer. "What Google Knows: Privacy and Internet Search Engines." *Utah Law Review*, Forthcoming, 2007, p. 1463.

[57] EU. *Charter of Fundamental Rights of the European Union*. *Communities.* 2000.

collecting her personally identifiable information, it is the company that owns the data and may use, reuse, or sell it to third parties at will.[58]

Principle 4 – security of personal data

In order to government and private actors serving legal process, IT Corporation's information goldmine is bound to attract hackers and data thieves. Valuable databases get infiltrated all the time, regardless of the robustness of security measures. Security breaches abound even in highly guarded industries such as financial services, health services, and telecommunications.[59] Unfaithful employees may sell data to marketing company or criminals; negligent employees lose laptops; computers are stolen and back-up tapes lost; passwords are possibly compromised and firewalls lowered.

The point is that no matter what security measures are in place, data stored will eventually be data breached. The best method to secure data, and consequently guard individuals' privacy, [60] is not to store them in the first place.[61] To sum up, far from being restricted to use by search engines themselves, search-query logs may haunt users in future government investigations or private litigation and can be illicitly accessed by hackers and data thieves.[62]

Principle 5 – information to be generally available

An analogy of the basic prohibition on confidential databases is the right of individuals in Europe to be notified which data are collected about them, by whom, and for what purposes.[63] Solove refers to "the failure to provide individuals with notice and input

[58] Cohen, Julie E. "Examined Lives: Informational Privacy and the Subject as Object." *Stanford Law Review*, 2000, pp.1373-4.

[59] Kennedy, John B. "Slouching towards Security Standards: The Legacy of California's SB 1386." *Privacy Law Institute (Seventh Annual)*, 2006, pp. 91, 97–98.

[60] Brin, David. *The Transparent Society: Will Technology Force Us to Choose between Privacy and Freedom?*. Basic Books, 1999. pp. 8–9.

[61] LoPucki, Lynn M. "Human Identification Theory and the Identity Theft Problem." *Tex. L. Rev.*, vol. 80, 2001, pp. 89, 108.

[62] Tene, Omer. "What Google Knows: Privacy and Internet Search Engines." *Utah Law Review*, Forthcoming, 2007, p. 1457.

[63] EU. *Directive 95/46/EC*. Articles 10–11.

about their records as *exclusion*."[64] He explains that "exclusion creates a sense of vulnerability and uncertainty in individuals. . . . In a world where personal information is increasingly used to make important decisions about our lives, powerlessness in this arena can be significantly troublesome."[65]

Public awareness to the extent of data collection by search engines is minimal. A survey held pursuant to the government's request for Search Engine Corporation's search records reveals that "89% of respondents believe that their Web searches are kept private, and 77% believe that Google web searches do not reveal their personal identities."[66] To a great extent, then, many users think Google's collection of search queries is a de facto "secret database." [67]

In its complaint to the FTC concerning the Google/Double Click merger, EPIC points out that a user must click on four links from Google's ubiquitous homepage[68] in order to obtain information concerning the company's data collection practices.[69] Moreover, even the full privacy policy fails to explain clearly what Google does with information in search-query logs. In addition, it is not clear whether and to what extent users have access to their search-query logs.[70]

Principle 6 – access to personal data

Individuals are entitled to access their personally identifiable information and, if necessary, correct or amend them.[71] User access to search-query logs is now provided as part of the IT Corporation Web History service. Users of IT Corporation Web History may access their search-query logs and edit or delete items therein. Yet such access comes at a significant

[64] Solove, Daniel J. "A Taxonomy of Privacy." *University of Pennsylvania Law Review*, 2006, p. 523.

[65] Ibid, pp. 523-524.

[66] Rosencrance, Linda. "Survey Finds Solid Opposition to Release of Google Data to Feds." *Computerworld*, 24 Jan. 2006, www.computerworld.com/article/2561275/data-privacy/survey-finds-solid-opposition-to-release-of-google-data-to-feds.html. Accessed 7 Nov. 2015.

[67] Ibid.

[68] "Google Privacy Chief Talks." www.out-law.com/page-8285. Accessed 7 Nov. 2015.

[69] Winston, Joel. "Letter from Joel Winston, Acting Assoc. Dir., Div. of Fin. Practices, FTC, to Christine Varney, Esq." *Hogan & Hartson*, 2001.

[70] "Privacy Policy – Privacy & Terms – Google." www.google.com/policies/privacy/. Accessed 7 Nov.2015.

[71] EU. *Directive 95/46/EC*. 1995, Article 12.

privacy cost, because IT Corporation stores not only the *search queries* of Web History users, but also the *web pages* visited. Moreover, the users who do not subscribe to Web History, ostensibly due to that very "cost", [72] are arguably already paying a similar privacy price, given IT Corporation's retention of their search-query logs.

Finally, counter to Web History users, search engine users are not provided with the opportunity to edit or delete search-query logs (at least not by simple means).[73]

3.2. Hard Case Study under US legal system

This section will bring in the cases from the practice in the real-life situations and the case studies present in the courts. The cases from the everyday-life practice illustrate the relationship between the IT Corporation and State Authority. The Court Case studies emphasize the legal precedent of Personal Data Protection when it encounters with inconvenient incidents in various scenarios.

3.2.1. Suspicion cases on the Relation between Corporations and State Agencies

The exploration of the cooperation or relationship between State and IT Corporation is crucial to understand the impacts of Data Processing on Personal Data Protection. It seems to be sure that IT Corporation has a power to control over personal data. People do not know whether IT Corporation will share it with government or not while some IT Corporations usually share personal data and information with state agencies.[74] This kind of relation implies that there might be consistently sharing of information among State Authorities and Private Companies on the basis of reciprocity or by the mandate law enforcement.

In addition to personal data protection and exercising security technologies, sustaining trust in cyberspace requires rules, transparent practices, accountability standards, and means

[72] Tene, Omer. "What Google Knows: Privacy and Internet Search Engines." *Utah Law Review,* Forthcoming, 2007, p. 1461.

[73] Ibid, p.1462.

[74] Ingram, Mick. "Google Publishes Figures on Government Requests for Data." *World Socialist Web Site, 26* www.wsws.org/en/articles/2010/04/goog-a26.html. Accessed 31 Oct. 2012.

of redress acceptable to users.[75] Accordingly, International efforts for agreements to protect and sustain cyberspace security are unavoidable in the macro policy of State and micro practice of IT Corporation.

However, do you think it is just the IT Corporation who really uses processed/collected data? On the contrary, state especially government and security agencies do sharing, mining and processing the information with IT Corporation[76] occasionally. The Old School excuses of the state are: to support the flourishing of economy and protect National Security[77] which are vague and undermine the fundamental rights of individual as a customer and people. As such, the Dilemma like theme question has been sprouted.

The notorious US Global Internet Surveillances on PRISM program, NSA cooperates with 9 big ICT Corporations on Electronic Mass Surveillance,[78] gave evidences confirming the threats from IT Corporation on Personal Data Protection of Internet citizen worldwide.

The problems on data collection, mining and processing sharing of ISPs start the controversial arguments at first place.[79] The reveals of state massive electronic surveillance, interception and collection of personal communication and data are highly spotted because US has targeting surveillance on the executive of other states and mass surveillance[80] on everyone in the world. As NSA‘s PRISM project collect data from the most powerful IT Corporations of the world such as Google,[81] Yahoo, Facebook etc. The PRISM project has main objective to watch on every communication devices which connect to the Internet; CPU, Laptop, Pad, Mobile phone. The identification of place time and activity of people

---

[75] Hurwitz, Roger. "Depleted Trust in the Cyber Commons." *DTIC Document*, 2012, p. 26.

[76] "Frequently Asked Questions." *Google Transparency Report,* www.google.com/transparencyreport/userdatarequests/faq/#are_the_observations_comprehensive. Accessed 31 Oct. 2012.

[77] Council of Europe. *Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data*. 1981, Article 9(2)(a).

[78] Bowden, Caspar. *The US Surveillance Programmes and Their Impact on EU Citizens' Fundamental Rights.* 2013, p. 13.

[79] Thompson, Marcelo. "In Search of Alterity: On Google, Neutrality and Otherness." *Google and the Law*, Springer, New York, 2012, Introduction.

[80] Kerschischnig, Georg. *Cyberthreats and International Law.* Eleven International Publishing, Hague, 2012, pp. 245-254.

[81] Lopez-Tarruella, Aurelio. "Introduction: Google Pushing the Boundaries of Law." *Google and the Law*, Springer, New York, 2012, Preamble.

could be track and trace orderly from the Big Data Collection[82] that gathering from Everyday-Life practice.

PRISM was enabled under President Bush by the Protect America Act 2007 and by the FISA Amendments Act 2008, which immunizes private companies from legal action when they cooperate with U.S. government agencies in intelligence collection. In 2012 the act was renewed by Congress under President Obama for an additional five years, through December 2017.[83] According to the FISA Amendments Act of 2008, it gives mandate for "specifically authorizes intelligence agencies to monitor the phone, email, and other communications of U.S. citizens for up to a week without obtaining a warrant" when one of the parties is outside the U.S.[84] which means the rights of Non-US Citizen are ignored.

Internal NSA presentation slides included in the various media disclosures show that the NSA could unilaterally access data and perform "extensive, in-depth surveillance on live communications and stored information" with examples including email, video and voice chat, videos, photos, voice-over-IP chats (such as Skype), file transfers, and social networking details.[85]

The NSA databank, with its years of collected communications, allows analysts to search that database and listen "to the calls or read the emails of everything that the NSA has stored, or look at the browsing histories or Google search terms that you've entered, and it also alerts them to any further activity that people connected to that email address or that IP address do in the future."[86]

PRISM data using terms intended to identify suspicious communications of targets whom the analysts suspect with at least 51 percent confidence to not be US citizens. Training materials for analysts tell them that while they collect of foreign U.S. data, "it's nothing to

[82] Ingram, Mick. "Google Publishes Figures on Government Requests for Data." *World Socialist Web Site, 26* www.wsws.org/en/articles/2010/04/goog-a26.html. Accessed 31 Oct. 2014.

[83] Shane, Peter M. "Foreword: The NSA and the Legal Regime for Foreign Intelligence Surveillance." 2014, p. 25.

[84] McAllister, Neil. "Senate Votes to Continue FISA Domestic Spying through 2017-All Proposed Privacy Amendments Rejected." *The Register,* 29 Dec. 2012.

[85] Greenwald, Glenn and MacAskill, Ewen. "NSA Prism Program Taps in to User Data of Apple, Google and Others." *The Guardian*, vol. 7, no. 6, 2013, pp. 1-43.

[86] Rea, Kari. "Glenn Greenwald: Low-Level NSA Analysts Have 'Powerful and Invasive'search Tool." *ABC News*, vol. 28, 2013.

worry about"[87] which shows the ignorance to the right to data protection of Non-US citizen worldwide.

3.2.2. Legal Analysis on IT Corporation cases in the US Court

Various court cases brought against US National Security Authorities as the many agencies have diverse surveillance programmes which may breach right to personal data protection of Internet users worldwide. The United States Court of Appeals held decisions in regard to non-governmental organization request relating communications between NSA and IT Corporation. The problem come from the validation that court had given under the broad ambit of Sections of the National Security Agency Act because any internal risk assessment conducted by NSA constitutes as an undisputed NSA function. The result is that the court protects IT Corporation and National Security Authority interests at the expense of individual rights regarding personal data protection. These decisions benefit private sector and intelligence unit because they get to work with each other in handling cyber security issues without the fear of potential critiques from the public as a result of information being revealed to individuals as a result of a information request. Despite the court decision were supported in a legal context, its decision to place national security concerns ahead of the right to access government-held information undermines Individual and Public the ability for to know about the effects of cyber attacks on businesses and the coordination between IT Corporation and National Intelligence Authority. The effects of court decisions to personal data protection will be scrutinized below as well as the changes that court may post through their verdicts.

3.2.2.1. Right to Personal Data Protection of Individual

The decisions that US Courts have made set the precedent on Data Collecting and Sharing of IT Corporation and State Authority because they are the subjects under US jurisdiction.[88]

---

[87] Gellman, Barton and Poitras, Laura. "US, British Intelligence Mining Data from Nine Us Internet Companies in Broad Secret Program." *The Washington Post*, vol. 6, 2013.

[88] Fahey, Elaine and Curtin. Deirdre. *A Transatlantic Community of Law: Legal Perspectives on the Relationship between the EU and US Legal Orders.* Cambridge University Press, UK, 2014.

On December 16, 2013, the U.S. District Court for the District of Columbia ruled in *Klayman v. Obama* that the NSA's bulk collection of domestic telephone call detail records likely violated the Fourth Amendment (right to privacy, data privacy and personal data protection). The Court of Appeals for the D.C. Circuit found that the Plaintiff, as a Verizon customer, had standing to challenge the constitutionality of the NSA's collection of call detail records.[89] This case celebrated the full constitutional rights enjoyment of US citizen but the protection for Non-US citizen stills remain a question.[90]

Since this collection was not based on any particularized suspicion of wrongdoing, all call records were collected in bulk from ISPs every day. Specifically, the FISA order required that Verizon turn over "all call detail records or 'telephony metadata' created by Verizon for communications (i) between the United States and abroad; or (ii) wholly within the United States, including local telephone calls." Once revealed, the government confirmed the existence of the Verizon order and of the telephone metadata program.[91] In this case, the Plaintiff, a Verizon Wireless customer, brought suit in the U.S. District Court for the District of D.C., alleging that the government is conducting a "secret and illegal scheme to intercept and analyze vast quantities of domestic telephone communications [and] of communications from the Internet and electronic service providers."[92]

On May 7, 2015, the U.S. Court of Appeals for the Second Circuit reversed a lower court decision and held that the "bulk telephone metadata program is not authorized by [Section] 215" of the USA PATRIOT Act. The court first rejected the Government's argument that the ACLU and other plaintiffs lacked "standing" to bring the case under Article III of the U.S. Constitution. The court found that the plaintiffs in this case "need not speculate that the government has collected, or may in the future collect, their call records. To the

[89] U.S. District Court for the District of Columbia. *Case 957 F. Supp. 2d 1 Klayman v. Obama.* 2013, 16/12/2013.

[90] Kerr, Orin S., "The Fourth Amendment and the Global Internet." *GWU Law School Public Law Research,* Paper No. 2014-30, 2014.

[91] Donohue, Laura K. "Bulk Metadata Collection: Statutory and Constitutional Considerations." *Harvard Journal of Law and Public Policy*, vol. 37, no. 3, 2014, p. 759.

[92] Medine, David et al. "Report on the Telephone Records Program Conducted under Section 215 of the USA Patriot Act and on the Operations of the Foreign Intelligence Surveillance Court." *Privacy and Civil Liberties Oversight Board*, vol. 23, 2014.

contrary, the government's own orders demonstrate that appellants' call records are indeed among those collected as part of the telephone metadata program." Finally, the court rejected the Government's argument that the NSA metadata collection was authorized under Section 215 of the USA PATRIOT Act, which allows the FBI to apply to the Foreign Intelligence Surveillance Court for an order requiring the production of records or "tangible things" that are "relevant to an authorized investigation."[93] Specifically, the court rejected the Government's interpretation of the term "relevant" to include all domestic telephone records. The court found that "such an expansive concept of 'relevance' is unprecedented and unwarranted" under the law, and would not be equivalent to the permissible scope of a subpoena in the grand jury context. The court also rejected the argument that Congress "implicitly" endorsed this broad interpretation of the term "relevance" when it reauthorized the provision in 2010 and 2011.[94] The court declined to rule on the Fourth and First Amendment issues because it found the program was not legitimate by the statute.

The decision in the *Hearst Case* is a reasonable indicator where U.S. courts are coming from: The U.S. Court of Appeals for the Second Circuit held that a newspaper was not required to remove stories about a woman's arrest, even though the arrest was later expunged from her record.[95] In so holding, the judge observed that the expunged record is a legal fiction that "does not and cannot undo historical facts or convert once-true facts into falsehoods."[96] Although in a recent defamation case before a New York state trial court, a judge commented that a statutory "right to be forgotten" would, "under certain conditions, give plaintiffs the opportunity to attain the redress they deserve,"[97] the comment remains an outlier without precedential effect.

[93] US Court of Appeals Second Circuit. *Opinion ACLU v. Clapper*. 7 May 2015.

[94] Medine, David et al. "Report on the Telephone Records Program Conducted under Section 215 of the USA Patriot Act and on the Operations of the Foreign Intelligence Surveillance Court." *Privacy and Civil Liberties Oversight Board*, January, vol. 23, 2014, p. 96.

[95] US Court of Appeals for the District of Columbia. *Case 777 F.3d Martin v. Hearst Corp*. 2015, paras. 546, 552,

[96] Ibid, para. 551.

[97] US Trial Court of New York state. *Case 151769/2013 Anonymous v. Does*. 3 Dec. 2014, para. 4.

In *Electronic Privacy Information Center v. National Security Agency*[98], the United States Court of Appeals for the District of Columbia Circuit held that the NSA's *Glomar* response, in regard to EPIC's FOIA request regarding communications between NSA and Google, was valid under the broad ambit of Section 6 of the National Security Agency Act because any threat assessment conducted by NSA constitutes as an undisputed NSA function.[99] The result is that the court protects business interests at the expense of individual rights regarding free access to information.[100] This decision benefits businesses because they get to work with NSA in handling cyber security issues without the fear of potential backlash from the public as a result of information being turned over to individuals as a result of a FOIA request.[101] Even though the decision was supported in a legal context, its decision to place national security concerns ahead of the right to access government-held information undermines FOIA and the ability for the public to know about the effects of cyber attacks on businesses.[102]

Since the orders of the FISC are classified and companies are required to maintain secrecy with regard to the assistance they are required to provide, there are no avenues, judicial or administrative, for either EU or US data subjects to be informed of whether their personal data is being collected or further processed.[103] There are no opportunities for individuals to obtain access, rectification or erasure of data, or administrative or judicial redress which are data subjects' rights.

Even though some of these cases are not directly base on the communication in Cyberspace but it also contains the same basis on arbitrary interference communication by State. Especially the relationship between ICT Corporation and National Security Agency, the case can shine the light to more accountable procedure to conduct mass surveillance or

[98] US Court of Appeals for the District of Columbia. *Case 678 F.3d Electronic Privacy Information Center v. National Security Agency*. 2012, para. 926.

[99] Ibid, para. 935.

[100] Chazen, Joshua R. "Electronic Privacy Information Center V. National Security Agency: How Glomar Responses Benefit Businesses and Provide an Epic Blow to Individuals." *J. Bus. & Tech. L.*, vol. 9, 2014, p. 328.

[101] Ibid, pp. 329-31.

[102] Ibid, pp. 332-3.

[103] Council of the European Union. *Report on the findings by the EU Co-chairs of the ad hoc EU-US Working Group on Data Protection*. 2013, p. 27.

non-targeting spy on vast majority people. The court decision make standard and precedent on exception of exercising data subject's right to personal data protection which base on more precise conditions.

3.2.2.2. Obligation of the Data Controller and Data Processor

On March 17, 2009, Electronic Privacy Information Center (EPIC) filed a complaint with the Federal Trade Commission (FTC), urging an investigation into Google's cloud computing services to determine "the adequacy of the privacy and security safeguards." The complaint followed a reported security breach of Google Docs.[104] EPIC observed that Google repeatedly assured consumers that their services stored user-generated data securely, but had opted to not encrypt the personal information stored or transmitted on its computer network by default, automated process decision without embedded privacy by design, which might compromise the integration of personal data.

On February 4, 2010, EPIC filed a Freedom of Information Act ("FOIA") request with the National Security Agency ("NSA"). EPIC requested the following agency records (Data Retention):[105]

- All records concerning an agreement or similar basis for collaboration, final or draft, between the NSA and Google regarding cyber security;
- All records of communication between NSA and Google concerning Gmail, including but not limited to Google's decision to fail to routinely encrypt Gmail messages prior to January 13, 2010; and
- All records of communications regarding NSA's role in Google's decision regarding the failure to routinely deploy encryption for cloud-based computing service, such as Google Docs.

In *Elecronic Privacy Information Center v. National Security Agency*, the D.C. Circuit held that the NSA's *Glomar* response sufficiently satisfied the exemption requirements of the Act because threat assessment is an undisputed NSA function and,

[104] Drummond, David. "A New Approach to China." *The official Google blog*, vol. 12, 2010.

[105] EPIC. "Freedom of Information Act Request and Request for Expedited Processing." 4 Feb. 2010, https://epic.org/privacy/nsa/foia/NSA-Google_FOIA_Request.pdf. Accessed 16 Nov. 2015.

therefore, the NSA was not required to confirm or deny existence of any responsive records.[106] In reaching this holding, the court correctly determined that if private companies knew their attempts to contact the NSA could be made public through a FOIA request, these companies might not contact the agency, thereby limiting NSA's activities or functions.[107] This decision not only puts federal agencies in a power position but also facilitates public-private partnerships in combating cyber threats.[108] However, this decision negatively impacts the purpose of FOIA and the rights of individuals,[109] and ultimately goes too far by ignoring the public's interest in ensuring their information is under constant protection by companies.[110]

The D.C. Circuit's holding McConnell's idea, A relationship between the private sector and the Government that revolves around national security issues,[111] by allowing the NSA to issue *Glomar* responses in regards to EPIC's request for information regarding NSA communications with Google.[112] By justifying the NSA's decision to issue *Glomar* responses, the court opens the door for businesses to begin communicating with NSA without fear that their problems will be exposed as a result of a FOIA request.[113] This has huge benefits to businesses, which can use NSA resources without fear of private communications with government agencies becoming exposed.[114]The D.C. Circuit analyzed, in the event of a cyber attack on its operations or servers, would be reluctant to work with

[106] US Court of Appeals for the District of Columbia. *Case 678 F.3d Electronic Privacy Information Center v. National Security Agency*. 2012, paras. 934-5.

[107] Ibid, para. 932.

[108] Chazen, Joshua R. "Electronic Privacy Information Center V. National Security Agency: How Glomar Responses Benefit Businesses and Provide an Epic Blow to Individuals." *J. Bus. & Tech. L.*, vol. 9, 2014, pp. 328-332.

[109] Ibid, pp. 332-334.

[110] Ibid.

[111] Former CIA Director. For more information on McConnell, who as of this writing is the Vice Chairman of Booz Allen Hamilton, see http://www.boozallen.com/about/leadership/executive-leadership/.

[112] US Court of Appeals for the District of Columbia, *Case 678 F.3d Electronic Privacy Information Center v. National Security Agency*. 2012, para. 926.

[113] Nakashima, Ellen. "Banks Seek NSA Help Amid Attacks on Their Computer Systems." *Washington Post*, vol. 11, 2013, p. A03.

[114] US Court of Appeals for the District of Columbia. *Case 642 F.3d 1161 Roth v. Dep't of Justice*. 2011.

federal agencies.[115] If private companies are unwilling to report cyber attacks, it would likely limit the ability of federal agencies, such as the

NSA or CIA, to determine the source of these cyber attacks, how to stop or contain them, and analyze the attacks so that they do not happen again. This decision firmly puts businesses in the driver seat and gives the government the means to pursue stronger methods of defense.[116] The NSA can justify its actions based on its Information Assurance mission.[117]

The justification of secret relationship between IT Corporation and National Security Authority is the fact that an agency's judgment to issue a *Glomar* response is given "substantial weight"[118] and the D.C. Circuit did not find it necessary to overturn the NSA's decision to issue a *Glomar* response in this scenario. Section 6 of the NSA Act was already regarded as broad enough to allow agencies to defend their withholding of records more easily.[119] But this broad scope granted to Section 6 of the NSA Act allows government officials to consider information to be classified even when the public already knows about the information.[120]

[115] US Court of Appeals for the District of Columbia, *Case 678 F.3d Electronic Privacy Information Center v. National Security Agency*. 2012, para. 932.

[116] Bumiller, Elisabeth. "Pentagon Expanding Cybersecurity Force to Protect Networks against Attacks." *The New York Times*, vol. 27, 2013, p. A7.

[117] According to the National Security Agency/Central Security Service, "[t]he Information Assurance mission confronts the formidable challenge of preventing foreign adversaries from gaining access to sensitive or classified national security information. The Signals Intelligence mission collects, processes, and disseminates intelligence information from foreign signals for intelligence and counterintelligence purposes and to support military operations. This Agency also enables Network Warfare operations to defeat terrorists and their organizations at home and abroad, consistent with U.S. laws and the protection of privacy and civil liberties."

[118] US Court of Appeals for the District of Columbia. *Case 257 F.3d Students against Genocide v. Dep't of State*. 2001, paras. 828, 840.

[119] US Court of Appeals for the District of Columbia. *Case 565 F.3d Larson v. Dep't of State*. 2009, paras. 857, 868; US Second Circuit, *Case 592 F.3d 60 Wilner v. Nat'l Sec. Agency*. 2009, para. 75.

[120] US Court of Appeals Second Circuit. *Opinion ACLU v. Clapper*. 7 May 2015, paras. 547, 561.

3.2.2.3. Implementation of Personal Data Protection

There are obstacles for public to check the abuse of power of National Security Authorities as most of National Security laws contain a barrier in order to seal the secret by using National Security Matters excuse. Most of the laws, Foreign Intelligence Surveillance Act, Homeland Security Act and Patriot Act set up internal mechanism to approve the subpoena and order for such task force to conduct surveillance. When it comes to the case that public skeptic on the relation between Intelligence Units and IT Corporations, the individual or non-governmental organization must launch complaint to exact Authority or file a law suit to the court.

In EPIC vs. NSA and Google case, EPIC file complaint by letter dated March 10 that the NSA acknowledged receipt of EPIC's FOIA Request and granted EPIC's request for a fee waiver. The NSA's letter invoked FOIA exemption b (3) and Section 6 of the National Security Agency Act in order to issue a Glomar response. A Glomar response is the Agency's act of neither confirming nor denying the existence of Agency records responsive to the Request.[121]

On May 7, 2010, EPIC filed an administrative appeal stating that the NSA had failed to present factual evidence that the requested documents fell within Section 6 and that established FOIA exemptions could sufficiently conceal protected information. The NSA never replied to EPIC's appeal or produced responsive documents.[122] EPIC filed a complaint in United States District Court for the District of Columbia on September 13, 2010.[123] The NSA argued that the Agency was under no obligation to conduct a search prior to determining that any potentially responsive records would implicate the Agency's functions or activities. Judge Richard Leon deferred to the NSA's judgment in a Memorandum Opinion dated July 8, 2011.[124] EPIC filed a Notice of Appeal in the D.C. Circuit Court on September

[121] Electronic Privacy Information Center. *NSA's March 10, 2010 letter acknowledging of receipt of EPIC's FOIA request and invoking the Glomar Response*. 10 Mar. 2010.

[122] Electronic Privacy Information Center. *EPIC's May 7, 2010 Administrative Appeal to the NSA*. 7 May 2010.

[123] Electronic Privacy Information Center. *EPIC's Complaint against NSA*. 13 Sep. 2010.

[124] District Court Memorandum Opinion. *798 F.Supp.2d 26 (D.D.C. 2011)*. 8 Jul. 2011.

9, 2011.[125] Oral argument is schedule for March 20, 2012 before Judge Brown, Judge Kavanaugh, and Judge Ginsburg.[126]

On May 7, 2015, the U.S. Court rejected the Government's argument that the ACLU and other plaintiffs lacked "standing" to bring the case under Article III of the U.S. Constitution. The court then rejected the Government's argument that judicial review of the NSA program was precluded by law, finding that Congress "did not intend to preclude targets of [Section] 215 orders . . . from bringing suit" and found that the plaintiffs could challenge the program under the Administrative Procedure Act.[127]

The intent of the US FISA (and PATRIOT) laws to acquire "foreign intelligence information' concerning people who are not American citizens or legal residents while they are not protected by US laws; Constitution, Privacy Act and Freedom of Information Act. Problems that emerged from FISA were left to the interpretation (in secret proceedings) of the *Foreign Intelligence Surveillance Court* (FISC and the higher Review court FISCR) whose judges are appointed solely by the Chief Justice of the Supreme Court. It appears that the FISA courts agree with the government's argument that it is common in investigations for some indefinitely large corpus of records to be considered "relevant", in order to discover the actual evidence.[128] Some official de-classifications of the secret FISC(R) Opinions might be progress, but have not that far described this logical anomaly.

The targeting and minimisation procedures approved by FISC under Section 702 are aimed at reducing the collection, retention and dissemination of personal data of or concerning US persons. These procedures do not impose specific requirements or restrictions with regard to the collection, processing or retention of personal data of individuals in the EU, even when they have no connection with terrorism, crime or any other unlawful or dangerous activity.[129] Oversight of the surveillance programmes aims exclusively at protecting US persons.

---

[125] Electronic Privacy Information Center. *EPIC's Notice of Appeal*. 9 Sep. 2011.

[126] US Court of Appeals for the District of Columbia. *Opinion*. 20 Mar. 2012.

[127] US Court of Appeals Second Circuit. *Opinion ACLU v. Clapper*. 7 May 2015.

[128] Bowden, Caspar. *The US Surveillance Programmes and Their Impact on EU Citizens' Fundamental Rights.* 2013, p. 12.

[129] Council of the European Union. *Report on the findings by the EU Co-chairs of the ad hoc EU-US Working Group on Data Protection*. 2013, p. 26.

These cases have shown the complicated situations for Non-US citizen data subjects. If EU citizen want to know whether their sensitive personal data is compromised they have no channel to request for acknowledgement or lodge the complaints. Since the Close system of US National Security Laws require the complaint to walk through many stages before reaching the very final end and most of the paths are not for Non-US citizen, EU citizen.

Various layers of oversight by the three branches of Government apply to activities on the base of Section 215 of Patriot Act and Section 702 of FISA. There is judicial oversight for activities that imply a capacity to compel information, including FISC orders for the collection under Section 215 and annual certifications that provide the basis for collection under Section 702. There is no judicial approval of individual selectors to query the data collected under Section 215 or tasked for collection under Section 702. The FISC operates *ex parte* and *in camera*. Its orders and opinions are classified, unless they are declassified. There is no judicial oversight of the collection of foreign intelligence outside the US under Executive Order 12333,[130] which are conducted under the sole competence of the Executive Branch.

Nonetheless, the FISC is extremely resolute, and careful, about ensuring that the NSA and FBI comply with the terms of the FISC's own orders, including the so-called "minimization" requirements–in part because the lawyers in . . . Department of Justice (DOJ)'s National Security Division, take very seriously their responsibility to bring to the court's attention any compliance problems. When it comes to the more fundamental legal questions about the proper statutory and constitutional scope of a proposed program, however, the FISC process is not nearly as thorough or reliable, in large measure because the court hears from only one side.[131]

Moreover, it remains unclear whether Article III of US Constitution would permit a designated advocate to appeal FISC orders to a higher court or whether it is possible

[130] Ibid, p. 27.

[131] Lederman, Marty. "The Kris Paper, and the Problematic FISC Opinion on the Section 215 "Metadata" Collection Program." *Just Security*, 1 Oct. 2013, http://justsecurity.org/2013/10/01/kris-paper-legality-section-215-metadata-collection/. Accessed 14 Feb. 2017.

to conduct an effectively adversarial system consistent with the level of secrecy that a system of foreign intelligence surveillance might well require.[132]

As the normal Court of Justice in US has a basic function of adjudicative authority, the court can sanction various measure to implement the right to personal data protection; civil damage, criminal punishment and administrative action. However, the sophisticate cases come from the special internal court, Foreign Intelligence Surveillance Court (FISC) under the provision of Foreign Intelligence Surveillance Act (FISA), which attached to the security administrative sector. The check-and-balance functions of FISC as adjudicative authority or oversight mechanism turn to be a "Rubber Stamp" for administrative authority in order to penetrate into personal data collection.

To wrap up failures from US system, in many cases the personal data has been transferred from the private data controller/processor, IT Corporation, to state authority such as NSA without well standard oversight. The incompetent of US IT Corporation to set forts, precautionary measure or data breach notification or alternative dispute resolution mechanism, for protecting customers from the mass electronic surveillance of US government may drop the level of data protection standard to the lower point. This weak guard and absent of redress mechanism are definitely less than what EU personal data protection regime expected.

3.3. Hard Case Study under EU legal system

This section will bring in the cases from the practice in the everyday-life situations and the court decisions. The cases from the real-life practice illustrate the penetration to the filling system of the IT Corporation did by State Agency. The Court Case studies, Court of Justice of European Union (CJEU), point out the legal baseline of Personal Data Protection when it faces with difficult circumstances in many situations.

[132] Shane, Peter M. "Foreword: The NSA and the Legal Regime for Foreign Intelligence Surveillance." *Journal of Law and Policy for the Information Society*, Vol.9, 2014, p. 36.

3.3.1. Tension across Atlantic due to the relationship between IT Corporation and US Authority

The research explores the cooperation among States and IT Corporation. It seems to be sure that IT Corporation has a power over personal data processing. People will never know whether they share it with government or not. IT Corporation usually share personal data and information with state agencies[133] which consistently exchange the information on political basis and IT Corporation may gain economical benefit in return as article has shown on the above section.

Ultimately, are just the internet surfers who really use IT Corporation's information? On the contrary, State especially government and security agencies do processing, mining and sharing the information with IT Corporation.[134] The orthodox excuses of the state are; to support the flourishing of economy and protect National Security[135] which is vague and undermine the fundamental rights of individual as a customer and people.

This leads to the question whether the acts of IT Corporation as US Internet spy on Global Citizen could harm the right to privacy and Personal Data Protection in diverse aspects.

The scandalous US Global Internet Surveillances on MUSCULAR program, NSA wire tapping in marine cable of famous ICT Corporations, gave evidences confirming the threats from IT Corporation on Personal Data Protection of Global Netitizen.

The NSA's acquisitions directorate sends millions of records every day from internal IT Corporation networks to data warehouses at their agency's headquarters in Maryland. The program operates via an access point known as DS-200B, which is outside the United States, and it relies on an unnamed telecommunications operator to provide secret access for the NSA and the GCHQ.[136]

---

[133] Ingram, Mick. "Google Publishes Figures on Government Requests for Data." *World Socialist Web Site, 26* www.wsws.org/en/articles/2010/04/goog-a26.html. Accessed 31 Oct. 2012.

[134] Google. *Google Transparency Report*. http://www.google.com/transparencyreport/userdatarequests/faq/. Accessed 31 Oct. 2014.

[135] Council of Europe. *Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data*. 1981, Article 9(2)(a).

[136] Gellman, Barton and DeLong, Matt. "How the NSA's Muscular program collects too much data from Yahoo and Google." *The Washington Post*. http://apps.washingtonpost.com/g/page/world/how-the-

According to the *LIBE Report on Mass Electronic Surveillance*, the MUSCULAR program collects more than twice as many data points compared to the better known PRISM. Unlike PRISM, the MUSCULAR program requires no (FISA or other type of) warrants.[137]

Because of the huge amount of data involved, MUSCULAR has presented a special challenge to NSA's Special Source Operation. The NSA's PINWARE database (their primary analytical database for the Internet) was quickly overwhelmed with the data coming from MUSCULAR.[138]

Closely related program are called INCENSER and TURMOIL. TURMOIL, belonging to the NSA, is a system for processing the data collected from MUSCULAR.[139]

According to the presentation these Program, the exploitation relied on the fact that (at the time at least) data was transmitted unencrypted inside IT Corporation's private cloud, with "Google Front End Servers" stripping and respectively adding back SSL from/to external connections. There is a strong confirm that "Two engineers with close ties to Google exploded in profanity when they saw the drawing."[140] After the information about MUSCULAR was published by the press, many IT Corporations announced that it was working on deploying encrypted communication between its datacenters. [141]

After the Revelations in 2013, IT Corporation like Google made the announcement that "Google cares deeply about the security of our users' data. We disclose user data to

---

nsas-muscular-program-collects-too-much-data-from-yahoo-and-google/543/#document/p3/a129339. Accessed 28 Feb. 2015.

[137] Bowden, Caspar. "Directorate General For Internal Policies." *The Us Surveillance Programmes and Their Impact on Eu Citizens' Fundamental Rights,* 2013, p. 18.

[138] Gallagher, Sean. "How the NSA's Muscular tapped Google's and Yahoo's private networks." *Ars Technica*, 31 Oct. 2013, http://arstechnica.com/information-technology/2013/10/how-the-nsas-muscular-tapped-googles-and-yahoos-private-networks/. Accessed 6 Mar. 2015.

[139] Gellman, Barton and Soltani, Ashkan and Peterson, Andrea. "How we know the NSA had access to internal Google and Yahoo cloud data." *The Washington Post*, 4 Nov. 2013. http://www.washingtonpost.com/blogs/the-switch/wp/2013/11/04/how-we-know-the-nsa-had-access-to-internal-google-and-yahoo-cloud-data/. Accessed 6 Mar. 2015.

[140] Ibid.

[141] Gellman, Barton and Soltani, Ashkan. "NSA infiltrates links to Yahoo, Google data centers worldwide, Snowden documents say." *The Washington Post*. 30 Oct. 2013, http://www.washingtonpost.com/world/national-security/nsa-infiltrates-links-to-yahoo-google-data-centers-worldwide-snowden-documents-say/2013/10/30/e51d661e-4166-11e3-8b74-d89d714ca4dd_story.html. Accessed 6 Mar.2015.

government in accordance with the law, and we review all such requests carefully. From time to time, people allege that we have created a government "back door" into our systems, but Google does not have a backdoor for the government to access private user data."[142] Furthermore, "Any suggestion that Google is disclosing information about our users' Internet activity on such a scale is completely false"[143] but suspicious from society remains as it has shown from revelations.

The coordinate of IT Corporations and their inter-action with State Agencies put personal data at risk. The more IT Corporation collects, processes and shares data, the more individual rights are arbitrary breached. In economical law perspective, it brings the consumer rights problems into E-market which could deter customer confident to spend on Internet. In civil and political rights perspective, it harms the democratic legitimacy sphere.

3.3.2. Legal Analysis on IT Corporation cases in the CJEU

The Court of Justice of European Union took a pro-active stand, aimed at providing EU citizens with data protection under the pre-reform legal frameworks as it did in the famous cases; Google Spain and Schrems or even in less notable case, Digital Rights Ireland, Weltimmo and Bara case. The CJEU ensured that companies could not avoid the law of the Member State where they pursue the real activities in the context of which the personal data is processed, by artificially attaching themselves to the law and enforcement regime of another, more lenient, Member State . In Digital Rights Ireland and Schremes cases, the CJEU protected the right of the individual data subject to be informed about the collection and/or transmission of his or her personal data, subject to specific exceptions laid down by law and not just an internal and unpublished governmental protocol. Notably, although these judgments concern interpretations of the Directive 95/46/EC and invalidate Data Retention Directive and Safe Harbour Agreement, even Directive 95/46/EC will remain relevant until 25 May 2018, when the GDPR will apply. While the GDPR will change the legal situation in

[142] Lardinois, Frederic. "Google, Facebook, Dropbox, Yahoo, Microsoft and Apple Deny Participation in NSA PRISM Surveillance Program." *TechCrunch*, 6 Jun. 2013. http://techcrunch.com/2013/06/06/google-facebook-apple-deny-participation-in-nsa-prism-program/. Accessed 6 Mar. 2015.

[143] Lee, Timothy B. "Here's Everything We Know About PRISM to Date." *Wonkblog*, 12 Jun. 2013. http://www.washingtonpost.com/blogs/wonkblog/wp/2013/06/12/heres-everything-we-know-about-prism-to-date/. Accessed 6 Mar. 2015.

both cases, its provisions seeks to affirm at least an equivalent protection of personal data standard as recognized by the CJEU and provided by Article 8 of the Charter of Fundamental Rights of the EU.

3.3.2.1. Right to Personal Data Protection of Individual

In the *Weltimmo case*[144], the CJEU considers the meaning of "establishment" in the sense of Art. 4 (1) a) of the Directive 95/46/EC.[145] That article prescribes that each Member State shall apply its national rules adopted pursuant to the Directive when the processing of personal data takes place in the context of the activities of the establishment of the controller on that Member State's territory. The CJEU repeats its argumentation from the Google Spain case and states that the concept of establishment, justifying the application of EU law, "implies the effective and real exercise of activity through stable arrangements".[146] The legal form of those arrangements, including the place of incorporation, does not matter,[147] nor does the extent of the real activity.[148] The CJEU finds that Weltimmo did pursue an effective and real activity in Hungary, since it runs a website in Hungarian, aimed at Hungarian properties, which charges fees after the introductory period of one month has lapsed.[149] Thus, for the purposes of the Directive, it is established in Hungary.[150] The CJEU then goes on to examine whether the processing of personal data by Weltimmo was carried out in the context of that establishment. It finds, referring to its Google Spain and Lindqvist cases[151], that there can be no doubt that Weltimmo's activity of loading personal data on its Internet page must be considered as a processing of personal data in the

[144] CJEU. *Case C-230/14 Weltimmo s.r.o. v. Nemzeti Adatvédelmi és Információszabadság Hatóság*. 2015.

[145] The CJEU also considers the factual circumstances of establishment in its preliminary observations, see CJEU. *Case C-230/14 Weltimmo s.r.o. v. Nemzeti Adatvédelmi és Információszabadság Hatóság*. 2015, paras. 15-18.

[146] Ibid, para. 28.

[147] Ibid.

[148] Ibid, para. 31.

[149] Ibid, para. 32.

[150] Ibid, para. 33.

[151] CJEU. *Case C-101/01 Criminal proceedings against Bodil Lindqvist*. 2003, para. 596.

sense of Art. 2 (d) of the Directive.[152] Therefore, Hungarian law applies to Weltimmo's processing of personal data and under Art. 4, read in conjunction with Art. 28 of the Directive, the Hungarian Data Protection Authority (HDPA) is competent to act[153], being an organ of the Hungarian State.

The extraterritorial application of EU data protection law was re-affirmed more strongly in *Google Spain v. AEPD and Mario Costeja Gonzalez*[154] from May 2014. One of the issues in this case was whether EU data protection law could apply when a company (in this case Google Inc.) has an establishment in an EU Member State that promotes a search engine that orients its activity towards the inhabitants of that State, even though the actual data processing is carried out by the establishment's parent company located outside the EU. In finding that EU data protection law did apply in such a case, the Court noted that the Directive should be interpreted to have 'a particularly broad territorial scope'.[155]

The essential components of data protection are included in the International Instruments and not left to the discretion of the Member States.[156] These precedents give a path for EU internet users to exercise their rights with Trans-Border IT Corporations even such Legal Persons are not EU nationals.[157]

The CJEU again takes a data protection friendly view in the Bara case[158], requiring the data subject to be informed beforehand in all cases where his or her personal data is being transferred, even between public authorities. Nonetheless, articles 11(2) and 13 of the Directive allow national legislators to enact rules deviating from this right to prior

[152] CJEU. *Case C-230/14 Weltimmo s.r.o. v. Nemzeti Adatvédelmi és Információszabadság Hatóság*. 2015, paras. 35-38.

[153] Gryffroy, Pieter. *Taking a look at two cases in the margin of the CJEU's "Privacy Spring", before and after the General Data Protection Regulation: Weltimmo and Bara*. 2016, p. 2.

[154] CJEU. *Case C-131/12 Google Inc. v Agencia Española de Protección de Datos, Mario Costeja González.* 13/5/2014.

[155] Ibid, para. 54.

[156] This would not be in line with the case law of the Court of Justice of European Union, particularly Joined cases C-293/12 and C-594/12, Digital Rights Ireland (C-293/12) and Seitlinger (C-594/12), ECLI:EU:C:2014:238, paras. 54-62.

[157] Rivero, Álvaro F. *Right to Be Forgotten in the European Court of Justice Google Spain Case: The Right Balance of Privacy Rights, Procedure, and Extraterritoriality*. 2017.

[158] CJEU. *Case C-201/14 Smaranda Bara and Others v Președintele Casei Naționale de Asigurări de. Sănătate and Others*. 1 Oct. 2015.

information.[159] Exception to exercise right to personal data protection must rely on historical or scientific research purposes and legitimate exemptions.

On October 6, 2015, the CJEU issued a decision that invalidated Safe Harbor (effective immediately), as currently implemented. The CJEU decision stemmed from a complaint brought to the Irish DPA by an Austrian national, Maximillian Schrems, concerning Facebook's transfer of some or all of his data from Facebook's EU-based servers in Ireland to its servers located in the United States in light of the unauthorized disclosures in June 2013 of U.S. surveillance activities.[160]

On 8 April 2014, *Digital Rights Ireland Case*, the Court of Justice of the European Union repealed the Directive 2006/24/EC on the retention of telecommunications data because of its disproportionate intrusion into the fundamental right to data protection.[161]

The judgments of the Court of Justice in *Digital Rights Ireland*[162] and, recently, in *Schrems*[163] further confirm the importance of a high level of protection especially in connection with law enforcement and national security. In *Digital Rights Ireland*, the Court warns that the instrument of data retention was "*likely to generate in the minds of the persons concerned the feeling that their private lives are the subject of constant surveillance*"[164]. In *Schrems*, the Court considers that access of public authorities on a generalized basis to the content of electronic communications affects the very essence of the right to privacy[165].

The essential components of data protection, laid down in Article 8 of the Charter of the Fundamental Rights of the Union, are respected and that exceptions fulfill the

[159] Gryffroy, Pieter. *Taking a look at two cases in the margin of the CJEU's "Privacy Spring", before and after the General Data Protection Regulation: Weltimmo and Bara*. 2016, p. 4.

[160] Weiss, Martin A and Archick, Kristin. " US-EU Data Privacy: From Safe Harbor to Privacy Shield." *Congressional Research Service*. 2016, p. 6.

[161] CJEU *C-293/12 Digital Rights Ireland*. 2014 and CJEU. *C-594/12 Seitlinger*. 2014, paras. 6–7.

[162] CJEU. *Joined cases* C-*293/12 and C-594/12, Digital Rights Ireland (C-293/12) and Seitlinger (C-594/12)*. 2014, para. 238.

[163] CJEU. *Case C-362/14 Schrems v Data Protection Commissioner*. 2015.

[164] CJEU. Joined cases *C-293/12 and C-594/12, Digital Rights Ireland (C-293/12) and Seitlinger (C-594/12)*. 2014, para. 37.

[165] CJEU. *Case C-362/14 Schrems v Data Protection Commissioner*. 2015, para. 94.

strict test of proportionality, as specified in *Digital Rights Ireland*[166]. In this Opinion, it can be pointed particularly on the principle of purpose limitation, on the right to access of individuals to their personal data and on the control by independent data protection authorities[167].

In considering the broad category of data to be retained, the CJEU observed that such data may allow very precise conclusions to be drawn concerning the private lives of the persons whose data has been retained, such as the habits of everyday life, permanent or temporary places of residence, daily or other movements, the activities carried out, the social relationships of those persons and the social environment.[168] The Court observed that under such circumstances, even though it is not permissible to retain the content of communications, it is possible that the freedom of expression of subscribers or registered users might be in jeopardy.[169]

In *Google Spain v AEPD and González*, The Court also held that the right to delete data under the EU Data Protection Directive applies to the results of Internet search engines (popularly referred to as the 'right to be forgotten').[170] The CJEU held that search engine operators are, in certain circumstances, obliged to de-list links to third-party webpages (URLs) from the list of search results when searching for the individual's name.[171] This is

[166] CJEU. Joined cases *C-293/12 and C-594/12, Digital Rights Ireland (C-293/12) and Seitlinger (C-594/12)*. 2014, para. 238.

[167] Control is an essential component of the protection of the individual: Recital (62) of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281/31, and case law of the CJEU, most recently, *Case C-362/14, Schrems*. 2015, para. 42.

[168] CJEU. *Case C–293/12 Digital Rights Ireland Ltd. v. Minister for Communications, Marine and Natural Resources*. 8 Apr. 2014, para. 27.

[169] Ibid, para. 28.

[170] CJEU. *Case C-131/12 Google Inc. v Agencia Española de Protección de Datos, Mario Costeja González.* 13 May 2014, paras. 89-99.

[171] The webpage itself is not deleted from the original publisher's source nor from the search engines indexes. A search using search terms other than an individual's name may still list the webpage at the centre of the request – see Article 29 Date Protection Working Party, *Guidelines on the implementation of the Court of Justice of the European Union on the judgment on "Google Spain and Inc v. Agencia Espanola de Proteccion de Datos (AEPD) and Mario Costeja Gonzalex" C-131/12*, adopted on 26 Nov. 2014.

commonly referred to as 'the right to be forgotten' (right to erasure). The Court found that the use by search engine operators of information published by third parties amounts to the processing of personal data for the purposes of the Data Protection Directive. It also found that searching for a person by name is likely to return information about their private life in a structured format, which allows the searcher to build a profile of the person searched for. As a result, the processing is likely to significantly affect a person's right to privacy and right to data protection. In such circumstances the search engine operator is a data controller and must ensure that its activities comply with the requirements of the Data Protection Directive.[172] The Court ruled that personal data in search results is incompatible with the Data Protection Directive where, in light of all the circumstances of the case and the amount of time that has passed, the data is inaccurate, inadequate, irrelevant, or excessive to the specified purpose for which it was originally processed.[173]

The CJEU stated that the retention of data in order to allow access by the competent national authorities constitutes processing of data and therefore affects two basic rights of the Charter of Fundamental Rights: (a) the right to private life guaranteed by article 7, and (b) the protection of personal data guaranteed by article 8.[174]

In examining the issue of interference with the rights to privacy and the protection of personal data, the CJEU made the following observations:[175]

- The obligation imposed on providers of electronic communications services or public communications networks "constitutes in itself an interference with the rights guaranteed by article 7 of the Charter,"
- Access of the national authorities to data "constitutes a further interference with that fundamental right," and
- The interferences described above also violate the right to protection of personal data.

[172] Houses of the Oireachtas Tithe an Oireachtas. *European Union Data Protection Law & Policy*. 2016, p. 10.

[173] Ibid.

[174] CJEU. Case *C–293/12 Digital Rights Ireland.* 2014, para. 28.

[175] Ibid, paras. 34-36.

Article 52(1) of the Charter requires that any limitation on the exercise of rights guaranteed by the Charter must be provided by law and must respect the essence of such rights. Any limitations are subject to a proportionality test and can be imposed only if they are necessary and meet the objectives of general interest as recognized by the EU or the need to protect the rights and freedoms of others.[176]

The Court went on to state that the retention of data affects not only persons whose data may contribute to the initiation of legal proceedings, but also those for whom there is not a shred of evidence to suggest that their conduct might be connected to a serious crime. It also observed that no one is exempted from this rule; it even applies to those whose communications are subject to professional secrecy, according to national rules.[177]

In further discussing the Directive, the CJEU observed the absence of any link between the data retained and a threat to public security. It also noted that the restriction is not limited to the data of persons related to a particular time period, or to a particular geographic zone, or to a group of persons who could possibly have a tie to a serious crime.[178]

Moreover, the CJEU reviewed whether the Directive contained any general limits on the right of national authorities to access the retained data. In this regard, the CJEU observed the lack of any general limits. Then, it proceeded to state that the Directive (a) fails to establish either substantive or procedural limits on access by competent national authorities to the data retained,[179] (b) fails to make access by national authorities conditional on a prior review carried out by a court or any other independent administrative authority whose review is essential in order to limit access to the data and their use to what it is absolutely necessary, and (c) does not require the Member States to establish such limits.[180]

---

[176] Ramos, Mario H. "Una Vuelta De Tuerca Más a Las Relaciones En Materia De Protección De Datos Entre La Ue Y Los Estados Unidos: La Invalidez De La Decisión Puerto Seguro." *Revista General de Derecho Europeo*, no. 39, 2016, p. 31.

[177] CJEU. *Case C–293/12 Digital Rights Ireland Ltd. v. Minister for Communications, Marine and Natural Resources*. 8 Apr. 2014, para. 58.

[178] Ramos, Mario H. "Una Vuelta De Tuerca Más a Las Relaciones En Materia De Protección De Datos Entre La Ue Y Los Estados Unidos: La Invalidez De La Decisión Puerto Seguro." *Revista General de Derecho Europeo*, no. 39, 2016, p.32.

[179] CJEU. *Case C–293/12 Digital Rights Ireland Ltd. v. Minister for Communications, Marine and Natural Resources*. 8 Apr. 2014, paras. 59–61.

[180] Ibid, para. 62.

The Court reasoned that, based on the above, the Directive does not establish clear and precise rules that regulate the "extent of interference with the fundamental rights of Article 7 and 8 of the Charter". Therefore, it concluded that the Directive "entails a wide-ranging and particularly serious interference with those fundamental rights in the legal order of the EU, without such an interference being precisely circumscribed by provisions to ensure that it is actually limited to what it is strictly necessary."[181]

In *Schrems Case*, the CJEU ruling found that U.S. national security, public interest, and law enforcement requirements have "primacy" over the Safe Harbor principles, and that U.S. undertakings are bound to disregard, without limitation, the protective rules laid down by that scheme where they conflict with such requirements. Consequently, the CJEU concluded that the Safe Harbor scheme "enables interference" by U.S. authorities "with the fundamental rights of the persons whose personal data is or could be transferred from the European Union to the United States."[182] Moreover, the CJEU noted that the 2000 Commission's Decision on Safe Harbor does not refer to either the existence of U.S. rules or effective U.S. legal protections intended to limit such interference, such as the possibility of judicial redress.[183]

Furthermore, in *Schrems*, the Court stated that the accessing of private communications originating within a person's home by State Authorities directly engages the Constitutional right to privacy and the right to inviolability of the dwelling under Article 40.5.[184] The interception of private communications by the State is not in itself necessarily unlawful. The Court stated that where appropriate safeguards are in place, the interception or electronic surveillance of communications may be lawful where it is indispensable for the preservation of State security.[185]

---

[181] Ibid, para. 65.

[182] Weiss, Martin A and Archick, Kristin. "US-EU Data Privacy: From Safe Harbor to Privacy Shield." *Congressional Research Service*, 2016, p. 7.

[183] Gavilán, Elisa U. "Derechos fundamentales versus vigilancia masiva. Comentario a la sentencia del Tribunal de Justicia (Gran Sala) de 6 de octubre de 2015 en el asunto C-362/14 Schrems." *Revista de Derecho Comunitario Europeo*, Vol.53, 2016, pp. 261-282.

[184] CJEU. *Case C-362/14 Schrems v Data Protection Commissioner*. 2014, para. 48.

[185] Ibid, para.49.

These are just the examples of an approach in these cases and confirmed by the highest EU Court, which emphasizes the need for strong protection of individuals, as part of the value of the European Union.[186] This oversight and accountability approach must be brought into the EU General Data Protection Regulation and Directive on Criminal and Judicial Matters. Furthermore, the bilateral agreements between EU and US must also include the respective legal obligations laid down in International Human Rights Laws and EU laws.

3.3.2.2. Obligation of the Data Controller and Data Processor

The concept of adequate level of protection has been defined by the Court of Justice in the *Schrems case*, as requiring the third country in fact to ensure, by reason of its domestic law or its international commitments, a level of protection of fundamental rights and freedoms that is essentially equivalent to that guaranteed within the European Union.[187] The Court of Justice has also stated that the Commission's discretion as to the adequacy of the level of protection ensured by a third Country should be limited, considering, first, the important role played by the protection of personal data in the light of the fundamental right to respect for private life and, secondly, the large number of persons whose fundamental rights are liable to be infringed where personal data is transferred to a third country without ensuring an adequate level of protection[188]**.** In that respect it should be underlined that data processing in the police and criminal justice context was a field left until now outside EU law; that's why practically all Member States have bilateral agreements with third countries permitting the exchange of personal data for law enforcement related purposes, notwithstanding any "adequacy" finding in respect of the recipients' data protection safeguards.

On April 8, 2014, the Grand Chamber of the Court of Justice of the European Union (CJEU) delivered a much-anticipated judgment[189] concerning the legality of Directive

[186] European Commission. *Opinion 6/2015*. 28 Oct. 2015, pp. 4-5.

[187] CJEU. *Case C-362/14 Maximillian Schrems v Data Protection Commissioner*. 2015, para. 73.

[188] CJEU. *Case C-362/14 Maximillian Schrems v Data Protection Commissioner*. 2015, *para*. 78; CJEU. *Case C-293/12 Digital Rights Ireland Ltd. v. Minister for Communications, Marine and Natural Resources*. 2014, paras. 47-48.

[189] CJEU. *Case C-293/12 Digital Rights Ireland Ltd. v. Minister for Communications, Marine and Natural Resources*. 2014.

No. 2006/24/EC, commonly referred to as the Data Retention Directive.[190] The Directive was challenged on the grounds of infringement of the right to private life, and the right to the protection of personal data of individuals, as guaranteed in articles 7 and 8, respectively, of the Charter of Fundamental Rights of the European Union.[191]

The Data Retention Directive required the providers of publicly available electronic communications services or public communications networks to retain traffic and location data belonging to individuals or legal entities. Such data included the calling telephone number and name and address of the subscriber or register user, user IDs (a unique identifier assigned to each person who signs with an electronic communications service), Internet protocol addresses, the numbers dialed, and call forwarding or call transfer records.[192] The retention period was to last for a minimum period of six months and up to two years, and the sole purpose of processing and storing the data was to prevent, investigate, detect, and prosecute serious crimes, such as organized crime and terrorism.[193] The content of the communications of individuals was not retained.[194]

The CJEU took note of the basic objective of the Data Retention Directive, which is to assist the EU Members in their fight against serious crime and to contribute to maintaining public security. It also noted that the fight against international terrorism constitutes an objective of general interest. In this regard, it acknowledged that data retention is a valuable tool for the national authorities in their pursuit of fighting serious crime.[195] Based on these observations, the CJEU reached the conclusion that retention of data in order to give an opportunity to national authorities to access such data for the

[190] Official Journal of the European Union. *Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the Retention of Data Generated or Processed in Connection with the Provision of Publicly Available Electronic Communications Services or of Public Communications Networks and Amending Directive 2002/58/EC*, 2006 O.J. (L 105) 54, 13 Apr. 2006.

[191] European Union. *Charter of the Fundamental Rights of the European Union c 326/391*. 26 Oct. 2012.

[192] For a detailed description of the traffic and location data, see article 5 of *Directive 2006/24/EC*.

[193] Ibid, Articles. 6 and 1, para. 1.

[194] Ibid, Art. 5, para. 2.

[195] Ramos, Mario H. "Una Vuelta De Tuerca Más a Las Relaciones En Materia De Protección De Datos Entre La Ue Y Los Estados Unidos: La Invalidez De La Decisión Puerto Seguro." *Revista General de Derecho Europeo*, no. 39, 2016, p. 32.

prevention and investigation of serious crimes "genuinely satisfies an objective of general interest."[196]

In this regard, the Court stated that the EU legislation in question must contain clear and precise rules pertaining to the retention of personal data and must also include certain safeguards to ensure that individuals whose data are retained have certain guarantees to protect their personal data "against the risk of abuse and against any unlawful access and use of that data."[197]

The CJEU then proceeded to examine whether the interference by national authorities was proportionate to the objective pursued. In this regard, according to the settled case law, the standards to be met are that of being "appropriate" and "necessary"[198] in order to achieve the objectives:

- As far as the question of whether the retention of data was appropriate to achieve the objectives of Directive 2006/24/EC, the CJEU, after acknowledging that the means of electronic communication play a vital role in the investigation of crimes and at the same time the need of national authorities to access data, stated that retention of data is "a valuable tool" and "may be considered to be appropriate" to achieve the Directive's objectives.[199]
- As far as the necessity test, and whether the interference is limited to what is necessary, the Court made three significant observations: (a) the Directive requires the retention of all traffic data generated from a wide range of electronic communication modes, including fixed telephony, mobile telephony, Internet access, Internet email, and Internet telephony; (b) the Directive's scope extends to all subscribers and registered users; and

[196] CJEU. *Case C–293/12 Digital Rights Ireland Ltd. v. Minister for Communications, Marine and Natural Resources*. 2014, para.44.

[197] CJEU. *Case C–293/12 Digital Rights Ireland Ltd. v. Minister for Communications, Marine and Natural Resources*. 2014, para. 54.

[198] Ramos, Mario H. "Una Vuelta De Tuerca Más a Las Relaciones En Materia De Protección De Datos Entre La Ue Y Los Estados Unidos: La Invalidez De La Decisión Puerto Seguro." *Revista General de Derecho Europeo*, no. 39, 2016, p. 34.

[199] CJEU. *Case C–293/12 Digital Rights Ireland Ltd. v. Minister for Communications, Marine and Natural Resources*. 2014, para. 49.

(c) the Directive interferes with the fundamental rights of the entire European Union population.[200]

- As far as the period of retention, which runs from six months up to two years, the CJEU noted that the Directive does not set any objective criteria to determine the appropriate period of retention "to what is strictly necessary."[201]

Regarding the security and protection of data to be retained, the CJEU held that Directive 2006/24/EC does not contain sufficient safeguards, as required by article 8 of the Charter, to ensure effective protection of the data retained against the risk of abuse and against any unlawful access and use of that data. Article 8 of the Charter requires, *inter alia*, the consent of the data subject for the processing of personal data, and processing must be done for a specific person. The Court went on to state that Directive 2006/24/EC does not contain rules.[202] which are specific and adapted to (i) the vast quantity of data whose retention is required by that directive, (ii) the sensitive nature of that data and (iii) the risk of unlawful access to that data, rules which would serve, in particular, to govern the protection and security of the data in question in a clear and strict manner in order to ensure their full integrity and confidentiality. Furthermore, a specific obligation on Member States to establish such rules has also not been laid down.[203]

In Bara case, the CJEU only refers to the provision of the Directive 95/46/EC, it is important to note that the requirement of a legislative basis for transfers of personal data flows directly from the EU Charter. First, personal data must be processed fairly, on the basis of consent of the data subject or on another ground, laid down by law (Art. 8(2), first sentence EU Charter). Second, even when personal data has initially been processed lawfully, any restriction of an EU citizen's right to data protection must be provided by law and meet the principle of proportionality (Art. 8 read together with Art. 52(1) EU Charter). Since

[200] Ibid, para. 56.

[201] Ibid, para. 64.

[202] Ramos, Mario H. "Una Vuelta De Tuerca Más a Las Relaciones En Materia De Protección De Datos Entre La Ue Y Los Estados Unidos: La Invalidez De La Decisión Puerto Seguro." *Revista General de Derecho Europeo*, no. 39, 2016, p. 30.

[203] CJEU. *Case C–293/12 Digital Rights Ireland Ltd. v. Minister for Communications, Marine and Natural Resources*. 2014, para. 66.

transferring personal data between authorities without the data subject's consent or knowledge constitutes such a restriction, the Charter requires Member State law to expressly provide for it.[204]

The judgment in *Schrems Case* confirms the strict conditions for transfer of personal data to third countries. The CJEU found Safe Harbor to be invalid. The CJEU found that according to Article 25 of the Directive 95/46/EC, the European Commission is required to examine the domestic laws or international commitments of a third country prior to making a determination on the adequacy of their data privacy protection.[205] Since the 2000 Commission Decision recognizing the Safe Harbor Agreement did not make any such finding, that Decision is now invalid.[206] However, as Safe Harbor no longer provides a legal basis for U.S.-EU data transfers anymore, other methods such as Standard Contractual Clauses or Binding Corporate Rules (BCRs) can be used instead.

3.3.2.3. Implementation of Personal Data Protection

On 6 October 2015, the CJEU issued its judgment and declared the Safe Harbor Decision invalid. In its ruling[207], the CJEU also confirmed that a national EU Data Protection Authority (DPA) is always empowered to challenge the adequacy of data transfers and only the CJEU can invalidate a Commission's decision of adequacy.[208]

In Weltimmo case, activity of loading personal data on its Internet page must be considered as a processing of personal data in the sense of Article 2 (d) of the Directive.[209] Thus, Hungarian law applies to Weltimmo's processing of personal data and

[204] Gryffroy, Pieter. *Taking a look at two cases in the margin of the CJEU's "Privacy Spring", before and after the General Data Protection Regulation: Weltimmo and Bara*. 2016, p. 5.

[205] Ramos, Mario H. "Una vuelta de tuerca más a las relaciones en materia de protección de datos entre la UE y los Estados UnidosLa invalidez de la Decisión Puerto Seguro." *Revista General de Derecho Europeo*, Vol.39, 2016, pp. 27-31.

[206] Weiss, Martin A and Archick, Kristin. " US-EU Data Privacy: From Safe Harbor to Privacy Shield." *Congressional Research Service*, 2016, p. 7.

[207] CJEU, *Case C-362/14 Schrems*. 2015.

[208] Hogan Lovells. *Legal Analysis of the EU-US Privacy Shield*. 2016, p. 13.

[209] CJEU. *Case C-230/14 Weltimmo s.r.o. v. Nemzeti Adatvédelmi és Információszabadság Hatóság*. 2015, paras. 35-38.

under Article 4, read in conjunction with Art. 28 of the Directive, then Hungarian Data Protection Authority (HDPA) is competent to act[210], as an organ of the Hungarian State.

The CJEU also addresses the question what action the HDPA could have taken had Slovakian law been applicable.[211] The CJEU holds that in any case, the HDPA may investigate any complaint it receives, before even knowing the applicable law.[212] However, when the HDPA or another national data protection authority comes to the conclusion that the law of another Member State is applicable, it cannot impose penalties or sanctions outside the territory of its own Member State because those sanctions have their legal basis in the national law of said Member State.[213] In such a case, the national data protection authority in question has, under the duty of cooperation of Art. 28(6) of the Directive, to request the supervisory authority of the Member State whose law is applicable to intervene, potentially on the basis of the information gathered by the first national data protection authority.[214]

On 9 March 2010, the CJEU ruled that 'complete independence' means that DPAs may not be subject to state oversight or scrutiny.[215] They must be 'free from any external influence'. The Court also stated that any directions or any other external influence, whether direct or indirect, which could call into question the performance by those authorities consisting of establishing a fair balance between the protection of the right to private life and the free movement of personal data must be avoided.[216] Also, the risk that other authorities could exercise a political influence over the decisions of the supervisory authorities is enough to hinder the latter authorities' independent performance of their tasks[217] and thus not consistent with the requirement of independence.

---

[210] Gryffroy, Pieter. *Taking a look at two cases in the margin of the CJEU's "Privacy Spring", before and after the General Data Protection Regulation: Weltimmo and Bara*. 2016, p. 2.

[211] CJEU. *Case C-230/14 Weltimmo s.r.o. v. Nemzeti Adatvédelmi és Információszabadság Hatóság*. 2015, paras. 54-60.

[212] Ibid, 57.

[213] Ibid, paras. 56-57, 59.

[214] Ibid, paras. 57-58.

[215] CJEU. *Case C*- 518/07 *Commission v Germany*. 2010.

[216] Ibid, para. 30.

[217] Ibid, para. 36.

The CJEU stated that the guarantee of the independence of national supervisory authorities is intended to ensure the effectiveness and reliability of the monitoring of compliance with the provisions concerning protection of individuals with regard to the processing of personal data and must be interpreted in the light of that aim. It was established in order to strengthen the protection of individuals and bodies affected by the decisions of those authorities.[218]

As every person in the scope of EU laws can pursuit for legal remedy from competence authorities including domestic courts and regional courts, which based on the jurisprudence anyone can go to court if they have a legitimate reason to suspect an interference of their fundamental rights.[219] The entitled natural person or group of person could lodge their complaint to available mechanism.

In January 2016, Digital Rights Ireland (DRI), a privacy advocacy group, commenced legal proceedings against the Irish State challenging the independence of the Commissioner.[220] In the legal papers served on the State, DRI alleged that the Commissioner did not effectively monitor databases containing personal data that had been created by public bodies and, as a result, failed to act independently.[221] Furthermore, the legal papers noted that the Commissioner is integrated with the Department of Justice and that her staffs are civil servants.[222] The CJEU has described the independence of NDPAs as being "an essential component of the protection of individuals with regard to the processing of personal data". The CJEU has also confirmed that NDPAs must be free to perform their duties free of external influence,[223] including political economy influence.

The CJEU also held that the security and protection of personal data cannot be fully guaranteed in the absence of review of compliance by an independent authority of the

[218] CJEU. *Case C-362/14 Schrems.* 2015, para. 41.

[219] ECtHR. *Case 47143/60 Roman Zakharov v. Russia. 4 Dec. 2015,* para. 171.

[220] "DRI challenges independence of Ireland's Data Protection Authority." *Digital Rights Ireland,* DRI challenges independence of Ireland's Data Protection Authority, 28 Jan. 2016.

[221] Edwards, Elaine. "Independence of Data Protection Commissioner Questioned." *The Irish Times,* 28 Jan. 2016, www.irishtimes.com/business/technology/independence-of-data-protection-commissioner-questioned-1.2513682. Accessed 10 Nov. 2016.

[222] Ibid.

[223] CJEU. *Case C-288/12 European Commission v Hungary*. 08 Apr. 2014, paras. 51-55 and 62.

rules on data protection, as required by article 8 of the Charter of Fundamental Rights,[224] as well as the decision issued in Schrems Case.[225] Foremost, the CJEU found that the existence of the Commission Decision on the Safe Harbor Agreement does not eliminate or reduce the powers available to the national DPAs. The CJEU found that national DPAs "must be able to examine, with complete independence, any claim concerning the protection of a person's rights and freedoms in regard to the processing of personal data relating to him" and assess their compliance with the DPD[226] and the EU's Charter of Fundamental Rights.

The concerns of the legality of Directive No.2006/24/EC case arose before the CJEU as preliminary questions from the High Court of Ireland and the Constitutional Court of Austria. The national courts, in adjudicating cases, have the right to refer legal inquires to the CJEU. The CJEU decides on the validity of European Union law, or the interpretation of treaties or secondary legislation, and the decision on the specific case is left to the national court.[227] Accordingly, the Exhaustion of Domestic Remedy Principle must be applied to the case before referring the case to Regional Court.

Consequently, the High Court in Ireland had to adjudicate a dispute between the Irish company Digital Rights Ireland and the Irish authorities on the legality of national measures implementing the retention of data of electronic communications.[228] Meanwhile, the Austrian Constitutional Court (CC) had before it several actions filed by a large number of applicants seeking the annulment of the Austrian telecommunications law that transposed the Data Retention Directive into national laws. Whereas, the domestic court is the primary mechanism to protect data subjects' rights, not the Regional one which is the supplementary redress.

Base on the decision of CJEU on *Digital Rights Ireland Case*, it can be concluded that the EU legislative bodies, by adopting Directive 2006/24/EC, exceeded the

[224] CJEU. *Case C–293/12 Digital Rights Ireland*. 2014, para. 66.

[225] CJEU. *The Court of Justice Declares that the Commission's US Safe Harbour Decision Is Invalid*. 6 Oct. 2015.

[225] Weiss, Martin A and Archick, Kristin. "US-EU Data Privacy: From Safe Harbor to Privacy Shield." *Congressional Research Service*, 2016, p. 6.

[227] "Summaries of EU Legislation: The Reference for a Preliminary Ruling." *Europa*, http://europa.eu/legislation_ summaries/institutional_affairs/decisionmaking_process/l14552_en.htm. Accessed 20 Feb. 2013.

[228] CJEU. *Case C–293/12 Digital Rights Ireland*. 2014, paras. 17–18.

limits imposed by the principle of proportionality in light of articles 7, 8, and 52(1) of the Charter. Consequently, it held the Directive invalid.[229] The Data Retention Directive becomes invalid *ab initio* (invalidated since the first day it was entry into force), that is from the time it became effective in 2006, since the CJEU did not specify otherwise.[230] The EU Members that have transposed the Directive into their national legal systems are required to revise their legislation or take further steps to ensure compliance with the judgment.

In exercising its right to initiative, the European Commission will have to adhere to the CJEU's judgment when it introduces new legislation on data protection and privacy. Any pending legislation must also be in conformity with the CJEU's case law affecting personal data. In particular, the proposal for the Directive on the Protection of Individuals with Regard to the Processing of Personal Data by Competent Authorities for purposes of addressing criminal offenses must be in conformity with the CJEU's ruling.[231]

Put a highlight on the Sanctions and Enforceability of right to personal data protection, the Right to be Forgotten/Erasure is a good case to use as example. From the decision of CJEU on Google Spain Case, the obligation of Google Inc. to de-list the links, lead to the out-of-date information of data subject, must be balanced against other fundamental rights and freedoms and the interest of the public in having access to the information, such as the role the individual plays in public life. The assessment and the decision to de-list are made by the relevant search engine operator on a "case-by-case basis".[232] The decision does not constitute a universal precedent to delist any links or contents from the Internet promptly. On the contrary, it need a specific court order to delete specific link which is out-of-date or not meet the old purpose data subject given consent for processed or published. Therefore, the decision of one case does not represent the interpretation or precedent of further relevant cases in the future, in term of sanctions and remedies.

---

[229] CJEU. *Case C–293/12 Digital Rights Ireland*. 2014, para. 73.

[230] Ramos, Mario H. "Una vuelta de tuerca más a las relaciones en materia de protección de datos entre la UE y los Estados UnidosLa invalidez de la Decisión Puerto Seguro." *Revista General de Derecho Europeo*, Vol.39, 2016, p. 32.

[231] Europa. *Proposal for a Directive of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data by Competent Authorities for the Purposes of Prevention, Investigation, Detection or Prosecution of Criminal Offences or the Execution of Criminal Penalties, and the Free Movement of Such Data, COM/2012/010final*. 25 Jan 2012.

[232] Houses of the Oireachtas Tithe an Oireachtas. *European Union Data Protection Law & Policy*. 27 Oct. 2016, p. 10.

In the Weltimmo Case, the CJEU clearly honours the territoriality principle that underpins the system of the Directive. Following this approach, national laws provide for the precise extent of the powers of the national data protection authorities, and the jurisdictional reach is territorially limited not only because of the national nature of the laws in question, but also because of the conflicting jurisdiction of the neighboring Members States, having their own national laws on the subject and their own supervisory data protection authorities, all based on the Directive. [233] The decision also prevents companies from escaping the harsher enforcement of one EU Member State by creating an alternate corporate reality linking them to another. In doing so, the CJEU aims to protect the right to privacy and data protection of the EU citizens dealing with such corporate actors. The companies have an interest at all in attaching themselves to the law and supervisory authority of a different Member State is because at the present time not all national data protection authorities are equally active and a certain disparity in the rules transposing the Directive into national law cannot be avoided. [234]

Not only the domestic mechanism to protect their nationals within their own territory but also the extraterritorial protection. Thus, National DPA should be able to monitor the Trans-border activities done by alien Legal Person. In Schrems Case, the CJEU considered whether the Irish DPA could conduct an investigation into Facebook's data protection practices to assess their adequacy or whether the Irish DPA had to defer to the European Commission's earlier approval of the Safe Harbor framework. [235]

To propose new Instruments such of the EU Directive on Criminal Matters or EU-US Umbrella Agreement on Criminal Cooperation, it should be reconsidered with due respect to the Schrems case judgment. This means any adequacy decision must be based on a full assessment of the law enforcement sector.[236] The adequacy decision principle must not deprive the supervisory authority of the power to investigate on a specific transfer and to take enforcement action in case the transfer does not meet the standard required.

---

[233] Gryffroy, Pieter. *Taking a look at two cases in the margin of the CJEU's "Privacy Spring", before and after the General Data Protection Regulation: Weltimmo and Bara*. 2016, p. 3.

[234] Ibid, p. 4.

[235] Weiss, Martin A and Archick, Kristin. "US-EU Data Privacy: From Safe Harbor to Privacy Shield." *Congressional Research Service*, 2016, p. 6.

[236] European Commission. *Opinion 6/2015*. 2015, p. 8.

The new regime on EU and EU-US personal data protection should reflect that right to personal data protection of data subject is a crucial core value for individual internet users and for cyber society.

3.4. Preliminary remarks from the Court decisions on Personal Data Protection

This last section of the Chapter will highlight the parameter precedents that the Courts set in cases concerning personal data protection in EU and US regimes which are directly affect to the standard of data subjects' protection.

First of all, the decisions of the US Courts, predominant country in Cyberspace and the Head Quarter State of most powerful IT Corporation, will be reviewed. Some US court cases have shown the shortfalls of US legal system, on protecting data subjects around the world, especially the ones without US nationality.

Rights of Data Subject

The US Court celebrated the full constitutional rights enjoyment of US Nationals data subject but the protection for Non-US citizen stills remain a question.[237] The production of records (data retentions) or "tangible things" must be "relevant to an authorized investigation." [238] Bulk telephone metadata program is not authorized by Section 215 of Patriot Act and not legitimate by Fourth and First Amendment. However, there are no opportunities for individuals to obtain access, rectification or erasure of data, or administrative or judicial redress which are data subjects' rights.

Obligation of Duty Bearer

In US National Security Agency's decision to issue *Glomar Responses* (A Glomar response is the Agency's act of neither confirming nor denying the existence of Agency

[237] Kerr, Orin S. "The Fourth Amendment and the Global Internet." *GWU Law School Public Law Research Paper,* No. 2014-30. 2014.

[238] US Court of Appeals Second Circuit. *Opinion ACLU v. Clapper*. 7 May 2015.

records responsive to the Request[239]) Case, the court opens the door for businesses to begin communicating with NSA without fear that their problems will be exposed as a result of a Freedom of Information Act (FOIA) request.[240] This has huge benefits to businesses, which can use NSA resources without fear of private communications with government agencies becoming exposed.[241] This broad scope granted to Section 6 of the NSA Act allows government officials to consider information to be classified even when the public already knows about the information.[242]

Legal Implementation

The intent of the US FISA and PATRIOT laws to acquire "foreign intelligence information" concerning people who are not American nationals or legal residents while they are not protected by US laws; Constitution, Privacy Act and FOIA. For Non-US citizen data subjects, If EU citizen want to know whether their sensitive personal data is compromised they have no channel to request for acknowledgement or lodge the complaints Since the Close system of US National Security Laws and only US Nationals entitle to appeal so it impossible for Non-US citizen, EU citizen,[243] to gain the redress in such remedy mechanism.

There is no judicial oversight of the collection of foreign intelligence outside the US under Executive Order 12333, which are conducted under the sole competence of the Executive Branch. Foreign Intelligence Surveillance Court (FISC) under the provision of Foreign Intelligence Surveillance Act (FISA), which attached to the security administrative sector. [244] The check-and-balance functions of FISC as adjudicative authority or oversight

[239] Electronic Privacy Information Center. *NSA's March 10, 2010 letter acknowledging of receipt of EPIC's FOIA request and invoking the Glomar Response*. 10 Mar. 2010

[240] Nakashima, Ellen. "Banks Seek NSA Help Amid Attacks on Their Computer Systems." *Washington Post*, vol. 11, 2013, p. A03.

[241] United States Court of Appeals for the Columbia Circuit. Case 642 F.3d 1161 Roth v. Dep't of Justice. 2011.

[242] US Court of Appeals Second Circuit. *Opinion ACLU v. Clapper*. 7 May 2015, paras. 547, 561.

[243] Fahey, Elaine and Curtin. Deirdre. *A Transatlantic Community of Law: Legal Perspectives on the Relationship between the EU and US Legal Orders.* Cambridge University Press, UK, 2014.

[244] Council of the European Union. *Report on the findings by the EU Co-chairs of the ad hoc EU-US Working Group on Data Protection*. 2013, p. 27.

mechanism turn to be a "Rubber Stamp" for administrative authority in order to penetrate into personal data collection.

On the contrary, the CJEU have given many progressive realizations for taking in to legal reformation account, within EU and US Single E-Market regimes, as will be crystallized below.

Rights of Data Subject

In *Wltimmo Case* the application of EU law, "implies the effective and real exercise of activity through stable arrangements", the legal form of those arrangements, including the place of incorporation, does not matter, nor does the extent of the real activity.[245] Furthermore, the extraterritorial application of EU data protection law was re-affirmed more strongly to have 'a particularly broad territorial scope'[246] in *Google Spain Case*. These precedents give a path for EU internet users to exercise their rights with Trans-Border IT Corporations even such Legal Persons are not EU nationals.

The CJEU also held the right to delete data under the EU Data Protection Directive applies to the results of Internet search engines[247] ('right to be forgotten' or 'right to erasure') which give a light to apply the data protection law to forthcoming innovative information technology.

In the Bara case, The CJEU takes a data protection friendly view requiring the data subject to be informed beforehand in all cases where his or her personal data is being transferred, even between public authorities.[248] Nonetheless, the Directive 95/46/EC allows national legislators to enact rules deviating from this right to prior information but Exception

[245] CJEU. *Case C-230/14 Weltimmo s.r.o. v. Nemzeti Adatvédelmi és Információszabadság Hatóság*. 2015, paras. 28-31.

[246] Rivero, Álvaro F. "Right to Be Forgotten in the European Court of Justice Google Spain Case: The Right Balance of Privacy Rights, Procedure, and Extraterritoriality." *European Union Working Papers*, no.19, Stanford-Vienna Transatlantic Technology Law Forum, 2017.

[247] CJEU. *Case C-131/12 Google Inc. v Agencia Española de Protección de Datos, Mario Costeja González.* 2014, paras. 89-99.

[248] CJEU. *Case C-230/14 Weltimmo s.r.o. v. Nemzeti Adatvédelmi és Információszabadság Hatóság*. 2015, 1 Oct. 2015.

to exercise right to personal data protection must rely on historical or scientific research purposes and legitimate exemptions[249] only.

Obligation of Duty Bearer

In *Digital Rights Ireland Case*, CJEU emphasize on the principle of purpose limitation,[250] on the right to access of individuals to their personal data and on the control by independent data protection authorities.[251] However, data retention needs a shred of evidence to suggest that their conduct might be connected to a serious crime and no one is exempted from this rule; it even applies to those whose communications are subject to professional secrecy, according to national rules.[252] The retention of personal data must include certain safeguards to ensure that individuals whose data are retained have certain guarantees "against the risk of abuse and against any unlawful access and use of that data."[253]Aftermath, the Data Retention Directive was invalidated by CJEU since it did not meet the EU principle of proportionate[254] and necessary[255] exemptions.

The concept of adequate level of protection has been defined by the CJEU in the *Schrems case*, [256] as requiring the third country in fact to ensure, by reason of its domestic law or its international commitments, a level of protection of fundamental rights and freedoms

[249] Gryffroy, Pieter. *Taking a look at two cases in the margin of the CJEU's "Privacy Spring", before and after the General Data Protection Regulation: Weltimmo and Bara*. 2016, p. 4.

[250] CJEU. *Joined cases Digital Rights* Ireland (C-293/12) and Seitlinger (C-594/12). ECLI:EU:C:2014:238.

[251] Control is an essential component of the protection of the individual: Recital (62) of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281/31, and case law of the Court of Justice, most recently, *Case C-362/14, Schrems, EU:C:2015:650*, p. 42.

[252] Ramos, Mario H. "Una vuelta de tuerca más a las relaciones en materia de protección de datos entre la UE y los Estados UnidosLa invalidez de la Decisión Puerto Seguro." *Revista General de Derecho Europeo*, Vol.39, 2016, p. 32.

[252] CJEU. *Case C–293/12Digital Rights Ireland.* 2014, para. 54.

[254] Ibid, para. 49.

[255] Ibid, para. 56.

[256] Weiss, Martin A and Archick, Kristin. "US-EU Data Privacy: From Safe Harbor to Privacy Shield." *Congressional Research Service*. 2016, p. 7.

that is essentially equivalent to that guaranteed within the European Union.[257] The CJEU ruling found that U.S. national security, public interest, and law enforcement requirements have "primacy" over the Safe Harbor principles, and that U.S. undertakings are bound to disregard, without limitation, the protective rules laid down by that scheme where they conflict with such requirements.[258] Consequently, the CJEU concluded that the Safe Harbor scheme "enables interference" by U.S. authorities "with the fundamental rights of the persons whose personal data is or could be transferred from the EU to the US."[259] Then the CJEU invalidated Safe Harbor since October 2015.

Legal Implementation

In *Digital Rights Ireland Case*, the access to data subject's personal data must be controlled by independent data protection authorities.[260] As well as *Schrems Case*, the CJEU observed that Safe harbor and US legislation do not providing for any possibility for an individual to pursue legal remedies in order to have access to personal data relating to him, or to obtain the rectification or erasure of such data compromises the essence of this fundamental right, which is an important component of the rule of law.[261] The CJEU stated that the guarantee of the independence of national supervisory authorities is intended to ensure the effectiveness and reliability of the monitoring of compliance.[262] Thus, the Safe Harbor Decision did not contain sufficient remedy measure for individual in case of violation by IT Corporation or State National Authority.

[257] CJEU. *Case C-362/14 Maximillian Schrems v Data Protection Commissioner*. 2015, para. 73.

[258] Gavilán, Elisa U. "Derechos fundamentales versus vigilancia masiva. Comentario a la sentencia del Tribunal de Justicia (Gran Sala) de 6 de octubre de 2015 en el asunto C-362/14 Schrems." *Revista de Derecho Comunitario Europeo*, Vol.53, 2016, pp.261-282.

[259] Ramos, Mario H. "Una Vuelta De Tuerca Más a Las Relaciones En Materia De Protección De Datos Entre La Ue Y Los Estados Unidos: La Invalidez De La Decisión Puerto Seguro." *Revista General de Derecho Europeo*, no. 39, 2016, pp. 27-31.

[260] CJEU. *Joined cases Digital Rights Ireland (C-293/12) and Seitlinger (C-594/12)*, ECLI:EU:C:2014:238.

[261] CJEU. *Case C-362/14 Maximillian Schrems v Data Protection Commissioner*. 2015, para 95.

[262] Ibid, para. 41.

These prerequisite precedents give a set of remarks for drafting EU and EU-US data protection instruments which will trigger the change in relationship of EU and the counterpart state US. These regulation and directive make impact both on domestic legal system of the US and the bi-lateral agreement between EU-US relevant to Personal Data Protection. The reforms which had taken place in EU then US and in between EU-US during 2013-2016 will be scrutinized in the next chapter.

Chapter 4 Reform of the EU and EU-US regime on Personal Data Protection in Cyberspace

There have been initiatives from US and EU to address the problem of personal data protection in digital age. The US and EU appointed committee to create changes for better solution to handle the problems. US Government had launched a set of laws to reform their surveillance activity and provide Non-US citizen stronger protection of their personal data. Accordingly, EU approves General Data Protection Regulation (GDPR) and Directive on judicial and criminal matters then brought US to sign agreement to implement those standards which are EU-US Privacy Shield for general data protection and EU-US Umbrella Agreement on judicial and criminal matters. These instruments show improvements on personal data protection in digital age is possible. As a sign of better consumer protection in their E-Market, those instruments boost a stronger Trans-Atlantic relation because of the trust restoration among EU-US. The Chapter will start with the reforms launched by the US to meet the requirements that EUCJ has set and to reach the adequacy criterions of EU's new regime. The changes in EU regime will be reviewed as there are some value-added and prominent provisions that created to handle the problems in Digital Age. However, the shortcomings of both EU and EU-US regime will be reflected too. Theses EU-USA reforms give important clues for the conditions under which a 'universal approach or regime' must be developed, which will be set forth in chapter 5.

4.1. Reform of the US legal framework on Personal Data Protection: US president Review of signal intelligence 2014, Freedom Act 2015 and Redress Act 2016

For embracing the precedents given by US Courts' verdicts and CJEU's decisions, US Government had launched a set of regulation reforms; Presidential Policy Directive 28, the revised Freedom Act and the improved Judicial Redress Act, from 2014 to 2016 respectively.

Presidential Policy Directive 28

In March 2014, the US government adopted six privacy principles to govern surveillance.[1] Secretary of State John Kerry announced the forthcoming US Framework at the Freedom Online Coalition conference.[2] President Obama issued Presidential Policy Directive[3] 28 (PPD-28),[4] which imposes important limitations for intelligence operations. It specifies that data collection by the intelligence services should be targeted. Additionally, the PPD-28 limits the use of bulk collection of data to six national security purposes (detect and counter threats from espionage, terrorism, weapons of mass destruction, threats to the Armed Forces or transnational criminal threats)[5] to better protect personal data of all persons including non-U.S citizens worldwide.

The Obama administration's principles provide a framework for US compliance with its own stated objectives (the US Framework).[6] The US Framework largely mirrors several of the International Principles on the Application of Human Rights to Communications Surveillance (Principles), an evaluative framework for assessing how human rights obligations and norms apply when conducting surveillance.[7] Below, there are comparisons of "US surveillance practices" to its own stated "Framework and the Principles".

---

[1] Busby, Scott. "State Department on Internet Freedom at RightsCon." 4 Mar. 2014, http://www.humanrights.gov/2014/03/04/ state-department-on-internet-freedom-at-rightscon/. Accessed 14 Nov. 2015.

[2] Kerry, John. "Remarks to the Freedom Online Coalition Conference." *US Secretary of State*, 28 Apr. 2014, www.state.gov/secretary/remarks/2014/04/225290.htm. Accessed 14 Nov. 2015.

[3] Look at the meaning and implication of Presidential Directive from Congressional Research Service. *Presidential Service: Background and Service*. 2008.:

> "Presidential Directive is a form of an executive order issued by the President of the United States with the advice and analysis of the National Security Council. The directives articulate the executive's national security policy and carry the "full force and effect of law"."

[4] Presidential Policy Directive 28 (PPD-28) contains of US Framework on Communication Surveillance which has 6 Privacy Principles to oblige their Intelligence Agencies.

[5] European Commission. *EU-U.S. Privacy Shield: Frequently Asked Questions.* Press Release Database, Brussels, 29 Feb. 2016.

[6] Busby, Scott. "State Department on Internet Freedom at RightsCon." 4 Mar. 2014, http://www.humanrights.gov/2014/03/04/ state-department-on-internet-freedom-at-rightscon/. Accessed 14 Nov. 2015; Kerry, John. "Remarks to the Freedom Online Coalition Conference." *US Secretary of State*, 28 Apr. 2014, www.state.gov/secretary/remarks/2014/04/225290.htm. Accessed 14 Nov. 2015.

[7] International Coalition of Communication. *International Principles on the Application of Human Rights to Communications Surveillance.* 10 Jul. 2013.

The US Framework expands upon President Obama's Presidential Policy Directive 28 (PPD-28) which establishes principles to guide surveillance. The six principles endorsed by the US are (1) rule of law, (2) legitimate purpose, (3) non-arbitrariness, (4) competent external authority, (5) meaningful oversight, and (6) increased transparency and democratic accountability.[8] However, there are overlaps between the US Framework and the Principles that US policy fails to comply with the US Framework:

1) **Rule of law** – In his speech setting out the US Framework, Assistant Secretary Busby discussed how surveillance operates "pursuant to statutes and executive orders that were adopted as part of our democratic process." This principle further requires that laws, and their subsequent policies, provide clarity for individuals within the jurisdiction. US surveillance policy has proven to be anything but clear and accessible to the public. Instead, surveillance practices often depend on loose legal interpretations written in secret, approved by secret courts, and overseen by secret Congressional committees. By contrast, the Principles require that the law contains a "standard of clarity and precision" [9] to provide users notice of the application of surveillance.
2) **Legitimate purpose** – The US Framework would permit surveillance only on the "basis of articulable and legitimate foreign intelligence and counter-intelligence purposes." This does not match the standard of the legitimate aim principle, which requires surveillance to be conducted only in the furtherance of a "predominantly important legal interest that is necessary in a democratic society." Further, PPD-28 permits bulk collection only for "detecting and countering" certain enumerated threats, and expressly prohibits the use of bulk collection for suppression of dissent, discrimination, or promoting US commercial interests. However, no similar restriction is placed on other non-bulk, yet highly intrusive forms of surveillance authorized under Section 702. [10] The government should specify – and

[8] Office of the Press Secretary. *Presidential Policy Directive/PPD-28.* The White House Office of the Press Secretary, 17 Jan. 2014.

[9] Stepanovich, Amie. Mitnick, Drew and Robinson, Kayla. "United States: the necessary and proportionate principle and US Government." *Global Information Society Watch 2014: Communication Surveillance in Digital Age*, 2014, p. 263.

[10] Ibid.

identify meaningful limits to – the purposes for which it acquires and collects foreign intelligence.

3) **Non-arbitrariness** – Non-arbitrariness, as articulated by the US Framework, requires surveillance to be tailored and intrusiveness minimized. [11] This element matches up to the proportionality, necessity and adequacy principles.
4) **Competent authority** – While the US Framework seeks guidance from a "competent external authority", the Principles specify that the authority be judicial. In contrast to the Principles, the Framework expressly retains an exception for some operational decisions to be made within intelligence agencies. FISC, the judicial authority that reviews surveillance programmes and applications, has been repeatedly misled by US intelligence agencies in their applications, which makes its rulings inherently unreliable.[12]
5) **Oversight** – The US Framework calls for meaningful oversight. To underscore US adherence to this element, Assistant Secretary Busby highlighted extant internal oversight mechanisms. However, despite claims that the NSA's activities have been approved by all three branches of government, the NSA has reportedly lied to or misled all three branches.[13]
6) **Increased transparency and democratic accountability** – The final element of the US Framework is transparency. Assistant Secretary Busby pointed to recent efforts to declassify FISC opinions and the government's intention to release the statistics on the issuance of national security orders and requests.[14]

[11] Ibid.

[12] Cushing, Tim. "Declassified FISA Court opinion shows NSA lied repeatedly to the Court as well." *Techdirt,* 21 Aug. 2013, www.techdirt.com/articles/20130821/16331524274/declassifiedfisa-court-opinion-shows-nsa-lied-repeatedly-to-court-as-well.shtml. Accessed 14 Nov. 2015.

[13] Ackerman, Spencer. "NSA Illegally Collected Thousands of Emails before FISA Court Halted Program." *The Guardian,* vol. 21, August 2013.

[14] Stepanovich, Amie and Mitnick, Drew and Robinson, Kayla. "United States: the necessary and proportionate principle and US Government." *Global Information Society Watch 2014: Communication Surveillance in Digital Age*, 2014, pp. 264-5.

Freedom Act

Another improvement is the review of USA Freedom Act, in June 2015, which would have achieved a number of significant human rights reforms, including preventing bulk collection by requiring a nexus to an investigation, bringing clarity to Section 215, increasing FISC oversight and introducing a special advocate, increasing the ability of companies to disclose government national security data requests, and increasing the power of internal oversight bodies, as well as adding external checks.[15] However, the White House retarded some of the reforms.

Congress' failure to enact reforms is a great disappointment. The US must change its laws if it is to bring its surveillance programmes closer in alignment with the Principles and other international human rights standards.[16] While the president's policy statement is an admirable standpoint to surveillance reform, the greater legal restrictions and increased external oversight of these programmes can assure the protection of personal data, and reaffirm the internet users that the US Government conducts its surveillance activities with more concern on Human Rights of people in World Wide Web.

The Congress passed the USA Freedom Act, which, among other things:[17]

1) prohibits bulk collection of intelligence information under Section 215 of the PATRIOT Act and other authorities;
2) increases transparency reporting by both companies and the U.S. government, by permitting companies to publish statistics on the national security requests they receive and requiring robust reporting by the U.S. government;
3) codifies the Administration's practice of systematically declassifying FISC decisions;
4) provides for "expert[s] in privacy and civil liberties" to advise the FISC.

The USA Freedom Act has created an Amicus Curiae advisory panel to the FISA Court to give (optional) advice in case of significant new legal interpretation. Their task is however to

[15] Ibid, p. 265.

[16] Ibid, p. 266.

[17] ITI. *The U.S. Privacy and Data Protection Framework: Basic Characteristics and Recent Reforms*. 18 Jan. 2016, p. 2.

provide unbiased advice, and not to defend the interest of a specific individual upon his/her request.[18]

Judicial Redress Act

The most important improvement might be the Judicial Redress Act, which has been signed by President Obama since 24th February 2016. It extends to EU citizens the same rights that U.S. citizens enjoy under the Privacy Act of 1974 with respect to the data protection obligations of U.S. government agencies. However, the limited application of the Judicial Redress Act (both in terms of substance as it excludes national security but also in relation to the persons who can rely upon the law), the many exemptions and the legal uncertainty regarding the agencies to which the Judicial Redress Act will apply, do not satisfy the requirement to offer an effective redress mechanism to all individuals concerned in national security intelligence surveillance cases.[19]

The Judicial Redress Act will give EU citizens access to U.S. courts to enforce privacy rights in relation to personal data transferred to the U.S. for law enforcement purposes. The Judicial Redress Act will extend the rights US citizens and residents enjoy under the 1974 Privacy Act also to EU citizens. This is a long-standing demand of the EU as President Juncker stated in his political guidelines: "*The United States must [...] guarantee that all EU citizens have the right to enforce data protection rights in U.S. courts, whether or not they reside on U.S. soil. Removing such discrimination will be essential for restoring trust in transatlantic relations*"[20]. So EU citizens will have the right to seek judicial redress before US courts in case of the US authorities deny access or rectification, or unlawfully disclose their personal data.

However, there remains debate whether the U.S. redress legislation will be sufficient to satisfy European critics. For example, the current legislation does not provide citizens of EU countries with redress that is exactly on par with that which U.S. persons enjoy under the Privacy Act. One area of particular concern is that the legislation currently being discussed does not extend privacy protections to records pertaining to non-U.S. persons collected by all

[18] European Data protection Supervisor. *Opinion 1/2016.* 12 Feb. 2016, p. 44.

[19] European Data protection Supervisor. *Opinion 1/2016.* 12 Feb. 2016, p. 43.

[20] European Commission. *EU-U.S. Privacy Shield: Frequently Asked Questions*. Press Release Database, Brussels, 29 Feb. 2016.

U.S. agencies. Personal information collected by non-law enforcement agencies (such as the Department of Health and Human Services, for example) would not be covered. [21]

The United States has also implemented several reforms to provide additional protections and safeguards with respect to U.S. surveillance activities., since 2013, the Review Group on Intelligence and Communications Technology ("Review Group")[22] and the Privacy and Civil Liberties Oversight Board ("PCLOB")[23] have provided independent, expert recommendations on how the United States can reform its approaches to surveillance to respect privacy and civil liberties while advancing national security.[24]

4.2. Reform of the EU law on Personal Data Protection: general trends

Not only because of the cases analyzed in Chapter 3 but also for many other reasons, EU data protection law was based on Directive 95/46/EC needed a reform. From 1995 to present there have been significant advances in information technology, and fundamental changes to the ways in which individuals and organizations communicate and share information. In addition, the various EU Member States have taken divergent approaches to implement the Directive, creating compliance difficulties for many businesses.

Since early 2012 the EU data protection legal framework was totally being revised in order to establish a comprehensive, consistent, modern and solid system for all data processing activities in the Union; whereas in January 2012 the Commission presented a package of legislative proposals: a General Data Protection Regulation (GDPR)[25], which will replace Directive 95/46/EC and establish a uniform law throughout the EU, and a Directive[26], which will lay down a harmonized framework for all data processing activities by law enforcement authorities for law enforcement purposes and will reduce the current divergences among national laws.

---

[21] Weiss, Martin A and Archick, Kristin. "Us-Eu Data Privacy: From Safe Harbor to Privacy Shield." *Congressional Research Service*, 2016, p. 15.

[22] Look at the reports on their website at https://www.dni.gov/index.php/intelligence-community/review-group

[23] Look at the reports on their website at https://www.pclob.gov/

[24] ITI. *The U.S. Privacy and Data Protection Framework: Basic Characteristics and Recent Reforms*. 18 Jan. 2016, p. 2.

[25] European Commission. *COM(2012)0011*. 25 Jan. 2012.

[26] Ibid.

Also a series of internal developments made a general review necessary: the ratification of the Lisbon Treaty, which acknowledged a "right to data protection"[27] separate from the "right to privacy"; the aging provisions of the 1995 Data Protection Directive;[28] the release of sector-specific instruments such as the E-Privacy Directive.[29] On 21 October 2013 the European Parliament's Committee on Civil Liberties, Justice and Home Affairs (LIBE Committee) adopted its legislative reports on the two proposals and a decision on the opening of negotiations with the Council with a view to having the legal instruments adopted during this legislative term. Although the European Council of 24/25 October 2013 called for the timely adoption of a strong EU General Data Protection framework[30] in order to foster the trust of citizens and businesses in the digital economy.[31] After four years of deliberations, on 27 April 2016, the Council has been able to arrive at a general approach on the General Data Protection Regulation (GDPR) replace Directive 95/46/EC.

The EU's legislative bodies have reached a political agreement on an updated and more harmonized data protection law (the "Regulation"). The GDPR will significantly change EU data protection law, strengthening individual's rights, expanding the territorial scope, increasing compliance obligations and improving regulator enforcement powers.[32] The formal adoption is in April 27th 2016, with the Regulation applying from May 25th 2018. Organizations will have two years to implement changes to their data protection compliance programmes, business processes, and IT infrastructure to reflect the Regulation's new requirements.

In addition, already-existing data protection instruments that protect security-related processing, such as the 2008 Framework Decision 2008/977/JHA(Police and Criminal Justice

[27] EU. *Treaty on the Functioning of the European Union*. 1957, Article 16.1, referred in O.J. C. 83, 30/3/2010.

[28] As opened by the European Commission's Communication, A comprehensive approach on personal data protection in the European Union. *COM(2010) 609 final*. Brussels, 4 Nov. 2010.

[29] Papakonstantinou, Vagelis and de Hert, Paul. "The Amended Eu Law on Eprivacy and Electronic Communications after Its 2011 Implementation; New Rules on Data Protection, Spam, Data Breaches and Protection of Intellectual Property Rights." *J. Marshall J. Computer & Info. L.*, vol. 29, 2011, pp. 29-74.

[30] Look at http://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/en/ec/139197.pdf

[31] LIBE Committee Inquiry. *Electronic Mass Surveillance of EU citizens*. 2014, p. 23.

[32] Hustinx, Peter. "Recent developments in the European Union." *30 years after: the impact of the OECD Privacy Guidelines*, Joint ICCP-WPISP Roundtable, Paris, 10 Mar. 2010.

Authorities Directive),[33] be properly substituted by the new Directive on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data (Directive 2016/680) on April 27th 2016 the same day as GDPR.

After three years of trilogies negotiations between the European Parliament, the Commission and the Council, an agreement was reached in December 2015 on the final text of the Police and Criminal Justice Authorities Directive in relation to data protection in the police and justice sectors.

Member States have a two-year period in which to implement the Police and Criminal Justice Authorities Directive into their national law; Member States must adopt any relevant legislative acts for compliance with the Directive by 6 May 2018.

Here is the time-table of the process for GDPR launching which was first released on 25 January 2012 and the EU Council aimed for formal adoption in spring 2016. The schedule is:[34]

- 21 October 2013: European Parliament Committee on Civil Liberties, Justice and Home Affairs (LIBE) had its orientation vote.
- 15 December 2015: Negotiations between European Parliament, Council and Commission (Trilogue) have resulted in a joint proposal.
- 17 December 2015: European Parliament's LIBE committee voted positively on the outcome of the negotiations between the three parties.
- 8 April 2016: Adoption by the Council of the European Union.
- 14 April 2016: Adoption by the European Parliament.
- The regulation will enter into force 20 days after its publication in the EU Official Journal. Its provisions will be directly applicable in all member states two years after this date.

[33] EU. *Council Framework Decision 2008/977/JHA on the Protection of Personal Data Processed in the Framework of Police and Judicial Cooperation in Criminal Matters*. 2008.

[34] "Timeline of the new EU Data Protection Regulation – latest developments and implementation." Allen&Overy, www.allenovery.com/publications/en-gb/data-protection/Pages/Timetable.aspx. Accessed 21 Jan. 2017.

- The GDPR will replace the Directive 95/46/EC and will be directly applicable in all Member States without the need for implementing national legislation on 25th May 2018.

On the other hand, The Directive 2016/680 on Criminal and Judicial Matters will replace the effect of Council Framework Decision 2008/977/JHA. The Directive entered into force on 5 May 2016 but Member States have until 6 May 2018 to adopt and publish the laws, regulations and administrative provisions to comply with the Directive requirements.

The set of EU data protection instruments will trigger the change in relationship of EU and the counterpart state US. These regulation and directive make impact both on domestic legal system of the US and the bi-lateral agreement between EU-US relevant to Personal Data Protection.

Indeed, EU data protection model is heavily reconstructed through GDPR and Directive on Criminal Matters. Consequently, also EU-US data protection legal frameworks needed to be reviewed in order to establish a comprehensive, consistent, modern and robust system for all data processing activities in the Union and across Atlantic. The set of EU-US reforms have been done through: Exchange of personal data between the EU and the U.S. for commercial purposes are addressed by the Safe Harbor Decision which provides a legal basis for transfers of personal data from the EU to companies in the U.S. which adhere to the Safe Harbor Principles. In July 12th 2016 EU-US have agreed to sign a new Personal Data Protection bilateral agreement, Privacy Shield, which replace the old Safe Harbor Agreement.

In addition, the EU and the US were also negotiating a framework agreement on data protection in the field of police and judicial cooperation area, "Umbrella Agreement", which allow competent authorities to share the personal data among criminal matters organization in order to prevent and suppress crime including terrorism. Negotiations were launched on 28 March 2011 and, after more than 5 years of plenty discussing rounds, it was agreed in June 2nd 2016 and was adopted by Council of the European Union on December 2nd 2016**.**

4.3. Legal content and consequences of the reform of the EU-US Personal Data Protection regime

This section will concentrate on 4 instruments; The EU General Data Protection Regulation (**GDPR**), Directive 2016/680 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data (**Directive on Criminal Matters**),The EU-US Privacy Shield (**Privacy Shield**) and The EU-US Umbrella Agreement (**Umbrella Agreement**), which setting a treaty-binding standard for personal data protection and State parties have obligation to comply with such instruments domestically and internationally.

Mention the consequences of 4 Instruments to state parties. It found the stronger obligation and brings in rights for individual and duty for controller/processor then creating a concrete system to monitor, remedy and sanction. The value added, improvements and shortcomings of those instruments will be reviewed in 12 different categories below.

4.3.1. Individual's Right to Personal Data Protection

First of all, the harmonization these 4 instruments try to create will be described. Then, the scope of application and definition of important terms will be illustrated. Third, the improvements in some rights due to the progress of information technology will be shown. Lastly, it draws the line of balance, between rights of Individual and the exception for to limit the full enjoyment of right to personal data protection for specific reason. All 4 issues that 4 instruments have given in their E-Market Regime will be the fundamental baseline for individual protection.

4.3.1.1. Legal Approval of Personal Data Protection

This section will concentrate on how these 4 instruments try to unify the regime of data protection in EU and EU-US E-Market. The achievements and failures of general protection of personal data and in specific area of criminal matters between EU and US regime will be depicted.

EU GDPR

General Data Protection Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data(Regulation level) (the "**GDPR**"), and repealing Directive 95/46/EC[35].

On 6 April 2016 the Council of the European Union published the final text of the GDPR. The GDPR will enter into force on 24 May 2018, two years after its publication in the Official Journal of the European Union ("**OJ**") and it will implement a harmonized data protection regime throughout the EU. The EU institutions agreed the text of the GDPR in December 2015 and this text was then translated and refined for publication in the OJ.

The GDPR will replace Directive 95/46/EC (the current European data protection law), on which the primary Irish data protection legislation, the Data Protection Acts 1988 and 2003, is based.[36] The GDPR contains a number of provisions which will serve to increase accountability of data controllers and processors including expansion of the duties of data controllers and processors; increased reporting obligations; and strengthened individual rights.

GDPR create Greater harmonization[37]: The Regulation introduces a single-legal framework that applies across all EU Member States without the need for national implementation. This means that businesses will face a *more consistent set of data protection obligations* from one EU Member State to the next, which should aid overall compliance. However, harmonization will not be complete and some differences will persist across the EU Member States.[38]

EU Directive on Criminal Matters

From May 6th 2018, the Directive on Criminal Matters will harmonize the laws in the Member States in respect of the exchange of information between police and

[35] EU. *General Data Protection Regulation*. 2016, Article 94.

[36] Arthur Cox. "Data Protection Update – New Legislation." *Technology & Innovation*, 2016, p. 1.

[37] EU. *General Data Protection Regulation.* 2016, Preamble Recital 2.

[38] Hunton&Williams. *Overview of the EU General Data Protection Regulation*. 2016, p. 1.

judicial authorities, whilst leaving discretion in specific areas (for example, penalties for breach of the Directive) in order to respect the different legal traditions of the Member States. The Directive applies to both cross-border and domestic processing of personal data and it aims to improve cooperation of the Member States in the fight against terrorism and other serious crime across the EU, in that, it guarantees that personal data transferred outside the EU by criminal law enforcement authorities will be adequately protected. The key principles of processing personal data only when necessary, proportional and pursuant to a specific purpose are also reflected in the Directive.

As Directive 95/46/EC does not apply to the processing of personal data in the course of an activity which falls outside the scope of European Community law and the Framework Decision 20008/977/ JHA does not regulate internal data processing activities of law enforcement, the Police and Criminal Authorities Directive bridges this legislative gap.[39] The Directive on Criminal Matters will create a coherent framework for data processing activities performed for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security.

EU-US Privacy Shield

On 29 February 2016, the European Commission published a Communication, a draft adequacy decision and the annexed texts constituting a new framework for transatlantic exchanges of personal data for commercial purposes: the EU-U.S. Privacy Shield, which seeks to replace the previous U.S. Safe Harbor invalidated by the Court of Justice of the European Union on 6 October 2015, in the Schrems case. The Privacy Shield could be assessed both the commercial aspects and the possible derogations to the principles of Personal Data Protection for national security, law enforcement and public interests purposes.

The Privacy Shield is the first adequacy decision that has been drafted and agreed since the texts of the GDPR were approved. Still, many of the improvements on the level of data protection offered to individuals are not reflected in the Privacy Shield. The review of this adequacy decision has taken place shortly after the GDPR enters into

[39] Arthur Cox. "Data Protection Update – New Legislation." *Technology & Innovation*, 2016, p. 2.

application in May 2016.[40] Moreover, the adequacy decisions issued for other third countries must be considered as well to meet the standard of GDPR.

The principles and guarantees afforded by the Privacy Shield are set out in both the adequacy decision and in its annexes makes the information both difficult to find, and at times, inconsistent. These separated documents affect the understanding of data subjects because of an overall lack of clarity regarding the new framework. As well as making accessibility for data subjects, organizations, and data protection authorities more difficult. Similarly, the language used lacks clarity.[41]

The EU-U.S. Privacy Shield framework ensures an adequate level of protection for personal data transferred to the U.S. The EU-US Privacy Shield consists of Privacy Principles that companies must abide by and commitments on how the arrangement will be enforced (written commitments and assurance by the State Secretary John Kerry, Commerce Secretary Penny Pritzker, the Federal Trade Commission and the Office of the Director of National Intelligence, amongst others).[42]

EU-US Umbrella Agreement

The EU-US data protection "Umbrella Agreement" puts in place a comprehensive high-level data protection framework for EU-US law enforcement cooperation. The Agreement covers all personal data (for example names, addresses, criminal records) exchanged between the EU and the U.S. for the purpose of prevention, detection, investigation and prosecution of criminal offences, including terrorism. The provisions of the Umbrella Agreement aim at the protection of the fundamental right to the protection of personal data and the right to an effective remedy and to a fair trial, as enshrined, respectively, in Article 8 and Article 47 of the Charter of Fundamental Rights of the European Union.

[40] Article 29 Data Protection Working Party. *Opinion 01/2016 on the EU – U.S. Privacy Shield draft adequacy decision*. 13 Apr. 2016, p. 58.

[41] Ibid, p. 3.

[42] European Commission. *EU-U.S. Privacy Shield: Frequently Asked Questions.* Press Release Database. Brussels, 29 Feb. 2016

The Umbrella Agreement will provide safeguards and guarantees of lawfulness for data transfers, thereby strengthening fundamental rights, facilitating EU-U.S. law enforcement cooperation and restoring trust. In particular, EU citizens will benefit from equal treatment: they will have the same judicial redress rights as US citizens in case of privacy breaches. This point was outlined by President Juncker in his political guidelines, when he stated: "*The United States must [...] guarantee that all EU citizens have the right to enforce data protection rights in U.S. courts, whether or not they reside on U.S. soil. Removing such discrimination will be essential for restoring trust in transatlantic relations*".[43] However, implementation by EU Member States will be necessary, but no major changes in the laws are to be expected since the substantive provisions of the Umbrella Agreement reflect to a large extent rules that are already applicable to EU and national authorities under EU and/or national law.

The Umbrella Agreement is expected to have a significant impact on police and law enforcement cooperation with the United States. By establishing a common and comprehensive framework of data protection rules and guarantees, it will enable the EU or its Member States, on the one hand, and U.S. criminal law enforcement authorities on the other hand to cooperate more effectively with each other. Moreover, it will ensure that existing agreements contain all necessary protections. This will enable continuity in law enforcement cooperation while ensuring greater legal certainty when transfers are made. The Agreement will also facilitate the conclusion of future data transfer agreements with the U.S. in the criminal law enforcement sector, as data protection safeguards have been agreed and will thus not have to be negotiated again and again.[44] Accordingly, setting common standards in this key but complex area of cooperation is an important achievement that can significantly contribute to restoring trust in transatlantic data flows.

In addition, Umbrella Agreement clearly states that "*the protections and remedies set forth in this Agreement shall benefit individuals and entities in the manner*

[43] European Commission. *Questions and Answers on the EU-US data protection "Umbrella agreement"*. Brussels, 8 Sep. 2015, p. 1.

[44] European Commission. *Proposal for a COUNCIL DECISION on the signing, on behalf of the European Union, of an Agreement between the United States of America and the European Union on the protection of personal information relating to the prevention, investigation, detection, and prosecution of criminal offenses*. 29 Apr. 2016, p. 3.

implemented in the applicable domestic laws of each Party",[45] which means that the Agreement, in order to be effective ("to benefit individuals and entities"), needs to be implemented in the domestic legal systems of the Parties. Further analysis is needed to verify to which extent, also in the light of the *Medellin* jurisprudence,[46] the Agreement can be considered as a self-executing agreement in the US legal order and which substantive provisions may be needed to be implemented by the US Congress[47] in order to make it binding domestic law.

4.3.1.2. Definition and Scope of Personal Data Protection

These 4 Instruments harmonize the basic terms, scope and element of Personal Data Protection in to one direction. Moreover, the most important issue on jurisdiction, the fragmented jurisdictions to deal with trans-border activities, will be resolved by the application of these instruments, at least within EU-US E-Market regime. This section will highlight on the influence of GDPR as the prominent law that others instrument refer to.

EU GDPR

Personal data is defined as "any information relating to an identified or identifiable natural person".[48] A low bar is set for "identifiable" – if anyone can identify a natural person using "all means reasonably likely to be used" [49] the information is personal data, so data may be personal data even if the organization holding the data cannot itself identify a natural person. A name is not necessary either – any identifier will do such as an identification number, location data, an online identifier or other factors which may identify that natural person.

Online identifiers are expressly called out in Recital 30 with IP addresses, cookies and RFID tags all listed as examples. Although the definition and recitals are broader

[45] EU-US. *Umbrella Agreement*. 2016, Article 5(2).

[46] Garcia, Michael J. "International Law and Agreements: Their Effect Upon Us Law." *Washington: Congressional Research Service, marzo*, 2013.

[47] European Data protection Supervisor. *Opinion 1/2016.* 12 Feb. 2016, p. 8.

[48] EU. *General Data Protection Regulation*. 2016, Article 4.

[49] Ibid, Recital 26.

than the equivalent definitions in the Directive 95/46/EC, for the most part they are simply codifying current guidance and case law on the meaning of 'personal data'. [50]

GDPR also includes a broader definition of "special categories" of personal data which are more commonly known as sensitive personal data. [51] The processing of these data is subject to a much more restrictive regime.

A new concept of 'pseudonymisation' is defined as the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organizational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.[52] Organizations which embed pseudonymisation techniques gain various benefits under GDPR.

Hence, the Regulation introduces a concept of *'pseudonymised data'* (i.e., key-coded or enhanced data). Pseudonymous data will still be treated as personal data, but is likely to help organisations comply with the Regulation and reduce the risks of non-compliance. The 'key' necessary to identify individuals from the pseudonymised data must be kept separately and subject to technical and organisational measures to ensure non-attribution to an identified or identifiable person.[53]

GDPR applies to processing of personal data "in the context of the activities of an establishment"[54] of any organization within the EU. For these purposes "establishment" implies the "effective and real exercise of activity through stable arrangements" [55] and "the legal form of such arrangements…is not the determining factor" [56], so there is a wide range of what might be covered from fully functioning subsidiary undertakings on the scope, to potentially any individual sales representative depending on the situations.

---

[50] DLA Piper. "EU General Data Protection Regulation - Key Changes." www.dlapiper.com/en/uk/focus/eu-data-protection-regulation/key-changes/. Accessed 10 May 2016.

[51] EU. *General Data protection Regulation,* Article 9.

[52] Ibid, Article 4.

[53] Hunton&Williams. *Overview of the EU General Data Protection Regulation.* p. 3.

[54] EU. *General Data Protection Regulation.* 2016, Article 3(1).

[55] Ibid, Recital 22.

[56] Ibid, Recital 22.

The Regulation elucidate that it also applies to companies established in a third country if they are offering goods and services, or monitoring the behavior of individuals, in the EU. Companies placed outside of the EU will be obliged to the same rules as companies based in the EU. This ensures the comprehensive protection of EU individuals' rights. It generates an arena between EU and foreign companies, thereby avoiding competitive imbalances between EU and foreign companies when operating in the EU or targeting consumers in the EU. Even if an organization is able to prove that it is not established within the EU, it will still be caught by GDPR if it processes personal data of data subjects who are in the Union where the processing activities are related "to the offering of goods or services"[57] (no payment is required) to such data subjects in the EU or "the monitoring of their behaviour"[58] as far as their behavior takes place within the EU. Internet use profiling[59] is expressly referred to as an example of monitoring.

Compared to the old Directive 95/46/EC, GDPR will capture many more overseas organizations. US tech should particularly take note as the provisions of GDPR have clearly been designed to capture them.[60] Overseas organizations not established within the EU who is nevertheless caught by one or both of the offering goods or services or monitoring tests must designate a representative within the EU[61].

GDPR also include an expanded territorial scope[62]: Non-EU businesses will be subject to the Regulation if they: (i) offer goods or services to EU residents; or (ii) monitor the behaviour of EU residents. Many non-EU businesses that were not required to comply with the Directive 95/46/EC *will be required to comply with the Regulation*.[63]

[57] Ibid, Article 3(2)(a).

[58] Ibid, Article 3(2)(b).

[59] Ibid, Recital 24.

[60] DLA Piper. "EU General Data Protection Regulation - Key Changes." www.dlapiper.com/en/uk/focus/eu-data-protection-regulation/key-changes/. Accessed 10 May 2016.

[61] EU. *General Data Protection Regulation.* 2016, Article 27.

[62] Ibid, Article 3.

[63] Hunton&Williams. *Overview of the EU General Data Protection Regulation.* p. 1.

EU Directive on Criminal Matters

The Scope of data protection and free movement of data processed by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties has been designated by the directive, allowing Member States a certain level of flexibility while incorporating it into their respective national laws,[64] whereas a regulation was adopted for regulating general processing of personal data. In this way the EU acknowledged a two-speed process in the effort to harmonize all EU personal data processing.

The new Directive on Criminal Matters has 3 perspectives, which scope is drawn and legal terms are defied, differently from the GDPR:

First, its scope is restricted to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, not covering personal data processing in the context of criminal court proceedings. In other words, where the personal data are processed in the course of a criminal investigation and court proceedings in criminal matters, Member States may provide for the exercise of the right to information, access and rectification or erasure of personal data to be carried out in accordance with their national law[65]. In this respect, therefore, the real added value of the Directive for data protection in the police and justice sectors depends on its implementation in national law and the willingness of national court to ensure that the Directive for data protection in the police and justice sectors is applied in a uniform manner across the EU. [66]

Second, the Directive on Criminal Matters does not regulate the processing of data in the course of an activity which falls outside the scope of Union law[67]. That provision has been interpreted[68] as relating to activities concerning national security, activities of

[64] Maesa, Costanza D F. *Balance Between Security and Fundamental Rights Protection: an Analysis of The Directive 2016/680 for Data Protection in The Police and Justice Sectors and the Directive 2016/681 on the Use of Passenger Name Record (PNR).* 2016, p. 4.

[65] EU. *Directive 2016/680 (Directive on Criminal Matters).* 2016, Recitals 20, 49 and 107 and Article 18.

[66] Maesa, Costanza D F. *Balance Between Security and Fundamental Rights Protection: an Analysis of The Directive 2016/680 for Data Protection in The Police and Justice Sectors and the Directive 2016/681 on the Use of Passenger Name Record (PNR).* 2016, p. 5.

[67] EU. *Directive 2016/680 (Directive on Criminal Matters).* 2016, Article 2(3).

[68] Ibid, Recitals 14.

agencies or units dealing with national security issues and the processing of personal data by the Member States when carrying out activities which fall within the scope of Chapter 2 of Title V of the Treaty of European Union. The formulation of that provision is therefore partially contradictory with the inclusion within the purposes set out in Article 1 of safeguarding against and the prevention of threats to public security. Even if it is not defined in the text, the concept of activities concerning public security seems to include the activities of safeguarding against and prevention of threats to public security. Until the Court of Justice interprets it, the scope of the Directive for data protection in the police and justice sectors depends again on the interpretation that national courts will give to the expression "activity which falls outside the scope of Union law" and of the way the Member States decide to implement the Directive[69] for data protection in the police and justice sectors.

Finally, the Directive on Criminal Matters does not apply to the processing of personal data by the Union institutions, bodies, offices and agencies. In other words, the data processing by the European institutions and bodies will continue to be governed by Regulation n.45/2001, which has not been amended yet. Unlike the Framework Decision 2008/977/JHA, the Directive for data protection in the police and justice sectors will actually regulate processing of personal data by Member States and not only intra-Member States exchanges of data, but it is still far from ensuring maximum harmonization of data processing in the criminal field. That is confirmed by Article 1(3), which states that the Directive for data protection in the police and justice sectors shall not preclude Member States from providing higher safeguards than those established in the Directive[70] for the protection of the rights and freedoms of the data subject. Directive, unlike the Framework Decision 2008/977/JHA, also applies to domestic processing of personal data.

Spy agencies and national security agencies are not bound by this Directive. (That means that it's okay for them to gather personal data, subject to their own mandates and contesting regulations.). As well as the Anonymous information is not covered by this Directive.

[69] Maesa, Costanza D F. *Balance Between Security and Fundamental Rights Protection: an Analysis of The Directive 2016/680 for Data Protection in The Police and Justice Sectors and the Directive 2016/681 on the Use of Passenger Name Record (PNR).* 2016, pp. 5-6.

[70] Ibid, p. 6.

As far as the scope of the Directive for data protection in the police and justice sectors is concerned, despite the apparent broad approach of the Directive for data protection in the police and justice sectors, its actual scope is more limited than it seems at first glance.

EU-US Privacy Shield

EU Data Protection laws apply not only to the processing operations carried out by data controllers established on EU member states territory, but also where data controllers (although not established in the EU), make use of equipment situated on EU territory, in particular for the collection of personal data. Hence, The Privacy Shield Principles will apply from the moment the data transfer takes place.[71] Moreover, the data controllers established in the EU and transferring data to a data processor in the U.S. remain subject to EU data protection law.

The Privacy Shield which allows personal data to be transferred from the EU to a company in the United States, provided that the company there processes (e.g. uses, stores and further transfers) personal data according to a strong set of data protection rules and safeguards. The protection given to user's personal data applies regardless of whether data subjects are an EU citizen or not.

When compare Privacy Shield to the Safe Harbor, improvements can be noticed on the addition of some key definitions such as 'personal data', 'processing' and 'controller'.

The Principles apply immediately upon organization's register to certification. However, organization shall certify within the two first months following the Privacy Shield's framework effective date of entry into force. In any event they should do so no later than nine months[72] from the date upon which they certify to the Privacy Shield.

EU-US Umbrella Agreement

The key terms of the Umbrella Agreement are defined in Article 2. The definitions of "personal information", "processing of personal information", "Parties",

[71] Article 29 Data Protection Working Party. *Opinion 01/2016 on the EU – U.S. Privacy Shield draft adequacy decision.* 13 Apr. 2016, p. 12.

[72] Ibid, p.18.

"Member State" and "Competent Authority" are substantially in line with how these concepts have been defined in other EU-U.S. agreements and/or in the EU data protection *acquis*.[73] The Agreement is proposed to achieve the policy objective of establishing a framework for the protection of personal data when transferred between the United States, on the one hand, and the European Union or its Member States, on the other, in the context of law enforcement;[74] for the prevention, investigation, detection or prosecution of criminal offences, including terrorism. By specifying that the Umbrella Agreement in itself shall not be the legal basis for any transfer of personal information and that a (separate) legal basis shall always be required, Article 1 also makes clear that the Umbrella Agreement is a genuine fundamental right agreement establishing a set of protections and safeguards applying to such transfers. [75] This includes transfers on the basis of domestic laws, EU-US agreements, Member States-U.S. agreements (e.g. Mutual Legal Assistance Treaties) as well as specific agreements providing for the transfer of personal data by private entities for law enforcement purposes.[76] The bilateral agreements between the *Member States* and the US are also brought in the scope of the Agreement. However, The Intelligence Authorities and national security agencies are not in the scope of the Agreement, pursuant to Article 3(2)[77] for example Central Intelligence Agency (CIA) which is under Privacy Shield provisions.

This means that the Umbrella Agreement must be seen in a wider context than just transatlantic law enforcement cooperation: it clearly links to:[78]

[73] European Commission. *Proposal for a COUNCIL DECISION on the signing, on behalf of the European Union, of an Agreement between the United States of America and the European Union on the protection of personal information relating to the prevention, investigation, detection, and prosecution of criminal offenses*. 29 Apr. 2016, p. 6.

[74] Ibid, p. 5.

[75] Ibid, p. 6.

[76] European Commission. *Communication From The Commission to The European Parliament and The Council Transatlantic Data Flows: Restoring Trust through Strong Safeguards, COM(2016) 117 final*. Brussels, 29 Feb. 2016, p. 13.

[77] EU-US. Umbrella Agreement. 2016, Article 3(2): "transfers or other forms of cooperation between the authorities of the Member States and of the United States other than those referred to in Article 2(5), responsible for safeguarding national security"

[78] Korf, Douwe. "EU-US Umbrella Data Protection Agreement : Detailed Analysis by Douwe Korff." *European Area of Freedom Security & Justice*, 2015, https://free-group.eu/2015/10/14/eu-us-umbrella-data-protection-agreement-detailed-analysis-by-douwe-korff/. Accessed 23 Dec. 2016.

- cooperation including data sharing between the Legal Enforcement Agencies (LEAs) of the EU and/or of the EU Member States (MSs), the security-related agencies of the EU, and the National Security Agencies (NSAs) of the MSs;
- cooperation and data sharing between LEAs of the USA and its NSAs (including the NSA);
- cooperation and data sharing between the NSAs of the EU MSs and those of the USA; and
- cooperation and data sharing between the NSAs of the EU MSs and those of the USA and the NSAs of other states ("third parties" in the terms of the Umbrella Agreement).

Umbrella Agreement does not contain any specific reference to the *rationae personae* scope of the Agreement. It establishes a wide *rationae materiae* scope.[79] This general reference to personal information seems to imply that the personal information of any individual equally enjoys the safeguards enshrined in the Agreement. This interpretation is encouraged by specific references to a wide personal scope of "Access" [80], "Rectification" [81] and "Administrative redress" [82] (since they refer to "any individual"). However, it may be contradicted by the general "Non-discrimination" provision in Article 4. According to this Article, each Party must comply with the obligations of the Agreement to protect "*personal information of its own nationals and the other Party's nationals"* without arbitrary discrimination. In addition, Article 19 "Judicial redress" only applies to "Nationals" of the Parties.

The agreed provisions will thus immediately increase the level of protection guaranteed to EU data subjects "when" data is transferred to the U.S. It will also increase legal certainty for transatlantic law enforcement cooperation by ensuring that exiting agreements contain all necessary protections and can thus withstand possible legal challenges

[79] EU-US. *Umbrella Agreement.* 2016, Article 3.

[80] Ibid, Article 16.

[81] Ibid, Article 17.

[82] Ibid. Article 18.

between EU State Members and US.[83] Nonetheless, the Agreement would not be compliant with the protection afforded by Articles 7, 8 and 47 of the EU Charter on Fundamental Rights, according to which the fundamental rights to privacy, personal data protection and an effective remedy apply to "everyone" in the EU, irrespective of nationality or status.[84]

4.3.1.3. Content of Data Subjects' Right to Data Protection

These 4 instruments unite the detail of Data Subjects' Rights. The content of Right includes some important issues that reflect the changing manner of data protection in the era of Internet, especially the Right to be Forgotten/Right to Erase and Data Portability. Furthermore, they give a more concise edge for all rights relate to Personal Data Protection. The instruments make it clear that the Right to Personal Data Protection is specific right, separate from right to privacy, but have some legal interaction to some other human rights.

EU GDPR

GDPR builds on the rights of individual data subjects under the Directive 95/46/EC, ensuring existing rights and offering a new right to data portability. These rights are supported with provisions making it easier to claim redress for compensation and for consumer groups to enforce rights on behalf of data subjects.

Those individual rights are as follows:

Transparency: One of the main constructing sets of GDPR's realized rights for data subjects is the requirement for clearer transparency. Vary information must be provided by controllers to data subjects in a concise, transparent and easily accessible form, using easy and understandable language[85].

The following information must be given at the time the data is acquired: [86]

- the identity and contact details of the controller

[83] European Data protection Supervisor. *Opinion 1/2016.* 12 Feb. 2016, p. 10.

[84] Ibid, pp. 10-11.

[85] EU. *General Data Protection Regulation.* 2016, Article 12(1).

[86] Ibid, Article 13.

- the Data Protection Officer's contact details (if there has to be)
- both the purpose for which data will be processed and the legal basis for processing including if relevant the legitimate interests for processing
- the recipients or categories of recipients of the personal data
- details of transborder transfers
- the period for which personal data will be stored or, if that is not possible, the criteria used to determine this
- the existence of rights of the data subject including the right to access, rectify, require erasure (the "right to be forgotten"), restrict processing, object to processing and data portability; where applicable the right to withdraw consent, and the right to lodge complaint to supervisory authorities
- the consequences of failing to meet data necessary to enter into a contract
- the presence of any automated decision making and profiling and the consequences for the data subject.
- In addition, where a controller intends to process existing data for a new purpose, they must notice data subjects of that further processing, providing the information mentioned above.

Slightly different transparency requirements apply where information have not been obtained from the data subject. [87]

Subject access rights: These widely follow the existing regime set out in the Directive 95/46/EC though some supplementary information must be revealed and there is no longer a right for controllers to charge a fee, with some narrow limitations. Information requested by data subjects must be provided within one month as a default with a limited right for the controller to extend this period for up to three months.[88]

[87] Ibid, Article 14.

[88] Ibid, Article 15.

Right to rectify: Data subjects continue to enjoy a right to require inaccurate or incomplete personal data to be corrected or completed "without undue delay".[89] However, GPDR does not give a specific meaning and scope of the condition mention above.

Right to erasure ('right to be forgotten'): This forerunner of this right made headlines in 2014 when Europe's highest court ruled against Google[90] as mentioned before in Chapter 4, in effect requiring Google to remove search results relating to historic proceedings against a Spanish national for an unpaid debt on the basis that Google as a data controller of the search results had no legal basis to process that information.

The right to be forgotten now has a separate single Article in GDPR. However, the right is not absolute; it only arises in quite limited situations notably where the controller has no legal basis for processing the information. As demonstrated in the Search Engine, requiring a search engine to remove search links does not mean the underlying content controlled by third party websites will necessarily be removed. In many cases the controllers of those third party websites may have entirely legitimate grounds to continue to process that information, even if that the information is less likely to be found if search results are removed from search engine results.[91]

The possible impact of Google Spain decision has been a great number of requests made to search engines for search results to be removed raising concerns that the right is being used to remove information that it is in the public interest to be accessible.

Right to restriction of processing: Data subject enjoys a right to restrict processing of their personal data in defined circumstances. These include where the accuracy of the data is contested; where the processing is unlawful; where the data is no longer needed save for legal claims of the data subject, or where the legitimate grounds for processing by the controller and whether these override those of the data subject are contested. [92]

Right to data portability: This is an obviously modes right in GDPR and has no previous in the Directive 95/46/EC. Where the processing of personal data is justified either on the basis that the data subject has given their consent to processing or where

[89] Ibid, Article 16.

[90] CJEU. *Case C-131/12 Google Inc. v Agencia Española de Protección de Datos.* 13 May 2014.

[91] Ibid, Article 17.

[92] EU. *General Data Protection Regulation.* 2016, Article 18.

processing is necessary for the performance of a contract, or where the processing is carried out be automated means, then the data subject has the right to receive or have transmitted to another controller all personal data relating them in a structured, commonly used and digital-readable format. This right is a good example of the regulatory downsides of relying on consent or performance of a contract to justify processing. [93]

The right to data portability comes with various packages under GDPR relative to other justifications for processing. Where the right is likely to arising controllers will need to develop procedures to facilitate the collection and transfer of personal data when requested to do so by data subjects. [94]

Right to object: The Directive 95/46/EC's right to object to the processing of personal data for direct marketing purposes at any time is maintained.

Supplementary, data subjects have the right to object to processing which is legitimized on the grounds either of the legitimate interests of the data controller or when processing is in the public interest. Controllers will then have to suspend processing of the data until such time as they expose "compelling legitimate grounds" for processing which overshadow the rights of the data subject or that the processing is for the establishment, exercise or defense of legal claims. [95]

The right not to be subject to automated decision taking, concerning profiling: This right expands the old Directive 95/46/EC right not to be subject to automated decision making, profiling. GDPR specially refers to profiling as a representation of automated decision making. Automated decision making and profiling "which produces legal effects concerning [the data subject] … or similarly significantly affects him or her" are only permitted where:[96]

(a) necessary for entering into or performing a contract

(b) authorized by EU or Member State law, or

(c) the data subject has given their explicit (i.e. opt-in) consent.

---

[93] Ibid, Article 20.

[94] DLA Piper. "EU General Data Protection Regulation - Key Changes." www.dlapiper.com/en/uk/focus/eu-data-protection-regulation/key-changes/. Accessed 10 May 2016.

[95] EU. *General Data Protection Regulation.* 2016, Article 21.

[96] Ibid, Article 22.

The scope of this right is possibly broad and may throw into question legitimate profiling for example to detect fraud and cybercrime. It also presents challenges for the online advertising industry and website operators who will need to revisit consenting mechanics to justify online profiling for behavioral advertising. This is an area where further guidance is needed on how Article 22 will be applied to specific types of profiling. [97]

EU Directive on Criminal Matters

One of the main differences between GDPR and Directive on Criminal Matters lies essentially in the rights of information and of access to personal data. If such rights provided for in the Data Protection Regulation were exercised to the fullest possible extent within the ambit of criminal law, [98] it would effectively make criminal investigations impossible.

Where the data subject is required to comply with a legal obligation, the data subject has no genuine and free choice, so that the reaction of the data subject could not be considered to be a freely given indication of his or her wishes. Whether the correct balance between individual data protection and the interests of the police and criminal justice process is respected depends once again on how Member States implement the exemptions[99] contained in the Directive for data protection in the police and justice sectors.

Consent is not needed for the collection of personal data for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties since the nature of investigation is undercover to keep secret from targeted convicts.

Data subject have the right to know who has collected personal data about them and the purposes of the collection, and the right to lodge a complaint and have the data

[97] DLA Piper. "EU General Data Protection Regulation - Key Changes." www.dlapiper.com/en/uk/focus/eu-data-protection-regulation/key-changes/. Accessed 10 May 2016.

[98] Maesa, Costanza D F. *Balance Between Security and Fundamental Rights Protection: an Analysis of The Directive 2016/680 for Data Protection in The Police and Justice Sectors and the Directive 2016/681 on the Use of Passenger Name Record (PNR).* 2016, p. 4.

[99] Ibid, p. 6.

expunged.[100] If the data controller refuses, then the reasons for the refusal have to be disclosed.

Data subject be free from "automatic processing" that "profiles" them and they should have the right to challenge any profiling. "Profiling" means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyze or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location or movements. [101]

The issue of further processing could be permitted as long as the controller was authorized to process the personal data for such purpose according to either Union or Member State law and that the processing was necessary and proportionate to the other purposes in accordance with Union or Member State law. [102]

The right to access has been restricted, the Member States must provide that controller informs the data subject of the reasons for this refusal, unless the purpose of the measure, for example an investigation would be jeopardized if the data subject would be informed[103] about the reasons for the restriction.

The data subject has the right to rectify, erase or restrict the processing of his or her personal data. The data subject can restrict his or her personal data instead of erasing them in two specified cases. The first situation is where the data subject contests the accuracy of the data and it is not possible to verify whether the data is accurate or not. The other case relates to situations where the personal data is kept for the purpose of evidence. [104] The corresponding recital specifies that examples of the latter case can be situations where there are reasonable grounds to believe that the legitimate interests of the data subject could be affected. In the latter situation the data can be processed only for the reasons which prevented their erasure.

[100] Council of the European Union. *5418/16 ADD 1*. 2016, p. 11.

[101] EU. *Statement of the Council's reasons: Position (EU) No 5/2016 C158/46*. 2016, p. 5.

[102] Ibid, p. 7.

[103] Council of the European Union. *5418/16 ADD 1.* 2016, p. 11.

[104] EU. *Statement of the Council's reasons: Position (EU) No 5/2016 C158/46.* 2016, p. 4.

EU-US Privacy Shield

The Privacy Shield maintains the Safe Harbor's access principle, including the rights to amend, correct, or delete inaccurate data. The Privacy Shield improves these rights, enabling data subjects to correct, amend, or delete even accurate personal data where such information is processed in violation of the Privacy Shield principles.[105]

The Privacy Shield provides for a right to opt-out to disclosure of personal information to a third party or to the use of personal information for a purpose materially different.[106] In addition, individuals benefit from an 'opt-out' right to the use of personal information for direct marketing purpose at any time.[107]

Data subject have the right to ask the Privacy Shield organization to give data subject access to personal data of data subject.[108] This means that data subjects have a right to have data communicated to them but also to get information about the purpose for which the data are processed,[109] the categories of personal data concerned and the recipients to whom the data are disclosed.

Data subject can then request the company to correct, change or delete them if they are not accurate, outdated or have been processed in violation of the Privacy Shield rules.[110] The company also has to confirm whether or not it holds or processes personal data.[111]

Data subject are normally not obliged to give any reasons as to why data subject would like to access personal data, however, the company may ask data subject to do so if the request is too broad or vague.[112] The company has to respond to data subject's access request within a reasonable time frame. A company may sometimes be able to limit

[105] Wilmer Cutler Pickering Hale and Dorr LLP. "Comparison of Requirements under the Privacy Shield/Safe Harbor Principles." *Lexology*, 25 Jul. 2016, p. 7.

[106] EU-US. *Privacy Shield.* 2016, Annex II, III, 2.

[107] Ibid. Annex II, III.12.a. This is identical as what was provided in the Safe Harbor scheme and not changed has been made as this regard.

[108] EU-US. *Privacy Shield.* 2016, Annex II, III.8.

[109] European Commission. *Guide to EU-US Privacy Shield.* 2016, p. 11.

[110] EU-US. *Privacy Shield.* 2016, Annex II, II.6.

[111] European Commission. *Guide to EU-US Privacy Shield.* 2016, p. 11.

[112] EU-US. *Privacy Shield.* 2016, Annex II, III.8.a.i.

access rights of data subject, but only in specific situations such as when providing access would undermine confidentiality, breach professional privilege or conflict with legal obligations.[113]

The right to access can be particularly useful if personal data are used for a decision which might significantly affect data subject. In those situations where this typically becomes relevant[114] (e.g. a positive or negative decision about a job, a loan etc.), U.S. law provides additional rights that allow data subject to better understand[115] to what extent personal data have been taken into account.

If the company does not follow the rules of the Privacy Shield and violates its obligation to protect your personal data,[116] data subjects have the right to complain and obtain a remedy, free of any cost.[117] For instance data subject can choose alternative dispute resolution (ADR) or submit to the oversight of a national Data Protection Authority (DPA).

EU-US Umbrella Agreement

The Umbrella Agreement provides for several rights of the data subject: the right to be informed[118], the right of access[119], the right to rectification - which also refers to erasure and blocking[120], the rights to administrative and judicial redress[121] and the right not to be subject to automated decisions[122]. The rights of the data subject, and in particular the rights to access and rectification, are enshrined as essential elements of the right to personal data protection in Article 8(2) of the EU Charter on Fundamental Rights.

[113] European Commission. *Guide to EU-US Privacy Shield.* 2016, p. 11.

[114] EU-US. *Privacy Shield.* 2016, Annex II, III.8.e.

[115] European Commission. *Guide to EU-US Privacy Shield.* 2016, p. 11.

[116] EU-US. *Privacy Shield.* 2016, Annex I.

[117] European Commission. *Guide to EU-US Privacy Shield.* 2016, p. 12.

[118] EU-US. *Umbrella Agreement.* 2016, Article 20.

[119] Ibid, Article 16.

[120] Ibid, Article 17.

[121] Ibid, Articles 18-19.

[122] Ibid, Article 15.

The Excessive expenses may not be imposed as a condition to access one's data[123] due to the precise exemptions listed in article 16(2).

The right to rectification entitles any individual to request the correction or rectification of his or her personal data in case it is either inaccurate or it has been improperly processed. This may include supplementation, erasure, blocking or other measures or methods[124] for addressing inaccuracies or improper processing. The article 17(3) allows data subjects to appoint Oversight Authority or representative for acting on their behalf. The Competent Authority (Data Controller/Processor) must response to data subject 'if correction or rectification is denied or restricted'[125], setting forth the reasons for the denial or restriction of access or rectification, without undue delay.

However, The Umbrella Agreement fails to meet important substantive requirements of EU data protection law.[126] The Agreement does not contain a general human rights clause prohibiting the "sharing" or "onward transfers" of data on EU persons, provided subject to the Agreement, with or to other agencies, in the USA or elsewhere, in circumstances in which this could lead to serious human rights violations, including arbitrary arrest and detention, torture or even extrajudicial killings or "disappearances" of the data subjects (or others)**.**[127]

4.3.1.4. Exception to the exercise of Right to Personal Data Protection

By taking the court verdicts, analyzed in Chapter3, and the revelations of global data surveillance program of US into account. These 4 instruments give more precise category of limitations on exercising right to personal data protection of individual. They also draw the scope of necessary conditions, on what extent state can limit the right of person, and requirements, on how state must undertake the proportionate measure, in order to relieve the effects of such restrictions.

---

[123] Ibid, Article 16(3).

[124] Ibid, Article 17(2).

[125] EU-US. *Umbrella Agreement.* 2016, Article 17(4).

[126] Korf, Douwe. "EU-US Umbrella Data Protection Agreement : Detailed Analysis by Douwe Korff." *European Area of Freedom Security & Justice*, 2015, https://free-group.eu/2015/10/14/eu-us-umbrella-data-protection-agreement-detailed-analysis-by-douwe-korff/. Accessed 23 Dec. 2016.

[127] Ibid.

EU GDPR

EU Member States domestic data protection laws were very different among Member States. This is partly due to the vague in the Directive 95/46/EC being interpreted and implemented differently and partly due to the Directive allowing Member States to implement different or additional rules in some areas. As GDPR will become supranational direct effect implementing laws, there will be a higher degree of harmonization relative to the current regime. However, GDPR retains the right for Member States to introduce different domestic laws in many important areas and as a result we are likely to continue to see a patchwork of various data protection laws among Member States, for certain types of processing.

Each Member State is permitted to restrict the rights of individuals and transparency obligations[128] by legislation when the restriction "respects the essence of fundamental rights and freedoms and is a necessary and proportionate measure in a democratic society" to safeguard one of the following: [129]

(a) national security

(b) defense

(c) public security

(d) the prevention, investigation, detection or prosecution of breaches of ethics for regulated professions, or crime, or the execution of criminal penalties

(e) other important objectives of general public interest of the EU or a Member State, in particular economic or financial interests

(f) the protection of judicial independence and judicial proceedings

(g) a monitoring, inspection or regulatory function connected with national security, defence, public security, crime prevention, other public interest or breach of ethics

(h) the protection of the data subject or the rights and freedoms of others

(i) the enforcement of civil law claims

[128] EU. *General Data Protection Regulation.* 2016, Recital 73.

[129] Ibid, Article 23(1).

To be a valid exemption for the purposes of GDPR, any legislative exemption must contain specific provisions setting out: [130]

(a) the purposes of processing

(b) the categories of personal data

(c) the scope of the restrictions

(d) the safeguards to prevent abuse or unlawful access or transfer

(e) the controllers who may rely on the restriction

(f) the permitted retention periods

(g) the risks to the rights and freedoms of data subjects

(h) the right of data subjects to be informed about the restriction, unless prejudicial to the purpose of the restriction

Further to these permitted exemptions, Chapter IX of GDPR sets out various specific processing activities which include additional derogations, exemptions and powers for Member States to impose additional requirements. These include:

- Processing and freedom of expression and information[131]
- Processing and public access to official documents[132]
- Processing of national identification numbers[133]
- Processing in the context of employment[134]
- Safeguards and derogations to processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes[135]

[130] Ibid, Article 23(2).

[131] Ibid, Article 85.

[132] Ibid, Article 86.

[133] Ibid, Article 87.

[134] Ibid, Article 88.

[135] Ibid, Article 89.

- Obligations of secrecy[136]
- Existing data protection rules of churches and religious associations[137]

These necessary cases also appear in the Directive 95/46/EC, though in many cases have been amended or varied in GDPR.

EU Directive on Criminal Matters

There are differences between GDPR and Directive on Criminal Matters. Attempting to strike a balance between the individual right to data protection and the processing interests and concerns of the police and other law enforcement-related agencies, limitations on the rights to information, access and rectification have been included in Directive on Criminal Matters. Because it would undermine much of the work done by the police and the competent authorities within the criminal justice system if individual exercise to their fullest extent of these rights.[138] The level of flexibility accorded to this end depends once more on the breadth of national legislative measures implementing the Directive for data protection in the police and justice sectors, which can restrict, wholly or partly, the data subject's right in order to assure the due performance of investigations and protect national security, as set out in Article 15.

That is why special security-related needs have to be accommodated in the text of the Directive for data protection in the police and justice sectors. The Directive on Criminal Matters aims at balancing the data protection objectives with the security policy objectives and, while certainly contributing to the creation of a less fragmented general framework, [139] it doesn't solve all the shortcomings which had emerged before its entry into force. For example, the nature of investigation is undercover to keep secret from targeted convicts which against the principle of data subject's consent and noticed.

[136] Ibid, Article 90.

[137] Ibid, Article 91.

[138] Maesa, Costanza D F. *Balance Between Security and Fundamental Rights Protection: an Analysis of The Directive 2016/680 for Data Protection in The Police and Justice Sectors and the Directive 2016/681 on the Use of Passenger Name Record (PNR).* 2016, p. 6.

[139] Maesa, Costanza D F. *Balance Between Security and Fundamental Rights Protection: an Analysis of The Directive 2016/680 for Data Protection in The Police and Justice Sectors and the Directive 2016/681 on the Use of Passenger Name Record (PNR).* 2016, p. 4.

EU-US Privacy Shield

The Privacy Principles in Annex II of the Privacy Shield contain a derogation that is identical to the derogation that was laid down in the Safe Harbor Privacy Principles.

Consistent with the goal of enhancing privacy protection, organizations should moreover strive to implement the Principles fully and transparently, including indicating in their privacy policies where exceptions to the Principles permitted by the U.S. legal framework will apply on a regular basis. For the same reason, where the option is allowable under the Principles and/or U.S. law, organizations are expected to opt for the higher protection where possible. [140]

The Privacy Shield is stated that, adherence to the Privacy Principles may be limited:[141]

(a) to the extent necessary to meet national security, public interest, or law enforcement requirements;

(b) by statute, government regulation, or case law that creates conflicting obligations or explicit authorizations, provided that, in exercising any such authorization, an organization can demonstrate that its non-compliance with the Principles is limited to the extent necessary to meet the overriding legitimate interests furthered by such authorization; or

(c) if the effect of the Directive or Member State law is to allow exceptions or derogations, provided such exceptions or derogations are applied in comparable contexts.

Nonetheless, there are rules in place in the United States designed to limit any interference for national security purposes with the fundamental rights of the persons whose personal data are transferred from the EU to the US under the Privacy Shield to what is strictly necessary to achieve the legitimate objective in question.[142]

---

[140] Article 29 Data Protection Working Party. *Opinion 01/2016 on the EU – U.S. Privacy Shield draft adequacy decision.* 13 Apr. 2016, pp. 33-34.

[141] EU-US. *Privacy Shield.* 2016, Annex II, I.5.

[142] EU Commission. *Draft Commission Decision pursuant to Directive 95/46/EC of the European parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield.* 2016, para.75.

Privacy Shield requires the US authorities to set out the safeguards and limitation and oversight mechanism in place for any access to data by public authorities for national security purposes. Therefore, US affirm that there is no indiscriminate, mass surveillance. For complaints on possible access by national intelligence authorities, a new Ombudsperson mechanism will be set up for monitoring, independent from the intelligence services.[143]

EU-US Umbrella Agreement

Umbrella Agreement has given the sweeping exceptions and exemptions from the normal rules, already provided for in US law for the benefit of "national security", which is itself excessively widely defined in US law, and for "protecting law enforcement-sensitive information".[144] Article 16(2) and 20(2) would be a smaller shield to the US legislative authorities which could effectively neutralize the transparency seemingly provided for by the Agreement. The differences between the old and new regime therefore remain: in the US, subject access can be denied when this is "reasonable" to protect law enforcement activities, while in Europe, the denial must be "indispensable" to that end. [145] As such the different between EU and US standard stills prevail.

Even though the Umbrella Agreement set a clear list of exemptions[146] but the exemptions in practice, *de facto*, would bar the possibility for the person to have access to their own data. Even if limited or performed by a trusted third party in situations where access is denied to protect sensitive law enforcement information.[147] In the sense of Article 16(4) it provides for an indirect form of access, but its application is limited only to cases 'permitted under applicable domestic law'. Hence, the practice of US Authorities, especially National Intelligence Agencies, remains the substantial threats to the right of internet users around the world.

---

[143] European Commission. *EU-U.S. Privacy Shield: Frequently Asked Questions.* Press Release Database, Brussels, 29 Feb. 2016, p.4.

[144] Korf, Douwe. "EU-US Umbrella Data Protection Agreement : Detailed Analysis by Douwe Korff." *European Area of Freedom Security & Justice*, 2015, https://free-group.eu/2015/10/14/eu-us-umbrella-data-protection-agreement-detailed-analysis-by-douwe-korff/. Accessed 23 Dec. 2016.

[145] Ibid.

[146] EU-US. *Umbrella Agreement.* 2016, Article 16.2 and 20.2.

[147] European Data protection Supervisor, *Opinion 1/2016.* 12 Feb. 2016, p.10.

4.3.2. Obligation of the Data Controller and Data Processor

These 4 instruments relate to the role of both Private and Public Organizations who may produce effect to the enjoyment of right to personal data protection. By determining the basic obligations to such duty bearers, the instruments contribute critical improvements: design of the up-to-date obligation concerning the information technology in digital era, precise conditions and strong requirements in case of data processing and data retention, firm risk-based assessment measures and definite adequacy criterions for data transfer across border. This section not only surveys the progress but also analyzes the inferiors these instruments may retain.

4.3.2.1. Basic Duty of Data Controller and Processor

The Instruments draw scope on who are the controller and Processor. It becomes clear in the GDPR that all actors are included except the secret service authorities/ intelligence agencies. The implementation of GDPR and EU Directive are extra-territorial, burden of Data Controller and Processor apply beyond the border of EU. Furthermore, the bilateral agreements between EU and US cover the fundamental obligations duty bearer need to give. Nevertheless, these instruments do not apply to Non-EU Nationals even they are living in EU State Members' territory.

EU GDPR

For the first time, GDPR directly regulates data processors. As the old Directive 95/46/EC generally regulates controllers (i.e. those responsible for determining the purposes and means of the processing of personal data) rather than "data processors".

Under GDPR, processors will be required to comply with a number of specific obligations, including to maintaining adequate documentation[148], implement appropriate security standards[149], carry out routine data protection impact assessments[150], appoint a data

[148] EU. *General Data Protection Regulation.* 2016, Article 30.

[149] Ibid, Article 32.

[150] Ibid.

protection officer[151], comply with rules on international data transfers[152] and cooperate with national supervisory authorities[153]. These are in addition to the requirement for controllers to ensure that when appointing a processor, a written data processing agreement is put in place meeting the requirements of GDPR[154]. Repeatedly, these requirements have been enhanced and flourished compared to the equivalent requirements in the Directive 95/46/EC.

Processors will be directly liable to sanctions[155] if they fail to meet these criteria and may also face private claims by individuals for compensation[156].

The Regulation also requires detailed provisions in third-party processing contracts. This will have an impact on both controllers and processors, as they identify their processor agreements, review their commercial and legal positions for future agreements and renegotiate existing agreements. [157]

GDPR introduces a momentous new governance burden for those organizations which are covered by the new requirement to appoint a Data Protection Officer (DPO). Although this is already a requirement for most controllers in some countries under their own domestic data protection laws, it is an entirely new requirement for many organizations and might cost.

Here are the criterion of organizations which must appoint a DPO:[158]

- public authorities
- controllers or processors whose core activities consist of processing operations which by virtue of their nature, scope or purposes require regular and systemic monitoring of data subjects on a large scale
- controllers or processors whose core activities consist of processing sensitive personal data on a large scale.

[151] Ibid, Article 37.

[152] Ibid, Chapter V.

[153] Ibid, Article 31.

[154] Ibid, Article 28.

[155] Ibid, Article 83.

[156] Ibid, Article 79.

[157] Hunton&Williams. *Overview of the EU General Data Protection Regulation.* 2016, p. 2.

[158] EU. *General Data Protection Regulation.* 2016, Article 37.

DPOs must have "expert knowledge"[159] of data protection law and practices though perhaps in recognition of the current shortage of experienced data protection professionals, it is possible to outsource the DPO role to a service provider[160].

Controllers and processors are required to ensure that the DPO is involved "properly and in a timely manner in all issues which relate to the protection of personal data."[161] The role is therefore a sizeable responsibility for bigger controllers and processors.

The DPO must directly report to the highest management level, must not be told what to do in the exercise of their tasks and must not be dismissed or penalized for performing their tasks. [162]

The specific tasks of the DPO are set out in GDPR including: [163]

- to inform and advise on compliance with GDPR and other Union and Member State data protection laws
- to monitor compliance with law and with the internal policies of the organization including assigning responsibilities, awareness raising and training staff
- to advise and monitor data protection impact assessments
- to cooperate and act as point of contact with the supervisory authority

Accountability is a persisting theme of GDPR. Data governance is no longer just a case of doing the good thing; organizations need to be able to verify that they have done the correctness to regulators, to data subjects and probably to shareholders and the media more frequent after a decision was taken.

GDPR requires each controller to demonstrate compliance with the data protection principles.[164] This general principle reveals itself in specific enhanced governance obligations which include: (besides appointment of DPO)

[159] Ibid, Article 37(5).

[160] Ibid, Article 37(6).

[161] Ibid, Article 38(1).

[162] Ibid, Article 38(3).

[163] Ibid, Article 39.

[164] Ibid, Article 5(2).

- ***Keeping a detailed record of processing operations***

  The requirement in current data protection laws to notify the national data protection authority about data processing activities is repealed and supplanted by a more general obligation on the controller to retain extensive internal records of their data protection activities.[165] The level of detail required is far more gigantic compared to many existing Member State notification requirements. There is some relief granted to organizations employing fewer than 250 people though the exemption is very narrowly drafted. [166]

- ***Notifying and keeping a comprehensive record of data breaches***[167]

- ***Implementing data protection by design and by default***

  GDPR introduces the concepts of "data protection by design and by default". "Data protection by design" requires taking data protection risks into account throughout the process of designing a new process, product or service, rather than treating it as an afterthought. This means assessing carefully and implementing appropriate technical and organizational measures and procedures from the outset to ensure that processing complies with GDPR and protects the rights of the data subjects.[168] "Data protection by default" requires ensuring mechanisms are in place within the organization to ensure that, by default, only personal data which are necessary for each specific purpose are processed. This obligation includes ensuring that only the minimum amount of personal data is collected and processed for a specific purpose; the extent of processing is limited to that necessary for each purpose; the data is stored no longer than necessary and access is restricted to that necessary for each purpose. [169]

---

[165] Ibid, Article 30.

[166] DLA Piper. "EU General Data Protection Regulation - Key Changes." www.dlapiper.com/en/uk/focus/eu-data-protection-regulation/key-changes/. Accessed 10 May 2016.

[167] EU. *General Data Protection Regulation*. 2016, Articles 33-4.

[168] Ibid, Article 25.

[169] Hunton&Williams. *Overview of the EU General Data Protection Regulation.* 2016, p. 2.

In GDPR, it destroys the line between "Privacy by Design" and "Privacy by Default" Model and combines it into the comprehensive data protection package for Data Subject in digital era. As priority, GDPR emphasize the advancement of information technology by employing either the Principle of "Data Protection by Design" and the "Data Protection by Default": IT Corporations and State Authorities will be required to implement data protection *by design* (e.g., when creating new products, services or other data processing activities) and *by default* (e.g., by implementing data minimization techniques when collect or process data).[170] They will also be required to perform data protection impact assessments to identify privacy risks in new products launching to E-Market.

EU Directive on Criminal Matters

The Directive will be applied by competent authorities either domestically or when transmitting personal data between EU Member States or transferring personal data to third countries or international organizations. The competent authorities are defined as public authorities or anybody or entity entrusted by Member State law to exercise public authority and public powers. [171] The provisions of the Directive will be applied by public authorities and, under certain circumstances, private bodies.[172] When competent authorities as defined in this Directive are processing personal data not for the purposes of the Directive they must apply the Regulation.

The controller must implement appropriate technical and organizational measures to ensure and be able to demonstrate compliance of their processing. The obligations of the processor such as to only act on instructions from the controller; ensure that the persons authorized to process the data respect confidentiality; make available to the controller all information that show that they are fulfilling their obligations.[173]

The Member States must provide for the controllers to designate a data protection officer. Member States should however be able to exempt courts and other judicial

[170] Ibid.

[171] EU. *Statement of the Council's reasons: Position (EU) No 5/2016 C158/46.* 2016, p.6.

[172] Council of the European Union. *5418/16 ADD 1.* 2016, p.7.

[173] EU. *Statement of the Council's reasons: Position (EU) No 5/2016 C158/46.* 2016, p.6.

authorities when acting in their judicial capacity from this obligation.[174] The purpose of designating a data protection officer is to improve compliance with the Directive.

EU-US Privacy Shield

The Privacy Shield notice requirements are more specific and detailed than what was required by the Safe Harbor regime. Safe Harbor required a privacy policy to provide information on data processing activities and address conformity with the Safe Harbor's privacy principles, but the Privacy Shield imposes a number of specific new additions.[175]

A Privacy Shield company must inform data subject about:[176]

- The types of personal data it processes;
- The reasons why it processes personal data;
- If it intends to transfer personal data on to another company and the reasons why;
- Right to ask the company to access data subject's personal data;
- Right to choose whether you allow a company to use personal data in a "materially different" way or to disclose it to another company (also known as the right to "opt-out"). When the data are sensitive, (that is, data that reveal, for example, ethnic origin or the state of your health) the Privacy Shield company has to inform data subject about the fact that it may only use or disclose such data if you allow this (also known as the right to "opt-in");
- How to contact the company if data subject have a complaint about the use of personal data;
- The independent dispute resolution body, either in the EU or the U.S., where data subject can bring case;

[174] Ibid, p.7.

[175] Wilmer Cutler Pickering Hale and Dorr LLP. "Comparison of Requirements under the Privacy Shield/Safe Harbor Principles", *Lexology*, 25 Jul. 2016, p.2.

[176] EU-US. *Privacy Shield.* 2016, Annex II, III.15.

- The government agency in the U.S. that is responsible to investigate and enforce the company's obligations under the framework;
- The possibility that it may have to respond to lawful requests from U.S. public authorities to disclose information about you.

The Privacy Shield companies must provide data subject with a link to its privacy policy if it has a public website or where data subject can access it in case it does not have a public website. [177] It must also provide data subject with a link to the Privacy Shield List on the Department of Commerce website so that data subject can easily check the Privacy Shield status of the company. [178]

Under certain conditions and taking into account the purpose for which it received your personal data, the Privacy Shield companies may transfer them to another company. This can happen for instance when a company shares data subject's data (with a company that itself decides how to use the data, a so-called "controller") without data subject objecting to that or concludes a service contract with a (sub-) processor (a so-called "agent").[179]

Privacy Shield companies are obliged to provide an independent recourse mechanism to investigate unresolved complaints.[180]

EU-US Umbrella Agreement

The Umbrella Agreement, without any arbitrary or unjustifiable discrimination between its own nationals and those of the other Party, provides safeguards to individuals such as access, rectification and administrative redress. It ensures that European nationals will benefit, in principle,[181] from equal treatment with U.S. citizens when it comes to the practical implementation of these provisions by U.S. authorities. However, the obligation is

[177] European Commission. *Guide to EU-US Privacy Shield.* 2016, p. 9.

[178] Ibid, p. 10.

[179] Ibid, p. 11.

[180] Ibid, p. 12.

[181] EU-US. *Umbrella Agreement.* 2016, Article 4.

not covered by the agreement to Non-EU peoples, living in or traveling via the EU, the parties can collect, share or retain data as many distinctions[182] as they like.

Hence, Individuals are entitled to receive information regarding the purpose of processing and possible further use of their personal data. The person has right to know the laws or rules under which such processing takes place, the identity of third parties and to whom their personal information may be disclosed. As well as the access, rectification and redress mechanisms must be available for data subject.[183] Article 20 of the Umbrella Agreement appears to allow US domestic law to stipulate that any of the matters listed in Article 20(1) shall not be made public, as long as such a restriction on transparency is "reasonable" in US-domestic-legal terms. Given the sweeping exceptions and exemptions from the normal rules, already provided for in US law for the benefit of "national security" – which is itself excessively widely defined in US law – and for "protecting law enforcement-sensitive information" [184].

In simple terms: Article 14 does not in any way ensure accountability of the parties in respect of their compliance, or non-compliance, with the Agreement. There is no solid accountability between the state parties and no accountability towards the general public authority oversight bodies (such as National DPA), State Parliaments or to general public authority.[185]

Organizations have duty to raise the individuals' awareness as to why and by whom their data is processed contribute to the possibility for individuals to exercise their rights to access, rectification or redress.[186]

4.3.2.2. Condition and Requirement of Data Collection and Processing

The main conditions and requirements are mentioned is the principle of accountability and transparency. These instruments set the category of condition and push the

[182] Korf, Douwe. "EU-US Umbrella Data Protection Agreement : Detailed Analysis by Douwe Korff." *European Area of Freedom Security & Justice*, 2015, https://free-group.eu/2015/10/14/eu-us-umbrella-data-protection-agreement-detailed-analysis-by-douwe-korff/. Accessed 23 Dec. 2016.

[183] EU-US. *Umbrella Agreement.* 2016, Article 20.

[184] Korf, Douwe. "EU-US Umbrella Data Protection Agreement : Detailed Analysis by Douwe Korff." *European Area of Freedom Security & Justice*, 2015, https://free-group.eu/2015/10/14/eu-us-umbrella-data-protection-agreement-detailed-analysis-by-douwe-korff/. Accessed 23 Dec. 2016.

[185] Ibid.

[186] EU-US. *Umbrella Agreement.* 2016, Articles 16-19.

duty on controller/processer to acknowledge data subject in various details, different periods and with explicit manner. As GDPR is the most comprehensive legal instrument ever written about data processing, it will be the baseline of Data using conditions and requirements. How did the other three instruments embrace the principle of GDPR to their contents, and in which way, will be the mission of this section. As well as the consistencies and differences among these 4 instruments, conditions and requirements of Data Processing/Collection, will be reviewed.

EU GDPR

Even the core themes of the data protection principles in GDPR remain mainly as they were in the Directive 95/46/EC, though there has been an important boost of the standard for legitimate processing and the new principle of accountability has been put in.

GDPR emphasize that Personal data must be: [187]

- Processed lawfully, fairly and in a transparent manner (the "lawfulness, fairness and transparency principle")
- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (the "purpose limitation principle")
- Adequate, relevant and limited to what is necessary in relation to the purpose(s) (the "data minimization principle")
- Accurate and where necessary kept up to date (the "accuracy principle")
- Kept in a form which permits identification of data subjects for no longer than is necessary for the purpose(s) for which the data are processed (the "storage limitation principle")
- Processed in a manner that ensures appropriate security of the personal data, using appropriate technical and organizational measures (the "integrity and confidentiality principle")

[187] EU. *General Data Protection Regulation.* 2016, Article 5.

The controller is responsible for and must be able to prove compliance with the above principles (the "accountability principle").

The lawfulness, fairness and transparency principle amongst other things demands processing to fall within one or more of the approved legal justifications for processing. Where special categories of sensitive personal data are mentioned, additional much more restrictive legal justifications must also be reached.

Although the structure was present in the Directive 95/46/EC, the changes introduced by GDPR will make it much tougher for organizations to stay within the legal justifications for processing. Failure to comply with this principle is subject to the very highest fines,[188] whichever is the greater.

In particular:

- The bar for valid consents has been raised much higher under GDPR. Consents must be fully unbundled from other terms and conditions and will not be valid unless freely given, specific, informed and unambiguous.[189] Consent also attracts additional baggage for controllers in the form of extra rights for data subjects (the right to be forgotten and the right to data portability) relative to some of the other legal justifications. Consent must be as easy to withdraw consent as it is to give – data subjects have the right to withdraw consent at any time – and unless the controller has another legal justification for processing any processing based on consent alone would need to cease once consent is withdrawn.[190]
- To compound the challenge for controllers, in addition to a hardening of the requirements for valid consent, GDPR has also narrowed the legal justification allowing data controllers to process in their legitimate interests. This justification also appears in the Directive 95/46/EC though the interpretation of the concept in the old regime has varied significantly among the different Member States with some such as the UK and Ireland

[188] EU. *General Data Protection Regulation.* 2016, Article 83(4)(5).

[189] Ibid, Articles 4(11) and 6(1)(a).

[190] DLA Piper. "EU General Data Protection Regulation - Key Changes." www.dlapiper.com/en/uk/focus/eu-data-protection-regulation/key-changes/. Accessed 10 May 2016.

> taking a very broad view of the justification and others such as Germany taking a much more restrictive interpretation. GDPR has followed a more Germanic approach, narrowing the circumstances in which processing will be considered to be necessary for the purposes of the legitimate interests of the controller or a third party. In particular, the ground can no longer be relied upon by public authorities.[191] Where it is depended upon, controllers will need to specify what the lawful interests are in information notices and will need to consider and document why they consider that their lawful interests are not overshadow by the interests or fundamental rights and freedoms of the data subjects, such in Children's right case.

The justification allowing processing necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject to enter into a contract is preserved in GDPR, though continues to be narrowly drafted. Processing which is not necessary to the performance of a contract will not be covered. The less good news for controllers relying on this justification is that it comes with additional burdens under GDPR, including the right to data portability and the right to be forgotten[192] (unless the controller is able to rely on another justification).

Other justifications incorporate where processing is necessary for compliance with a legal duty; where processing is necessary to protect the critical benefits of a data subject or another person where the data subject is ineligible of expressing consent; where processing is necessary for conduct of a task undertake in the public interest in the exercise of official authority empower in the controller. These widely reflect justifications in the Directive 95/46/EC.

It is frequent the case that organizations will want to process data collected for one purpose for a new purpose which was not exposed to the data subject at the time the data was first collected. This is possibly in contra with the essence principle of purpose limitation and to certify that the rights of data subjects are protected, GDPR draws a set of prerequisites

[191] Ibid.

[192] Ibid.

that the controller must ensure whether the new process is compatible with the purposes for which the personal data were primarily collected. These considerations include: [193]

- any link between the original purpose and the new purpose
- the context in which the data have been collected
- the nature of the personal data, in particular whether special categories of data or data relating to criminal convictions are processed (with the inference being that if they are it will be much harder to form the view that a new purpose is compatible)
- the possible consequences of the new processing for the data subjects
- the existence of appropriate safeguards, which may include encryption or pseudonymisation.

If the controller sumps up that the new purpose is incompatible with the initial purpose, then the only groundes to justify the new purpose are a new consent or a legal obligation (more specifically an EU or Member State law which constitutes a necessary and proportionate measure in a democratic society).

As compare to the Directive 95/46/EC, GDPR sets a higher bar to justify the processing of special categories of personal data. These are defined to include "data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation." [194] Processing of these data are prohibited unless one or more specified grounds are met which are broadly similar to the grounds set out in the Directive. Processing of special categories of personal data is only permitted: [195]

- with the explicit consent of the data subject
- where necessary for the purposes of carrying out obligations and exercising rights under employment, social security and social protection law or a collective agreement

[193] EU. *General Data Protection Regulation.* 2016, Article 6(4).

[194] Ibid, Article 9(1).

[195] Ibid, Article 9(2).

- where necessary to protect the vital interests of the data subject or another natural person who is physically or legally incapable of giving consent
- in limited circumstances by certain not-for-profit bodies
- where processing relates to the personal data which are manifestly made public by the data subject
- where processing is necessary for the establishment, exercise or defense of legal claims or where courts are acting in their legal capacity
- where necessary for reasons of substantial public interest on the basis of Union or Member State law, proportionate to the aim pursued and with appropriate safeguards
- where necessary for preventative or occupational medicine, for assessing the working capacity of the employee, medical diagnosis, provision of health or social care or treatment of the management of health or social care systems and services
- where necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of health care and of medical products and devices
- where necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with restrictions set out in Article 89(1)

The requirements and conditions for processing sensitive data is the unique issue where Member States are allowed to introduce domestic laws including greater conditions and restrictions for processing.

GDPR urges the data controller to perform data protection impact assessment for high risk processing.[196] A data protection impact assessment will become a mandatory pre-requisite before processing personal data for processing which is likely to result in a high risk to the rights and freedoms of individuals. Specific examples are set out of high risk processing requiring impact assessments including: automated processing including profiling that produce legal effects or similarly significantly affect individuals; processing of sensitive

[196] Ibid, Article 35.

personal data; and systematic monitoring of publicly accessible areas on a large scale. DPOs, where in place, have to be consulted. Where the impact assessment indicates high risks in the absence of measures to be taken by the controller to mitigate the risk, the supervisory authority must also be consulted[197] and may second guess the measures proposed by the controller and has the power to require the controller to impose different or additional measures.[198]

EU Directive on Criminal Matters

GDPR largely mirrors the requirements of the Directive on Criminal Matters. This data may only be processed under official authority or when authorized by the Union or Member State law[199] which means this is another area where legal requirements and practice is likely to diverge among the different Member States.

Collaboration between the E.U. and Interpol are strengthened by promoting the exchange of personal information, but that exchange is balanced against personal rights regarding the "automatic processing of personal data".

Processing of personal data must be lawful, fair and transparent, and only for the purposes were laid down by law. However, this does not prevent the criminal justice system from carrying out covert investigations or video surveillance for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including keeping the public safe from threats, but always in accordance with the law. [200] This is declared to be necessary and proportionate measure in a democratic society, with due regard for the legitimate interests of the data subjects involved. The right of "fair data processing" [201] is different from the right to a fair trial.

The purposes for which the personal data are processed must be explicit and legitimate and determined at the time of the collection of the personal data. The personal data processed base on adequate and relevant purposes. The collection of personal data must not

[197] Ibid, Article 36.

[198] Ibid, Article 58.

[199] Ibid, Article 10.

[200] Council of the European Union. *5418/16 ADD 1.* 2016, pp. 7-8.

[201] Ibid, p. 7.

be excessive and data must not be kept longer than necessary for the purposes. Personal data could be processed only if the purpose of the processing would not reasonably be fulfilled by other means. [202] Personal data collected must be accurate. Incorrect personal data must not be knowingly shared.

The Directive on Criminal Matters has the different articles on data protection and connected rights compare to GDPR. However, several principles relating to processing of personal data are the same as those enshrined in the GDPR. Because of the peculiarity of the field, while the basic data protection principles are included in its text, some of those set out in the GDPR are not included in the Directive on Criminal Matters. For example, as far as the characteristics the data should have in order to be processed by the competent authorities are concerned, it may be observed that not all the conditions required by the GDPR in order to consider the data processing lawful and fair need to be met. [203] The consent of the data subject, for instance, is not a necessary condition for processing personal data by the competent authorities when they order natural persons to comply with requests made in order to perform the tasks of preventing, investigating, detecting or prosecuting criminal offences.[204]

The regulation of profiling deserves a separate mention, profiling is especially problematic in the police and criminal justice context, because if profiles are misused they can lead to stressful situations for individuals, who could be put under surveillance or arrested on the grounds of automated processing of personal data. The compatibility with the presumption of innocence can be questioned. [205] It is necessary to underline here that in this regard the Directive for data protection in the police and justice sectors provides substantial and procedural safeguards. Member States are prohibited from providing for a decision based solely on automated processing, including profiling, [206] which produces an adverse legal effect concerning the data subject or significantly affects him or her, unless authorized by Union or Member State law to which the controller is subject and which provides appropriate

[202] Ibid, p.8.

[203] Ibid, p.9.

[204] EU. *Directive 2016/680 (Directive on Criminal Matters).* 2016, Recital 35.

[205] Council of the European Union. *5418/16 ADD 1.* 2016, p.6.

[206] Ibid, p.10.

safeguards for the rights and freedoms of the data subject. [207] The Directive also stresses that profiling resulting in discrimination against natural persons shall be prohibited.[208]

EU-US Privacy Shield

In principle, a Privacy Shield company can use data subject's personal data only for the purpose for which it has originally collected your data or which data subjects have subsequently authorized.[209] If it wants to use data subject's data for a different purpose, this depends on how much the original purpose diverges from the new purpose:[210]

- Using personal data for a purpose that is incompatible with the original purpose is never allowed[211];
- If the new purpose is different but related to the original one (i.e. "materially different"), the Privacy Shield company may only use your data if data subject do not object or, in the case of sensitive data, only if data subject consent.[212]
- If the new purpose is different from the original one but still close enough that it would not be considered as materially different, such use is permissible.[213]

The lack of definition of what is to be regarded as a 'materially different' purpose will lead to confusion and legal uncertainty. It should be clarified that in any case, the Choice principle cannot be used to circumvent the Purpose limitation principle.[214] Choice should be applicable only where the purpose is materially different but still compatible since

[207] Maesa, Costanza D F. *Balance Between Security and Fundamental Rights Protection: an Analysis of The Directive 2016/680 for Data Protection in The Police and Justice Sectors and the Directive 2016/681 on the Use of Passenger Name Record (PNR).* 2016, p.8.

[208] EU. *Directive 2016/680 (Directive on Criminal Matters).* 2016, Article 11.

[209] EU-US. *Privacy Shield.* 2016, Annex II, II.5.a.

[210] European Commission. *Guide to EU-US Privacy Shield.* 2016, p.10.

[211] EU-US. *Privacy Shield.* 2016, Annex II, III.14.b.ii.

[212] Ibid, Annex II, III. 9.B.i.

[213] Ibid, Annex II, II.1.b, III.1.a.

[214] Ibid, Annex II, II.2. A concrete example of further incompatible processing authorized under the Choice principle is provided under Supplemental principle 9.b.i.

the processing for incompatible purpose is prohibited.[215] It has to be clarified that the right to opt-out cannot enable the organization to use data for incompatible purposes. Hence, it recommends harmonizing the related wording by using a single and defined wording (e.g. "materially different but nevertheless compatible purpose").

EU-US Umbrella Agreement

The Umbrella Agreement applies the purpose limitation principle to all transfers of personal data covered by the Umbrella Agreement. Processing can take place only for explicit and legitimate purposes within the scope of the Agreement. Further processing of personal information by other (law enforcement, regulatory or administrative) authorities than the first receiving authority of a Party is allowed on condition that it is not incompatible with the purposes for which it was originally transferred. The personal information shall only be processed if "directly relevant to and not excessive or overbroad in relation to the purposes of such processing".[216]

Article 6 is a key provision of the Agreement: it ensures that the application of the safeguards to the entire "life cycle": the right of data subject will be protected in all steps of the extended process. It confirm the protection to the given personal data set from the original transfer from the EU to its processing by a US competent authority and vice-versa, as well as its possible further sharing with/processing by another US authority. In the case of a data transfer from the US to a competent authority of the EU or (one of) its Member States and its possible further sharing with/processing by another EU or Member State authority will be regulated under the Article 6.[217]

Data quality and integrity of information Principle is ensured that transferred personal data is maintained with such accuracy, relevance, timeliness and completeness as is necessary and appropriate for lawful processing of the information. The receiving or

[215] Ibid, Annex II, II.5.a.

[216] EU-US. *Umbrella Agreement.* 2016, Article 6.

[217] European Commission. *Proposal for a COUNCIL DECISION on the signing, on behalf of the European Union, of an Agreement between the United States of America and the European Union on the protection of personal information relating to the prevention, investigation, detection, and prosecution of criminal offenses*. 29 Apr. 2016, p. 8.

transferring authority must give feasible advises to transferring/receiving authority of threats to information integrity.[218]

The processing of sensitive personal may only take place when appropriate safeguards are in place in accordance with law requiring supervisory approval to access the information. Agreements allowing the "bulk transfer" of personal data will have to further specify the standards and conditions under which special categories of data can be processed.[219] The provisions on special categories of data are coherent with the requirement that processing shall be directly relevant and not excessive purpose and use limitations under Article 6.

Data processing that may result in decisions having negative consequences on an individual (*Automated decision-making* e.g. in the context of profiling) may not be based solely on the automated processing of personal information, unless authorized by domestic law, and provided that appropriate safeguards are in place,[220] including the possibility to obtain human intervention. This is especially important in the area of law enforcement, where the consequences of profiling on individuals are potentially more severe. However, the threshold to be met before triggering the applicability of Article 15 is quite high, because it requires the decisions to produce "*significant adverse actions*" in order not to be solely based on automatic processing.[221] While EU law usually prohibits such profiling, it also requires 'appropriate safeguards that include the possibility to obtain human intervention' if the automated decision-making has taken place.

4.3.2.3. Data Security

The 4 instruments especially the Umbrella Agreement and Directive on Criminal Matters, which protect personal data relate to criminal matters, create the stronger protection when it deal with State Authority who may generate more sensitive issues to Data Security. Nonetheless, all of 4 instruments set out the common standard on Risk Assessment

[218] EU-US. *Umbrella Agreement.* 2016, Article 8.

[219] Ibid, Article 13.

[220] Ibid, Article 15.

[221] European Data protection Supervisor. *Opinion 1/2016.* 12 Feb. 2016, p. 14.

Procedure, that urge the data controller/processor to carry out assessment of their filing system and have the monitoring protocol for their system in period of time.

EU GDPR

The prominent change to be introduced by GDPR is a European wide requirement to notify data breaches to supervisory authorities and affected individuals. In the US, data breach notification laws are now in force in 47 States[222] and the hefty penalties for failing to notify have fundamentally changed the way US organizations investigate and respond to data incidents. Not notifying has become a high risk option.

In contrast, Europe currently has no universally applicable law requiring notification of breaches. In the majority of Member States there is either no general obligation to notify or minimal sanctions for failing to do so; for many organizations not notifying and thereby avoiding the often damaging media fall-out is still common practice in Europe. That is set to change fundamentally when GDPR comes into force.

GDPR requires "the controller without undue delay, and where feasible, not later than 72 hours after having become aware of it, [to] notify the … breach to the supervisory authority" [223] When the personal data breach is likely to result in a high risk to the rights and freedoms of individuals the controller is also required to notify the affected individuals "without undue delay"[224]. Processors are required to notify the controller without undue delay having become aware of the breach[225].

The notification to the regulator must include if capable the categories and approximate numbers of individuals and records concerned, the name of the organization's DPO or other contact, the likely consequences of the breach and the measures taken to relieve harm[226].

[222] Look at National Conference of State Legislature Website, www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx. Accessed 12 Jan. 2017.

[223] EU. *General Data Protection Regulation.* 2016, Article 33(1).

[224] Ibid, Article 34.

[225] Ibid, Article 33(2).

[226] Ibid, Article 33(3).

Although the obligation to notify is conditional on awareness, controllers are required to implement appropriate technical and organizational measures together with a process for regularly testing, assessing and evaluating the effectiveness of those measures to ensure the security of processing[227]. Controllers are also required to retain a record of all data breaches[228], whether or not notified to the supervisory authority, and allow monitors by the supervisory authority.

GDPR urge duty bearer to undertake risk-based approach to compliance. The Regulation recognizes a risk-based approach, under which IT Corporations would bear responsibility for assessing the degree of risk that their processing activities lay to data subjects which means Low-Risk processing activities encounter a decreased compliance burden. On the contary, the data protection impact assessments report will be required for high-risk processing activities. These compliance steps will need to be integrated into future product cycles[229] which will launch to the E-Market.

EU Directive on Criminal Matters

Under this Directive, there is an obligation on Data Controller to carry out an impact assessment which is necessary before the controller can carry out a processing where the processing is likely to result in a high risk for the rights and freedoms of natural persons. The Directive sets out the situations in which an impact assessment is compulsory in similar terms as the text of the Regulation. The elements that the impact assessment must contain are however less detailed than in the GDPR.[230] The assessment must contain at least a general description of the processing to be carried out, an assessment of the risks to the rights and freedoms of the data subjects, safeguards, security measures and mechanisms to ensure the protection of personal data[231] and to demonstrate compliance with the provisions of the Directive.

[227] Ibid, Article 32.

[228] Ibid, Article 33(5).

[229] Hunton&Williams. *Overview of the EU General Data Protection Regulation.* 2016, p.2.

[230] EU. *Statement of the Council's reasons: Position (EU) No 5/2016 C158/46.* 2016, p. 6.

[231] Council of the European Union. *5418/16 ADD 1.* 2016, p. 14.

EU-US Privacy Shield

Data security requirements are unchanged under the Privacy Shield Framework. Organizations joining the Privacy Shield Framework must take reasonable and appropriate measures to protect EU personal data from loss, misuse and unauthorized access, disclosure, alteration, and destruction, taking into "due account" the risks[232] involved in the processing and the nature of the personal data.

Thus, The registered company must ensure that any personal data are kept in a safe environment and secured against loss, misuse, unauthorized access, disclosure, alteration or destruction, taking due account of the nature of the data and the risks involved in the processing.[233] The data security risk assessment process may be introduced to routinely supervision.

EU-US Umbrella Agreement

The Article 9 and 10 of Umbrella Agreement contribute to ensuring a high level of security of personal data exchanged by the parties.

The employment of appropriate technical, security and organizational arrangements will be put in place by the Parties for the protection of personal information against accidental or unlawful destruction, accidental loss, and unauthorized disclosure, alteration, access or other processing.[234] Moreover, accession to personal data would be granted only to the authorized staff.

In case of a security incident presenting a significant risk of damage, appropriate action shall be promptly taken to mitigate the damage, including notification to the transferring authority and, where appropriate given the circumstances of the incident, the individual concerned.[235] Exceptions to the notification obligation are exhaustively listed in the provision and correspond to reasonable limitations (public safety, national security). The notification of information security incidents, Article 10(2)(b) allows for the omission of the

[232] Hogan Lovells. *Legal Analysis of the EU-US Privacy Shield.* 2016, p. 24.

[233] European Commission. *Guide to EU-US Privacy Shield.* 2016, p. 11.

[234] EU-US. *Umbrella Agreement.* 2016, Article 9.

[235] Ibid, Article 10.

notification of a data breach where the notification "*may endanger national security*",[236] with a vague effect on the ground of a possible consequence, '*may*', on national security is unclear. The necessity of omitting the notification altogether, and not merely delaying it or restricting for security reasons the quality of recipients entitled to receive the information. Moreover, specific conditions for delaying notifications to the transferring Competent Authority are not referred to in the text. [237]

4.3.2.4. Data Retention

Although all 4 instruments contain the set of provision relate to Data Retention, There are 2 specific instruments adopted to fix the problem of CJEU verdict that invalidate old EU Data Retention Directive. Not only the new EU Data Retention Directive but also the EU-US Umbrella agreement set up a better oversight system and bring in a Check and Balance Principle to data retention in criminal and security realm. All 4 instruments give rights to data subject to access, rectify, noticed and appeal to such data controllers/processors who detain their personal data for particular purpose.

EU GDPR

GDPR largely reflects the requirements of the Directive on Criminal Matters. This data may only be processed under official authority or when authorized by Union or Member State law[238] which means this is another area where legal requirements and practice is likely to diverge among the different Member States.

Under GDPR, processors will be required to comply with a number of specific obligations, including to maintaining adequate documentation[239], comply with rules on international data transfers[240] and cooperate with national supervisory authorities[241]. These

[236] European Data protection Supervisor. *Opinion 1/2016.* 12 Feb. 2016, p.12.

[237] Ibid.

[238] EU. *General Data Protection Regulation.* 2016, Article 10.

[239] Ibid, Article 30.

[240] Ibid, Chapter V.

[241] Ibid, Article 31.

requirements have been supplemented and crystallized due to the data retention requirements in the 2016 Directive on criminal matters.

This general principle manifests itself in specific enhanced governance obligation to keeping a detailed record of processing operations.[242] The requirement in the old data protection laws, to notify the national data protection authority about data processing operations, is eradicated and repealed by a more general obligation on the controller to keep comprehensive internal records of their data protection practices.

EU Directive on Criminal Matters

Public authorities (e.g., taxing authorities) that collect personal information are not to have their databases of personal information interlinked with those of the criminal justice system. Instead, requests for information should follow existing requirements of being in writing, authorized, and ad hoc.

Criminal justice authorities may collect data that extends beyond the amount required for the direct purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, [243] if they need to do so in order to understand the criminal activities or make links between criminal offences.

Data collected about persons for the purposes of the administration of criminal justice should distinguish between who is a subject, who is accused, who is convicted, who is a victim, who is a witness, etc.

There are obligations to the controller to provide a sufficient amount of information to fulfill the purpose of the records. It is for example compulsory for the controller to add information about categories of recipients to whom the personal data have been or will be disclosed, the categories of transfers of personal data to a third country or an international organization or where possible the envisaged time limits for erasure of the different categories of personal data.[244] The controller must also provide information about profiling, which is not the case in the GDPR.

[242] Ibid, Article 30.

[243] Council of the European Union. *5418/16 ADD 1.* 2016, p. 13.

[244] EU. *Statement of the Council's reasons: Position (EU) No 5/2016 C158/46.* 2016, p. 6.

It is important to keep logs for making it possible to establish the justification, date and time of certain processing operations in automated processing systems, such as collection, consultation, disclosure and transfers. Logs of consultation and disclosure also allow to identifying the person who has consulted or disclosed personal data as well as the identity of the recipient. A new element in the Directive on Criminal Matters is that the logs can also be used for criminal proceedings. [245] However, bringing automated processing systems into conformity is a very significance, lengthy and costly process. A supplementary extension for bringing automated processing systems into conformity is foreseen in exceptional cases for a particular automated processing system set up before the entry into force of the Directive[246] if this would otherwise cause serious difficulties for the operation of that particular automated processing system.

EU-US Privacy Shield

The Privacy Shield includes more detail on compatible purposes and includes new language on data retention limit: "Information may be retained in a form identifying or making identifiable the individual only for as long as it serves a purpose [consistent with the purpose limitation principle]."[247] The new framework explicitly states that, even if an organization terminates its certification in Privacy Shield, the organization remains bound by the Privacy Shield principles with respect to any personal data it retains that was collected under the Privacy Shield. Organizations must continue to affirm their commitment to apply the principles to any retained data. [248]

The Privacy Shield companies may only receive and process personal data to the extent they are relevant for the purpose of processing, and they have to ensure that the data used is accurate, reliable, complete and up to date. It is only allowed to keep data subject's personal data for as long as necessary for the purpose of processing. Companies may keep personal data for longer periods only if they need them for certain specified purposes such as archiving in the public interest, journalism, literature and art, scientific or

[245] Ibid, p. 6.

[246] Council of the European Union. *5418/16 ADD 1.* 2016, p.13.

[247] Wilmer Cutler Pickering Hale and Dorr LLP. "Comparison of Requirements under the Privacy Shield/Safe Harbor Principles." *Lexology*, 25 Jul. 2016, p. 5.

[248] Ibid, p. 6.

historical research, or for statistical analysis.[249] If personal data continue to be processed for these purposes, the company must of course comply with the Privacy Principles.

Monitoring and oversight[250]

The new arrangement will be transparent and contain effective supervision mechanisms to ensure that companies follow the rules they submitted themselves to. The US has committed to stronger oversight by the Department of Commerce as well as stronger cooperation between European Data Protection Authorities and the Federal Trade Commission. This will transform the system from a self-regulating one into an oversight system that is more responsive as well as proactive.

However, the lack of provisions imposing a limit on the retention of data under the Privacy Shield gives organizations the possibility to keep data as long as they wish, even after leaving the Privacy Shield, which is not in line with the essential data retention limitation principle.[251]

EU-US Umbrella Agreement

The Parties shall have in place effective methods (such as logs) for demonstrating the lawfulness of processing and use of personal information. This requirement represents a significant safeguard for individuals, as it puts the onus on law enforcement authorities to demonstrate that a given data processing operation was carried out in accordance with the law. The obligation to document data processing operations entails, in particular, that there will be a "trace" in case of unlawful processing.[252] This should facilitate the handling of complaints and the introduction of claims regarding the lawfulness of the processing operations.

Under the Umbrella Agreement, the processing of data will be subject to specific retention periods in order to ensure that data will not be retained for longer than

[249] European Commission. *Guide to EU-US Privacy Shield.* 2016, p. 10.

[250] European Commission. *EU-U.S. Privacy Shield: Frequently Asked Questions*. Press Release Database, Brussels, 29 Feb. 2016, p. 4.

[251] Article 29 Data Protection Working Party. *Opinion 01/2016 on the EU – U.S. Privacy Shield draft adequacy decision.* 13 Apr. 2016, p. 17.

[252] EU-US. *Umbrella Agreement.* 2016, Article 11.

necessary and appropriate. To determine the duration of these retention periods, a number of elements will have to be taken into account, in particular the purpose of processing or use, the nature of the data and the impact on the rights and interests of the data subjects concerned.[253] It is also specified that, where the Parties conclude an agreement on the transfer of "bulk data", such agreement must contain a specific provision on the applicable retention period.[254] With this provision, the Parties accept the principle that such bulk transfer agreements shall contain a specific retention period, which therefore will not have to be negotiated again and again, taking into account the principles of proportionality and necessity.

The retention periods will be subject to periodic reviews to determine whether changed circumstances require any modification of the applicable period. To ensure transparency, retention periods will have to be made publicly available or otherwise published.

4.3.2.5. Data Transfer

These 4 instruments are adopted on the fundamental data transfer Principle, Adequacy criterions of protection. Attempting to create a single E-Market, these instruments especially EU-US bilateral Agreements try to construct a Bloc of protection, with the same standard level, across Atlantic. However, there is a convenience from the US side since the duty does not automatically oblige to all IT corporations. Only the Privacy Shield registered company are abiding themselves to the EU standard in order to access EU E-Market. On the other hand, all EU entrepreneurs are bided to follow the standard in Mid-2018 due to the direct effect of GDPR and further Directive on Criminal Matters implementation in EU Member States. The adaptation path to common regime of EU-US E-Market will be elucidated in this section as it will displays possible options to reach the adequacy principle.

[253] Ibid, Article 12.

[254] European Commission. *Proposal for a COUNCIL DECISION on the signing, on behalf of the European Union, of an Agreement between the United States of America and the European Union on the protection of personal information relating to the prevention, investigation, detection, and prosecution of criminal offenses.* 29 Apr. 2016, p. 9.

EU GDPR

International transfers and particularly those to the US have regularly made front page headline news over the last 12 months with the successful torpedoing of the EU/US Safe Harbor regime by Europe's highest court. Data Controller/Processor duty to Adequacy principle, Most of GDPR part will not make any material changes to the current rules for transfers of personal data cross-border, largely it will reflect the same regime under the Directive 95/46/EC. On the contrary to the old regime where sanctions for breaching transfer restrictions are small, failure to comply with GDPR's transfer requirements attract the highest category of fines.

Transfers of personal data to third countries outside the EU are only permitted where the conditions laid down in GDPR are met.[255]

Transfers to third countries, territories or specified sectors or an international organization which the Commission has decided ensures an adequate level of protection do not require any specific authorization.[256] The adequacy decisions made under the Directive 95/46/EC shall remain in force under GDPR until amended or repealed[257]; so before 25th May 2018 transfers to some countries, accession to the old Directive 95/46/EC, are permitted.

Transfers are also permitted where adequate safeguards have been given by the controller or processor and on condition that enforceable data subject rights and effective legal remedies for the data subject are available. There are possible ways to transfer data from EU such as the list of adequate safeguards, binding corporate rules (BCR), which now enjoyable under GDPR and standard contractual clauses.[258] Again, decisions on adequacy made under the Directive 95/46/EC will generally be valid under GDPR until amended, replaced or repealed.

GDPR Binding Corporate Rules ("BCRs"), BCRs are binding data protection corporate policies and programmes that are used to lawfully transfer personal data globally within a group of companies. The GDPR formally recognizes BCRs. They will still require

[255] EU. *General Data Protection Regulation.* 2016, Article 44.

[256] Ibid, Article 45(1).

[257] Ibid, Article 45(9).

[258] Ibid, Article 47.

SA approval, but the approval process should become *less onerous than the current system*. BCRs are available to both *controllers and processors*.[259]

Two new mechanics are introduced by GDPR to justify international transfers: controllers or processors may also depend on a verified code of conduct pursuant to Article 40 or an approved certification mechanism pursuant to Article 42 together in each case with binding and enforceable commitments in the third country to apply these safeguards including as concerns data subjects' rights. GDPR also discards the need to notify and in some Member States pursue prior approval of model clauses from supervisory authorities. [260]

GDPR includes a list of derogations similar to those included in the Directive permitting transfers where: [261]

> (a) explicit informed consent has been obtained
>
> (b) the transfer is necessary for the performance of a contract or the implementation of pre-contractual measures
>
> (c) the transfer is necessary for the conclusion or performance of a contract concluded in the interests of the data subject between the controller and another natural or legal person
>
> (d) the transfer is necessary for important reasons of public interest
> (e) the transfer is necessary for the establishment, exercise or defense of legal claims
>
> (f) the transfer is necessary in order to protect the vital interests of the data subject where consent cannot be obtained
>
> (g) the transfer is made from a register which according to EU or Member State law is intended to provide information to the public, subject to certain conditions.

There is a very limited derogation to transfer when no other mechanic is available and the transfer is necessary for the purposes of compelling lawful benefits of the

[259] Hunton&Williams. *Overview of the EU General Data Protection Regulation.* 2016, p. 3.

[260] EU. *General Data Protection Regulation.* 2016, Article 46(2)(e) and (f).

[261] Ibid, Article 49.

controller which are not overcome by the interests and rights of the data subject; notification to the supervisory authority is required if basing on this derogation.

Transfers given precedents by courts, tribunals or administrative authorities of countries outside the EU are only recognized or enforceable (within the EU) where they are based on an international agreement such as a mutual legal assistance treaty in force between the requesting third country and the EU or Member State; otherwise transfer in response to such requests, where there is no other legal basis for transfer, may violate GDPR's restrictions. [262]

EU Directive on Criminal Matters

With regard to the transfer of personal data to third countries or international organizations the Directive for data protection in the police and justice sectors requires that personal information be allowed to be transmitted by an EU Member State to a third country only if the Commission has decided that the recipient ensures an "adequate" level of protection. The concept of adequate level of protection has been defined by the Court of Justice in the *Schrems case* as requiring the third country in fact to ensure, by reason of its domestic law or its international commitments, a level of protection of fundamental rights and freedoms that is essentially equivalent to that guaranteed within the European Union.

Therefore, here again the Directive for data protection in the police and justice sectors had to maintain a careful balance between, on the one hand, the requirements of police and criminal justice work and existing bilateral agreements and, on the other, the requirement for an increased level of personal data protection. The Directive for data protection in the police and justice sectors does little to affect bilateral agreements already in place. Admittedly this wording automatically turns all bilateral agreements into definite term ones, in need of amendment to match the Directive's standards immediately when the first opportunity arises.[263] However, if Member States – that are called upon, but not obliged to actively seek to amend bilateral agreements in the foreseeable future – do not take action, the prolonged existence of those bilateral agreements which apply lower standards than the

[262] EU. *General Data Protection Regulation.* 2016, Article 48.

[263] Council of the European Union. *5418/16 ADD 1.* 2016, p. 14.

Directive for data protection in the police and justice sectors could undermine the whole international data transfer edifice.[264]

The general principles lay down the choices for the controllers to transfer personal data, in descending order of preference, starting with the adequacy decisions. In the articles on transfers by way of appropriate safeguards and derogations for specific situations, such transfers must be documented and that the documentation must be made available to the supervisory authority[265] as well as the elements that the documentation must contain.

The personal data can be transferred only if the controller in the third country or international organization is an authority competent for the purposes in Article 1(1) of the draft Directive. Therefore allows the above-mentioned competent authorities, in individual and specific cases, and as long as the other provisions of the Directive are complied with and that a number of exhaustively listed conditions are fulfilled, to transfer personal data directly to recipients because international agreements do not always allow for the swift reply that may be required. [266] These conditions include that the transfer is strictly necessary for the performance of a task of the transferring competent authority as provided for by Union or Member State law for the purposes set out in Article 1(1), the transferring competent authority considers that the transfer to an authority that is competent for the purposes referred to in Article 1(1) in the third country is ineffective or inappropriate, in particular because the transfer cannot be achieved in good time and that the transferring authority informs the recipient of the specified purpose or purposes for which the personal data must be processed.[267] Like for the transfers on the basis of safeguards and on the basis of derogations of specific situations, an obligation of documentation of the transfer has been added. Such transfers could be particularly useful where there is an urgent need to transfer personal data to save the life of a person who is in danger of attacking,[268] a victim of a criminal offence or in the interest of preventing an imminent perpetration of a crime, including terrorism.

[264] Maesa, Costanza D F. *Balance Between Security and Fundamental Rights Protection: an Analysis of The Directive 2016/680 for Data Protection in The Police and Justice Sectors and the Directive 2016/681 on the Use of Passenger Name Record (PNR).* 2016, p. 7.

[265] Council of the European Union. *5418/16 ADD 1.* 2016, p. 14.

[266] Ibid, p. 15.

[267] EU. *Statement of the Council's reasons: Position (EU) No 5/2016 C158/46.* 2016, p. 7.

[268] Council of the European Union. *5418/16 ADD 1.* 2016, p. 15.

EU-US Privacy Shield

The well-publicized gap for transfers from the EU to US following the ruling that Safe Harbor is invalid then will be filled with the new EU-US Privacy Shield. To transfer personal data from the EU to the U.S. different tools are available such as contractual clauses, binding corporate rules and the Privacy Shield. If the Privacy Shield is used, U.S. companies must first sign up to this framework with the U.S. Department of Commerce. The obligation applying to companies under the Privacy Shield are contained in the "Privacy Principles".[269] In order to be able to certify, companies must have a privacy policy in line with the Privacy Principles. They must renew their "membership" to the Privacy Shield on an annual basis. If they do not, they can no longer receive and use personal data from the EU under that framework. The Privacy Shield List on the website of the Department of Commerce. This list gives details of all the companies taking part in the Privacy Shield, the kind of personal data they use, and the kind of services they offer. Data subject can also find a list of companies that are no longer part of the Privacy Shield. This means they are no longer allowed to receive data subject's personal data under the Privacy Shield.[270] Also, these companies may only keep personal data if they commit to the Department of Commerce that they will continue to apply the Privacy Principles.

The Privacy Shield imposes new requirements (and liability for) onward transfers of data to third parties. [271] The Privacy Shield provides for a right to opt-out to disclosure of personal information to a third party or to the use of personal information for a purpose materially different[272]. In addition, individuals benefit from an 'opt-out' right to the use of personal information for direct marketing purpose at any time[273].

Data subject also have a right to choose whether data subject allow a Privacy Shield company to pass on your personal data to another company, whether in the U.S. or in

[269] "Welcome to The Privacy Shield." *Privacy Shield.* www.privacyshield.gov/welcome. Accessed 11 May 2016.

[270] European Commission. *Guide to EU-US Privacy Shield.* 2016, p. 8.

[271] Wilmer Cutler Pickering Hale and Dorr LLP. "Comparison of Requirements under the Privacy Shield/Safe Harbor Principles." *Lexology*, 25 Jul. 2016, p. 4.

[272] EU-US. *Privacy Shield.* 2016, Annex II, III, 2. The Supplemental Principle 14.c.I provides for the right to withdraw from a Clinical trial, which might be seen as the right to object or to withdraw consent.

[273] Ibid, Annex II, III.12.a. This is identical as what was provided in the Safe Harbor scheme and not changed has been made as this regard.

another non-EU country.[274] While data subject's do not have such a choice when your data will be sent to another company (also known as an "agent") for processing on behalf, in the name and under the instructions of the Privacy Shield company, [275] the Privacy Shield company will have to sign a contract with the agent that obliges the latter to provide the same data protection safeguards as contained in the Privacy Shield framework.[276] And the Privacy Shield companies can be held liable for its agent's actions if the agent does not respect the rules.

Irrespective of its location, within or outside the U.S., the company that receives the data must ensure the same level of protection of your personal data as guaranteed under the Privacy Shield framework. This requires a contract between the Privacy Shield organization and the third party setting out the conditions under which the third party can use your personal data and its responsibilities to protect your data.[277] This contract will have to require the third party to inform the Privacy Shield company of situations where it cannot continue to meet its obligations, in which case it must stop using the data. Stricter rules apply where a third party is acting as an agent on behalf of a Privacy Shield company.[278]

Accordingly, the duty to put in place contracts to ensure that a third party Controller will provide at least the same level of privacy protection as is required by the Privacy Shield principles.[279] The purpose is to ensure that personal data continue to be protected adequately,[280] even after having been transferred onward.

The controller and agent must sign contract which has the same rules as GDPR Binding Corporate Rules ("BCRs").[281] Hereafter, the Privacy Shield organizations could be held liable for the sanctions of an agent that do not follow its obligations to protect personal data of data subject.[282]

---

[274] Ibid, Annex II, II.3.a.i; II.3.a.iii; II.3.a.iv; II.3.a.v; II.7.d.

[275] Ibid, Annex II, II.7.d.

[276] European Commission. *Guide to EU-US Privacy Shield.* 2016, p. 10.

[277] EU-US. *Privacy Shield.* 2016, Annex II, II.3.a.

[278] European Commission. *Guide to EU-US Privacy Shield.* 2016, p.11.

[279] EU-US. *Privacy Shield.* 2016, Annex II, II.3.a.

[280] Ibid, Annex II, II.5.

[281] Ibid, Annex II, III.10.b.

[282] Ibid, Annex II, III.10.a.ii.

However, guarantee will not apply in case an organization has chosen to cooperate with a DPA.[283]

EU-US Umbrella Agreement

The onward transfer limitations in Umbrella Agreement entail that in case a U.S. authority intends to further transfer data it has received from the EU or one of its Member States to a third country/international organization not bound by the agreement,[284] it will first have to obtain the consent from the law enforcement authority in the EU which has originally transferred the data to the United States. This rule equally applies in case an authority of the EU or one of its Member States intends to further transfer data it has received from the U.S. to a third country/international organization.

When deciding to grant its consent, the original transferring authority will have to take into due account all relevant factors, including the purpose for which the data was initially transferred and whether the third country or international organization offers an appropriate level of protection of personal information.[285] It may also subject the transfer to specific conditions.

Furthermore, as for the articles on purpose limitation[286], retention periods[287] and sensitive data[288], this Article expressly takes into account the special sensitivity of the transfer in bulk of data of unsuspected persons (e.g. PNR data of every passenger taking a flight, independently of any specific suspicion), in that it requires that any further transfer of personal information "other than in relation to specific cases"[289] may only take place under

[283] Ibid, Annex II, III.5.a in fine.

[284] Ibid, Article 7.

[285] European Commission. *Proposal for a COUNCIL DECISION on the signing, on behalf of the European Union, of an Agreement between the United States of America and the European Union on the protection of personal information relating to the prevention, investigation, detection, and prosecution of criminal offenses.* 29 Apr. 2016, p. 8.

[286] EU-US. *Umbrella Agreement.* 2016, Article 6.

[287] Ibid, Article 12.

[288] Ibid, Article 13.

[289] European Commission. *Proposal for a COUNCIL DECISION on the signing, on behalf of the European Union, of an Agreement between the United States of America and the European Union on the protection of*

specific conditions set forth in the agreement that provide due justification for the onward transfer.

The specific situation of onward transfers to another State within the EU (e.g. the French police sharing with the German police information received from the U.S. FBI) is also addressed in this Article[290] by providing that if under applicable rules such transfers are subject to prior consent, the authority which has originally sent the information (e.g. the U.S. FBI) will not be able to refuse consent or impose conditions on data protection grounds[291] (all the criminal matters authorities involved are bound by the Umbrella Agreement).

4.3.3. Implementation of Personal Data Protection

The most controversial issue in the negotiations among EU Member states and between EU and US to adopt these instruments is the implementation measures. As the old regime leave the implementation measure with domestic judicial system or National Data protection Authority, it depends on various domestic data protection laws. The value-added of new regime will be exhibited in three areas; monitoring, redress and enforcement. However, the obstacles to full enjoyment of right to personal data protection that come from the imperfections of EU-US regime will be mentioned too.

4.3.3.1. Monitoring Body and Supervisory Authority

EU GDPR provides One-stop shop for EU citizen to recourse their right in single channel but the solid mechanism has not been concluded yet. Old Directive 95/46/EC leaves each member state to set up the oversight/monitor system relate to the diversified of criminal procedure of each state. EU-US Privacy Shield use a regime of Self-Regulate which mean the registered must contain themselves in line otherwise they may be disapproved when

---

personal information relating to the prevention, investigation, detection, and prosecution of criminal offenses. 29 Apr. 2016, p. 8.

[290] EU-US. *Umbrella Agreement.* 2016, Article 7 para.3.

[291] European Commission. *Proposal for a COUNCIL DECISION on the signing, on behalf of the European Union, of an Agreement between the United States of America and the European Union on the protection of personal information relating to the prevention, investigation, detection, and prosecution of criminal offenses.* 29 Apr. 2016, p. 8.

the case is raise to Federal Trade Commission. EU-US Umbrella Agreement adopted a joint-committee to periodically oversight the data controller/processor.

EU GDPR

The long for a one-stop-shop ensuring that controllers present in multiple Member States would only have to answer to their lead home regulator failed to make it into the final draft. GDPR includes a complex, bureaucratic procedure allowing multiple 'concerned' authorities to input into the decision making process. Currently, a Data Protection Authority ("**DPA**") may exercise authority over businesses established in its territory or otherwise falling within its jurisdiction.[292] Under the Regulation, where a business is established in more than one EU Member State, the supervisory authority ("**SA**") of the main establishment of the business will act as the lead authority for data processing activities that have an impact throughout the EU and will co-ordinate its work with other SAs. In addition, each SA will have jurisdiction over complaints and possible violations of the Regulation in their own Member State.[293]

The starting point for enforcement of GDPR is that controllers and processors are regulated by and answer to the supervisory authority for their main or single establishment, the so-called "lead supervisory authority".[294]

Nonetheless, the lead supervisory authority is required to coordinate with all other "concerned" authorities and there are powers for a supervisory authority in another Member State to enforce where violation occur on its territory or essentially affects data subjects only in its territory.[295]

In circumstances where many supervisory authorities are involved in an investigation or enforcement process there must be a cooperation procedure[296] involving a

[292] DLA Piper. "EU General Data Protection Regulation - Key Changes." www.dlapiper.com/en/uk/focus/eu-data-protection-regulation/key-changes/. Accessed 10 May 2016.

[293] Hunton&Williams. *Overview of the EU General Data Protection Regulation.* 2016, p. 2.

[294] EU. *General Data Protection Regulation.* 2016, Article 56(1).

[295] Ibid, Article 56(2).

[296] Ibid, Article 60.

lengthy decision making process and a right to refer to the consistency mechanism[297] if a decision cannot be pursued, ultimately with the European Data Protection Board having the mandate to make a binding decision.

GDPR supply the Broad investigative and corrective powers. Supervisory authorities also enjoy wide investigative and corrective powers[298]including the power to undertake in-field data protection monitors and the power to issue public warnings, reprimands and orders to carry out specific reparation activities.

There is an urgency procedure for exceptional circumstances in GDPR, which allows a supervisory authority to adopt provisional measures on an interim basis where necessary to protect the rights and freedoms of data subjects. [299]

EU Directive on Criminal Matters

There is requirement to establishment of an independent supervisory authority entrusted with the task of monitoring the application of data protection law within the respective EU Member State. The Directive for data protection in the police and justice sectors permits assignment of this role to the authority established for similar purposes under the Data Protection Regulation. Data Protection Authorities, as independent supervisory authorities, have been already introduced by Directive 95/46 and have become the basic mechanism for enforcement and monitoring of data protection in the EU today. An ostensibly significant change brought by the EU data protection reform package to the EU data protection systems concerns the replacement of the old Article 29 Data Protection Working Party by the European Data Protection Board. The Board will replace the Article 29 Working Party but, as far as the Directive for data protection in the police and justice sectors is concerned, only apparently since it will essentially retain the same powers as. In this respect it should be noted that, while in the Data Protection Regulation the EU legislator assigned a

[297] Ibid, Articles 63-5.

[298] Ibid, Article 58.

[299] Ibid, Article 66.

central role to the Board, especially in the consistency mechanism,[300] no such role is provided for in the Directive for data protection in the police and justice sectors.

However, in the police and criminal justice context conflicts pertaining to processing of personal data may arise between the Data Protection Authority and the judicial authorities in order to determine if Data Protection Authority may monitor processing done by judicial authorities. The Directive for data protection in the police and justice sectors, in order to limit the discretionary power of the Member States, provides that the processing of data by judicial authorities must not be affected by its provisions when acting within their judicial capacity.[301] In spite of that it should be noted that Article 1 permits Member States to maintain a higher level of data protection which could ultimately be a cause of problems.

The monitoring of the Directive as well as the Regulation will be carried out by supervisory authorities. The rules on the supervisory authorities in the Directive are to a large extent taken over from the text of the Regulation. Member States are allowed to provide for the supervisory authorities established in the Regulation to be supervising the Directive as well.[302] The Directive however excludes the supervision by the supervisory authorities as defined in the Directive of processing operations of courts when they act in their judicial capacity. [303] Member States should be able to exclude the supervision by supervisory authorities as defined in the Directive of processing operations of other independent judicial authorities when they act in their judicial capacity.

The supervisory authorities powers should have in each Member State the same tasks and effective powers to allow them to carry out the tasks of effective, reliable and consistent monitoring of compliance with and enforcement of the Directive throughout the Union.[304] The powers of the supervisory authority, that have to be set out bylaw, in three different categories, namely effective investigative, corrective and advisory powers as well as the power to bring

---

[300] Maesa, Costanza D F. *Balance Between Security and Fundamental Rights Protection: an Analysis of The Directive 2016/680 for Data Protection in The Police and Justice Sectors and the Directive 2016/681 on the Use of Passenger Name Record (PNR).* 2016, pp. 6-7.

[301] Maesa, Costanza D F. *Balance Between Security and Fundamental Rights Protection: an Analysis of The Directive 2016/680 for Data Protection in The Police and Justice Sectors and the Directive 2016/681 on the Use of Passenger Name Record (PNR).* 2016, p. 7.

[302] Council of the European Union. *5418/16 ADD 1.* 2016, p. 16.

[303] EU. *Statement of the Council's reasons: Position (EU) No 5/2016 C158/46.* 2016, p. 7.

[304] Council of the European Union. *5418/16 ADD 1.* 2016, p. 16.

infringements of the provisions adopted pursuant to the Directive[305] to the attention of judicial authorities.

EU-US Privacy Shield

A Data Protection Authority is established in each EU Member State and is responsible for protecting and enforcing the data protection rules at national level.[306]

There is Monitoring and oversight[307] system, the new arrangement will be transparent and contain effective supervision mechanisms to ensure that companies follow the rules they submitted themselves to. The US has committed to stronger oversight by the Department of Commerce as well as stronger cooperation between European Data Protection Authorities and the US Federal Trade Commission.[308] This will transform the system from a self-regulating one into an oversight system that is more responsive as well as proactive.

The US Federal Trade Commission (FTC) and US Department of Commerce (DOC) will monitor and actively verify that companies' privacy policies are in line with the relevant Privacy Shield principle and readily available to the public. US companies will register to be on the Privacy Shield list and self-certify that they meet the high data protection standards set out by the arrangement.[309] They will have to renew their registration every year.

US companies have to commit to comply with advice by the competent EU Data Protection Authority (DPA), while other companies may voluntarily make such a commitment.[310] The Commission encourages companies to do so. EU citizen may take their complaint to DPA in their own 'home'**:** The DPA in each EU member state will refer the complaint to the US Department of Commerce, who will respond within 90 days, or the

[305] EU. *Statement of the Council's reasons: Position (EU) No 5/2016 C158/46.* 2016, p. 8.

[306] European Commission. *Guide to EU-US Privacy Shield.* 2016, p. 12.

[307] European Commission. *EU-U.S. Privacy Shield: Frequently Asked Questions.* Press Release Database, Brussels, 29 Feb. 2016, p. 4.

[308] EU-US. *Privacy Shield.* 2016, Annex II, III.7.e.

[309] European Commission. *EU-U.S. Privacy Shield: Frequently Asked Questions.* Press Release Database, Brussels, 29 Feb. 2016, p. 2.

[310] EU-US. *Privacy Shield.* 2016, Annex II, III.5.a.

Federal Trade Commission,[311] if the Department of Commerce is unable to resolve the matter.

The Privacy Shield sets up a new independent redress mechanism in the area of national security: the Ombudsperson Mechanism. The Privacy Shield Ombudsperson is a senior official within the U.S. Department of State who is independent from U.S. intelligence agencies. Assisted by a number of staff, the Ombudsperson will ensure that complaints are properly investigated and addressed in a timely manner, and that you receive confirmation that the relevant U.S. laws have been complied with or, if the laws have been violated, the situation has been remedied. [312] In carrying out its duties, and following up on the complaints received, the Ombudsperson will work closely with and obtain all the information from other independent oversight and investigatory bodies necessary for its response when it concerns the compatibility of surveillance with U.S. law. These bodies are the ones responsible to oversee the various U.S. intelligence agencies. This mechanism is not Privacy Shield specific. It covers all complaints relating to all personal data and all types of commercial transfers from the EU to companies in the U.S.,[313] including data transferred on the basis of alternative transfer tools such as standard contractual clauses or binding corporate rules (BCR).

The Ombudsperson will process data subject's request and, if it has any questions or if requires more information, it will contact the referring body. Once the Ombudsperson has determined that your request is complete, it will pass it on to the appropriate U.S. bodies. When the request relates to the compatibility of surveillance with U.S. law, it will be able to cooperate with one of the independent oversight bodies with investigatory powers. The Ombudsperson will have to receive the necessary information to be able to provide a response. It will confirm that your request has been properly investigated and that U.S. law has been complied with or, if not, that any violation of U.S. law has been remedied.[314] The response will not state whether you have been the target of surveillance by U.S. national intelligence services.

---

[311] European Commission. *EU-U.S. Privacy Shield: Frequently Asked Questions.* Press Release Database, Brussels, 29 Feb. 2016, p. 3.

[312] European Commission. *Guide to EU-US Privacy Shield.* 2016, p. 19.

[313] Ibid.

[314] Ibid.

There is Regular review of adequacy decisions The EU and the US have now agreed to establish a new mechanism to monitor the functioning of the Privacy Shield through an annual joint review. The European Commission and the US Department of Commerce will carry out this review, which will serve to substantiate the commitments made. [315] The joint review would involve, as appropriate, representatives of the US intelligence community and will provide a dynamic and ongoing process to ensure that the Privacy Shield is functioning in accordance with the principles and commitments made.

EU-US Umbrella Agreement

In terms of transparency and oversight, the Umbrella Agreement falls significantly short of fundamental European data protection and human rights requirements.[316]

The is the requirement under Article 21(1)(a) that oversight authorities must *"exercise independent oversight functions and powers"*. However, also in the light of the current debate regarding the effective powers to enforce data protection and privacy law of some of the US oversight authorities[317] enumerated in Article 21(3), we consider as essential that a bilateral explanatory declaration to the Agreement is signed by the parties to specifically list: [318]

- the supervisory authorities that have competence in this matter and the mechanism for the Parties to inform each other about future changes;
- the effective powers they may exercise;
- the identity and coordinates of the contact point which will assist with the identification of the competent oversight body (see Article 22(2)).

[315] European Commission. *EU-U.S. Privacy Shield: Frequently Asked Questions.* Press Release Database, Brussels, 29 Feb. 2016, p. 4.

[316] Korf, Douwe. "EU-US Umbrella Data Protection Agreement : Detailed Analysis by Douwe Korff." *European Area of Freedom Security & Justice*, 2015, https://free-group.eu/2015/10/14/eu-us-umbrella-data-protection-agreement-detailed-analysis-by-douwe-korff/. Accessed 23 Dec. 2016.

[317] European Data protection Supervisor. *Opinion 1/2016.* 12 Feb. 2016, p. 16.

[318] *See* EUCJ court cases*: Commission v Austria*; *Commission v Hungary*; *Commission v Germany* and *Schrems.*

By the provision of article 21, the Parties shall have in place one or more public authorities exercising independent oversight functions and powers, including review, investigation and intervention. These authorities shall have the power to accept and act upon complaints made by individuals relating to the measures implementing the Umbrella Agreement and refer violations of law related to this Agreement for prosecution or disciplinary action.[319] Taking into account the particularities of the U.S. system, a combination of supervisory authorities into a committee, will cumulatively exercise the oversight functions that data protection authorities carry out in the EU. Moreover, the composition of the authority, the method for appointing its members, the duration of exercise and conditions of cessation of their functions, the allocation of sufficient resources to the authority or the adoption of decisions without being subject to external orders or injunctions[320].

But overall, Article 22 does not ensure cooperation between the EU and US authorities that can result in real, effective, binding enforcement of the principles in the Agreement against the receiving US Legal Enforcement Authorities.[321] More in particular, the European DPAs have no formal standing in that regard at all.

4.3.3.2. Redress Mechanism and Individual Remedy

GDPR entitle right to remedy for EU citizen to complain in any state that EU citizen live in or violator settled the business appearance. EU Directive gives member states chance to establish their own system but use directive as minimum standard. Depend on EU-US agreements, general fine on private organization could be appeal from Civil Court in any countries of EU. But the sue against US Public Authority must be taken to US federal court since US has amended Judicial Redress Act to allow EU citizen to bring the case to US court.

---

[319] European Commission. *Proposal for a COUNCIL DECISION on the signing, on behalf of the European Union, of an Agreement between the United States of America and the European Union on the protection of personal information relating to the prevention, investigation, detection, and prosecution of criminal offenses.* 29 Apr. 2016, p. 13.

[320] Korf, Douwe. "EU-US Umbrella Data Protection Agreement : Detailed Analysis by Douwe Korff." *European Area of Freedom Security & Justice*, 2015, https://free-group.eu/2015/10/14/eu-us-umbrella-data-protection-agreement-detailed-analysis-by-douwe-korff/. Accessed 23 Dec. 2016.

[321] Ibid.

EU GDPR

GDPR supply data subject a Right to claim compensation makes it considerably easier for individuals to bring private claims against data controllers and processors. In particular:

- Any person who has suffered "material or non-material damage" as a result of a violation of GDPR has the right to claim compensation from the controller or processor. [322] The inclusion of "non-material" damage means that individuals will be able to appeal complaint for distress and hurt feelings even where they are not able to prove financial loss.
- Suffers have the right to ask a consumer protection body to exercise rights and bring claims on their behalf.[323] Although this falls short from a US style class action right, it definitely escalates the risk of group privacy claims against consumer businesses.

Individuals also enjoy the right to lodge a complaint with a supervisory authority[324]

All natural and legal persons, including individuals, controllers and processors, have the right to an effective judicial remedy against a decision of a supervisory authority concerning them or for failing to make a decision[325].

Data subjects enjoy the right to an effective legal remedy against a controller or processor.[326]

EU Directive on Criminal Matters

The powers of the supervisory authority, that have to be set out by domestic law of each member state, the power to bring infringements of the provisions adopted

[322] EU. *General Data Protection Regulation.* 2016, Article 82(1).

[323] Ibid, Article 80.

[324] Ibid, Article 77.

[325] Ibid, Article 78.

[326] Ibid, Article 79.

pursuant to the Directive to the attention of judicial authorities[327] of each country that breached citizen bound with.

EU-US Privacy Shield

As an individual, data subject have several possibilities to lodge a complaint, namely with the:[328]

1) US Privacy Shield company itself;

2) Independent recourse mechanism, such as ADR or DPA;

3) US Department of Commerce, only through a DPA;

4) US Federal Trade Commission (or the U.S. Department of Transportation if complaint relates to an airline or ticket agent);

5) Privacy Shield Panel, only once certain other redress options have failed.

Individual can obtain redress in the US if their data is misused by commercial companies. Any individual who considers that his or her data has been misused will have several redress possibilities under the new arrangement: [329]

- Lodge a complaint with the company itself: Companies commit to reply to complaints within 45 days. In addition, any company handling human resources data from individuals has to commit to comply with advice by the competent EU Data Protection Authority (DPA), while other companies may voluntarily make such a commitment. The Commission encourages companies to do so.
- Take their complaint to their 'home' DPA: The DPA will refer the complaint to the Department of Commerce, who will respond within 90 days, or the Federal Trade Commission, if the Department of Commerce is unable to resolve the matter.

[327] EU. *Statement of the Council's reasons: Position (EU) No 5/2016 C158/46.* 2016, p. 8.

[328] European Commission. *Guide to EU-US Privacy Shield.* 2016, p. 12.

[329] European Commission. *EU-U.S. Privacy Shield: Frequently Asked Questions.* Press Release Database, Brussels, 29 Feb. 2016, p. 3.

- Use Alternative Dispute Resolution, a free of charge tool to which US companies may sign up as one of the redress mechanisms required for participation under the Privacy Shield. The companies will be required to include information in their published privacy policies about the independent dispute resolution body where consumers can address their complaints. They must provide a link to the website of their chosen dispute resolution provider and the Department of Commerce will verify that companies have implemented this obligation.
- If a case is not resolved by any of the other means, as a last resort there will be an arbitration mechanism. Individuals will be able to have recourse to the Privacy Shield Panel, a dispute resolution mechanism that can take binding decisions against U.S. self-certified companies. It ensures that every single complaint is being dealt with and that the individual obtains a remedy. Several 'consumer-friendly' features (e.g. no cost, possibility to participate by video-conference, free of charge translation and interpretation) ensure that individuals are not discouraged from making use of the panel.

There will be a number of ways to address complaints, starting with dispute resolution by the Privacy Shield companies and free of charge alternative dispute resolution solutions. Individuals can also go to the Data protection authorities who will work together with the U.S. Department of Commerce and Federal Trade Commission to ensure that complaints by individuals are investigated and resolved. If a case is not resolved by any of the other means, as a last resort there will be an arbitration mechanism.

The arbitration will take place in the U.S. because the company you are complaining about is based there. At the same time, there are several "consumer friendly" elements that will greatly benefit you: [330]

- right to ask for local DPA's assistance to prepare your claim;
- possibility to join the proceedings by telephone or video-conference, so there is no requirement to be physically present in the U.S.;

[330] European Commission. *Guide to EU-US Privacy Shield.* 2016, p. 17.

- possibility to obtain free of charge interpretation and translation of documents from English into another language;
- arbitral costs (except for lawyer's fees) will be offset from a fund specifically set up by the Department of Commerce and funded from the Privacy Shield companies' annual contributions.

Redress in the area of national security for individuals will be handled by an Ombudsperson independent from the US intelligence services.[331] The protection of your personal data may also be affected by U.S. public authorities when they access your data. The Privacy Shield ensures that this will occur only to the extent necessary for pursuing a public interest objective such as national security or law enforcement. While existing U.S. law provides you with protections and remedies in the law enforcement area, the Privacy Shield framework for the first time creates a special instrument to address national security access, the so-called Ombudsperson mechanism.[332]

The possibility for redress in the area of national security for everybody whose data is transferred to the U.S. will be handled by an **Ombudsperson,** independent from the US intelligence services. This is a new mechanism introduced by the Privacy Shield arrangement. The Ombudsperson mechanism will deal with individual complaints from individuals if they fear that their personal information has been used in an unlawful way by US authorities in the area of national security. [333] This redress mechanism will inform the complainant whether the matter has been properly investigated and that either US law has been complied with or, in case of non-compliance, this has been remedied.

However, the Privacy Shield does not follow the earlier recommendation of Working Party 29 according to which EU individuals should be "able to bring claims for

[331] European Commission. *EU-U.S. Privacy Shield: Frequently Asked Questions.* Press Release Database, Brussels, 29 Feb. 2016, p. 4.

[332] European Commission. *Guide to EU-US Privacy Shield.* 2016, p. 13.

[333] European Commission. *EU-U.S. Privacy Shield: Frequently Asked Questions.* Press Release Database, Brussels, 29 Feb. 2016, pp. 3-4.

damages in the European Union" as well as be "granted the right to lodge a claim before a competent EU national court."[334]

EU-US Umbrella Agreement

The Umbrella Agreement also fails to meet important requirements of EU data protection law in terms of data subject rights and data subjects' access to real and effective remedies. [335]

Data subject will be entitled to seek administrative redress. As for access and rectification, to facilitate the effective exercise of this right, the data subject concerned is entitled to authorize an oversight authority (national data protection authority for an EU data subject of each member state) or another representative,[336] where permitted under applicable domestic law. The competent authority from which relief is appealed will provide the data subject concerned with a written response indicating, where applicable, the ameliorative or corrective actions taken.[337]

The citizens of each Party shall be able to seek judicial redress for the i) denial of access, ii) denial of rectification or iii) unlawful disclosure by the authorities of the other Party.[338]

At the moment, if an EU citizens' data is transferred to US law enforcement authorities and if their data is incorrect or unlawfully processed, EU citizens – non-resident in the US- are unable to obtain redress in US courts (unlike US citizens, who could ask for redress in European courts). The Umbrella Agreement will introduce the equal treatment of

[334] Article 29 Data Protection Working Party. *WP29 letter to Vice-President Reding*. Brussels, 10 Apr. 2014.

[335] Korf, Douwe. "EU-US Umbrella Data Protection Agreement : Detailed Analysis by Douwe Korff." *European Area of Freedom Security & Justice*, 2015, https://free-group.eu/2015/10/14/eu-us-umbrella-data-protection-agreement-detailed-analysis-by-douwe-korff/. Accessed 23 Dec. 2016.

[336] EU-US. *Umbrella Agreement.* 2016, article 18.

[337] European Commission. *Proposal for a COUNCIL DECISION on the signing, on behalf of the European Union, of an Agreement between the United States of America and the European Union on the protection of personal information relating to the prevention, investigation, detection, and prosecution of criminal offenses.* 29 Apr. 2016, p. 11.

[338] EU-US. *Umbrella Agreement.* 2016, article 19.

EU citizens, as called for by President Juncker in his political guidelines. [339] A bill extending the core of the judicial redress provisions of the US Privacy Act of 1974 to EU citizens has been formally introduced in the US Congress on 18 March 2016 (Judicial Redress Bill). Once adopted, it will give EU citizens the right to seek judicial redress before US courts in case US authorities have denied access or rectification, or unlawfully disclose their personal data. The adoption of the Judicial Redress Bill will allow for the conclusion of the umbrella agreement.

The Umbrella Agreement does not provide for equal rights and remedies for EU- and US nationals in the USA; but worse, non-EU citizens living in EU Member States who are not nationals of the Member State concerned – such as Syrian refugees or Afghan or Eritrean asylum-seekers, or students from Africa or South America or China – and non-EU citizens who have flown to, from or through the EU and whose data may have been sent to the USA, are completely denied judicial redress in the USA under the Umbrella Agreement.[340]

4.3.3.3. Enforceability of Right

Among other things, the EU system has created a new solid administrative measures and criminal sanctions to implement those rules in data protection instruments. Criminal penalties are introduced to both in general data protection and protection of personal data in criminal relating matters. The most interesting is the GDPR, damage institutes fine up to 4% of worldwide revenue or 20 million Euros. The other criminal sanction is up to the domestic law of EU states and US federal law.

EU GDPR

GDPR increased enforcement powers. Currently, fines under EU Member State law vary, and are comparatively low (e.g., the UK maximum fine is £500,000). The Regulation will significantly increase the ***maximum fine to €20 million, or 4% of annual***

[339] European Commission. *Questions and Answers on the EU-US data protection "Umbrella agreement".* Brussels, 1 Dec. 2016, p. 2.

[340] Korf, Douwe. "EU-US Umbrella Data Protection Agreement : Detailed Analysis by Douwe Korff." *European Area of Freedom Security & Justice*, 2015, https://free-group.eu/2015/10/14/eu-us-umbrella-data-protection-agreement-detailed-analysis-by-douwe-korff/. Accessed 23 Dec. 2016.

worldwide turnover, whichever is greater. In addition, national data protection supervisory authorities will be co-ordinating their supervisory and enforcement powers across the EU Member States, likely to lead to a more pronounced enforcement impact and risk for businesses.[341]

GDPR bring in **revenue based fines** principle, joins anti-bribery and anti-trust laws, as having some of the very highest sanctions for non-compliance including revenue based fines of up to 4% of annual worldwide turnover.[342]

To compound the risk for multinational businesses, fines are imposed by reference to the revenues of an undertaking rather than the revenues of the relevant controller or processor. Recital 150 of GDPR states that "undertaking" should be understood in accordance with Articles 101 and 102 of the Treaty on the Functioning of the European Union which prohibit anti-competitive agreements between undertakings and abuse of a dominant position. Unhelpfully the Treaty doesn't define the term either and the extensive case-law is not entirely straightforward with decisions often turning on the specific facts of each case. [343] However, in many cases group companies have been regarded as part of the same undertaking. This is bad news for multinational businesses as it means that in many cases group revenues will be taken into account when calculating fines, even where some of those group companies have nothing to do with the processing of data to which the fine relates provided they are deemed to be part of the same undertaking. The assessment will turn on the facts of each case. [344]

Fines are split into two broad categories:

1) The highest fines up to 20,000,000 Euros or in the case of an undertaking up to 4% of total worldwide turnover of the preceding year, whichever is higher apply to breach of: [345]

[341] Hunton&Williams. *Overview of the EU General Data Protection Regulation.* 2016, p. 1.

[342] EU. *General Data Protection Regulation.* 2016, Article 83(5).

[343] Hunton&Williams. *Overview of the EU General Data Protection Regulation.* 2016, p. 2.

[344] DLA Piper. "EU General Data Protection Regulation - Key Changes." www.dlapiper.com/en/uk/focus/eu-data-protection-regulation/key-changes/. Accessed 10 May 2016.

[345] EU. *General Data Protection Regulation.* 2016, Article 83(5).

- the basic principles for processing including conditions for consent
- data subjects' rights
- international transfer restrictions
- any obligations imposed by Member State law for special cases such as processing employee data
- certain orders of a supervisory authority

2) The lower category of fines is up to 10,000,000 Euros or in the case of an undertaking up to 2% of total worldwide turnover of the preceding year, whichever is the higher apply to breach of: [346]

- obligations of controllers and processors, including security and data breach notification obligations
- obligations of certification bodies
- obligations of a monitoring body

Supervisory authorities are not required to impose fines but must ensure in each case that the sanctions imposed are effective, proportionate and dissuasive[347].

Fines can be imposed in combination with some other sanctions.

There is an urgency procedure for exceptional circumstances which permits a supervisory authority to adopt provisional measures on an interim basis where necessary to protect the rights and freedoms of data subjects.[348]

GDPR establish wide corrective powers. Supervisory authorities also enjoy broad investigative and corrective powers[349]including the power to undertake on-site data protection audits and the power to issue public warnings, reprimands and orders to carry out specific remediation activities.[350]

[346] Ibid, Article 83(4).

[347] Ibid, Article 83(1).

[348] Ibid, Article 66.

[349] Ibid, Article 58.

[350] Council of the European Union. *5418/16 ADD 1.* 2016, p. 16.

EU Directive on Criminal Matters

The supervisory authorities powers may have in each Member State the same tasks and effective powers to allow them to carry out the tasks of effective, reliable and consistent enforcement of the Directive throughout the Union. The powers of the supervisory authority, that have to be set out bylaw, in two different categories, corrective and advisory powers as well as the power to bring infringements of the provisions adopted pursuant to the Directive[351] to the attention of judicial authorities. The enforcement is sanctioned by the domestic law relevant to personal data protection.

EU-US Privacy Shield

The Privacy Shield creates far stronger enforcement obligations and establishes new recourse mechanisms.[352] The US has committed to maintaining an updated list of current Privacy Shield members and removing those companies that have left the arrangement.

To verify that the self-certification is effective in practice, Privacy Shield organizations can make self-assessment or outside compliance reviews on the basis of "Self-Assessment".[353] The Department of Commerce will ensure that companies that are no longer member of Privacy Shield must still continue to apply its principles to personal data received when they were in the Privacy Shield, for as long as they continue to retain them.[354]

If the Privacy Shield Panel finds evidence of a violation of the Privacy Principles it can impose relief such as access, correction, deletion, or return of data subject's personal data. Even if the Privacy Shield Panel cannot award data subject monetary damages, individual has the possibility to obtain such relief in court. If data subject are not satisfied with the outcome of the arbitration, he can challenge it under U.S. law under the Federal

[351] EU. *Statement of the Council's reasons: Position (EU) No 5/2016 C158/46.* 2016, p. 8.

[352] Wilmer Cutler Pickering Hale and Dorr LLP. "Comparison of Requirements under the Privacy Shield/Safe Harbor Principles." *Lexology*, 25 Jul. 2016, p.8.

[353] EU-US. *Privacy Shield.* 2016, Annex II, III.7.c.

[354] European Commission. *Questions and Answers on the EU-US data protection "Umbrella agreement".* Brussels, 8 Sep. 2015, p. 2.

Arbitration Act.[355] The arbitration procedure will be finished within 90 days and response to the complainant within 45 days from the day data subject has sent notice to the company.

On behalf of Ombudsperson, it can order non-compliance to be remedied. In combination with the lack of clarity concerning the investigatory powers, it moreover remains unclear to what extent the Ombudsperson as such will be effectively capable of ordering non-compliance to be remedied and what the result of such an exercise would be.[356]

Moreover, the Privacy Shield does not provide for any appeal against or review of the "decision" by the Ombudsperson. The communication of the Ombudsperson to the complainant after her examination of a complaint, the Ombudsperson must not reveal, if there has been any unlawfulness behavior of the intelligence community.[357] The answer provided will always be the same and it will be unspecific.

EU-US Umbrella Agreement

The effective implementation of the articles concerning individual rights (access, rectification, administrative and judicial redress), as well as the issue of transfers to territorial entities not covered by the Agreement (*i.e.* U.S. States). The first joint review will be conducted no later than three years from the entry into force of the Agreement and thereafter on a regular basis.[358]

The Competent Authority from which relief is sought will carry out the appropriate inquiries and verifications and without undue delay will respond in written form, including through electronic means, with the result, including the ameliorative or corrective action taken where applicable.[359] Notice of the procedure for seeking any further administrative redress shall be provided.

In practice, an EU citizen's name is identical to that of a suspect in a transatlantic criminal investigation. Their data has been transferred from the EU to the US

[355] European Commission. *Guide to EU-US Privacy Shield.* 2016, p.18.

[356] Article 29 Data Protection Working Party. *Opinion 01/2016 on the EU – U.S. Privacy Shield draft adequacy decision.* 13 Apr. 2016, p. 50.

[357] Ibid, p. 51.

[358] EU-US. *Umbrella Agreement.* 2016, article 23.

[359] Ibid, article 18(3).

and erroneously gets collected and included on a US "black list". This can lead to a series of adverse consequences from the refusal of an entry visa, to a possible arrest. The EU citizen should be able to have their name deleted by the authorities – if necessary by a judge – once the mistake is discovered. Europeans (and Americans) have those rights in the EU. They should have them when their data is exchanged with the US too. The citizen who believes that their data is inaccurate also can authorize, where permitted under domestic law, an authority (for instance a Data Protection Authority) or another representative to seek correction or rectification on his or her behalf. If correction or rectification is denied or restricted, the US authority processing the data should provide the individual or the data protection authority acting on their behalf with a response explaining the reasons for the denial or restriction of correction or rectification. [360]

4.4. Prerequisite considerations for International Personal Data Protection Reform

The reforms of the EU-US E-Market regime create many effects in the near future which can categorize into 12 issues. The ramifications of reformation are not just legal binding area but socio-economic perspective. The model of their agenda could be use as a strategy to enlarge the E-Market and Informative Society with better harmonized standard.

These prerequisite considerations, extracted from the EU and EU-US E-Market regime, in 12 issues are:

1) Legal Approval: The Regime must create greater harmonization by introducing a single-legal framework. It may requires the periodically reviews. Especially in the context of criminal law enforcement cooperation, it should include harmonized rules for international transfers of personal data, data sharing and data retention. Besides, the regime must cover core data protection principles. For tight-integrated international organization or regional integration, it may suggest supra-national direct effect upon all State Party / Member State without further enacting domestic law.

2) Definition and Scope: The Regime should apply to organizations established in a third country if they are offering goods and services, or monitoring the behavior of individuals, in its E-Market. The instrument must give the common definition on basic data

[360] European Commission. *Questions and Answers on the EU-US data protection "Umbrella agreement".* Brussels, 1 Dec. 2016, p. 2.

protection terms. The regime must harmonize rules for law enforcement cooperation within Member States or State Parties in every level. It must guarantees that personal data transferred outside their territory by criminal law enforcement authorities will be adequately protected. The person covered by instrument should apply to all relevant Legal Persons, who offer services, and State Intelligence Agencies, who collect and process personal data, of State Parties' nationals.

3) Contents of Data Subjects' Right: The inventive Regime must affirm the rights relevant to digital age; right to data portability, right to be forgotten/erasure, right to access and rectify the out-of-date data. In the realm of Criminal Matters, it should raise the level of protection for individuals; victims, witnesses, and suspects of crimes, specifically the protection in the context of a criminal investigation or profiling. The fundamental rights relevant protection of personal data must be approved; Right to be noticed, make a choice, access the data and gain Redress. Furthermore, the instrument shall provide data subject judicial redress rights; right to denial of access, denial of rectification and unlawful disclosure.

4) Exception: As any instruments are inter-state law so the conditions and requirements of exception, necessary and proportionate principle, as written in UN Declaration on Human Rights and other International Human Rights Treaties must be reconfirmed. While the instrument relevant to data protection on Criminal Matters, the level of flexibility accorded to the exception conditions and requirements may depend more on the breadth of national legislative measures. Nevertheless, it should provide clear necessary restrictions, proportionate safeguards and oversight mechanisms for access by state agencies for law enforcement and national security purposes. The exemptions in practice, *de facto*, would bar the possibility for the person to have access to their own data, so its application must be limited only to cases "permitted under applicable domestic law".

5) Basic Duty: The Regime should put the direct obligation to Data Processor. It should promote the mixing approach between "Privacy by Default and Privacy by Design" to Data Controller/Processor. Organizations who collect and control personal data must appoint DPO to take care of protection and cooperate with DPA. It must embrace the "Right to opt-out" data transfer or data processing and "Right to opt-in" when company is going to process data. The participating organizations must provide data subject with a link to its privacy policy if it has a public website. It should urges organizations to raise the individuals'

awareness as to why and by whom their data is processed and contribute to the possibility for individuals to exercise their rights to access, rectification or redress.

6) Data Collection and Processing: The Regime should introduce the anonymity for data subject consist of appropriate safeguards, which may include encryption or "pseudonymisation". It is needed to take risk impact assessments in case of processing highly sensitive personal data, profiling. The profiling resulting in discrimination against natural persons shall be prohibited. The Fair Use principle must be embedded in data processing conditions and requirements; Notice, Choice, Onward Transfer and Data Integrity/Purpose Limitation. It has to be clarified that the right to opt-out cannot enable the organization to use data for incompatible purposes. It must ensure the application of the safeguards to the entire "life cycle" of a given data set from the original transfer from the host country to its processing by a competent authority in Counterpart-State and vice-versa. It also requires 'appropriate safeguards that include the possibility to obtain human intervention' if the automated decision-making, profiling, has taken place.

7) Data Security: The Regime must employ breach notification, to fulfill the provision on data security, organizations must notify the national supervisory authority of serious data breaches promptly, "without undue delay". So the data subjects can take appropriate measures then it clarifies the situation when derogations can be used. The Regime should acknowledge the existence of a risk-based approach to compliance of State Parties. For precautionary, set out the criterions in which an impact assessment is compulsory. In similar terms, requirements, risk assessment process, should be introduced to routinely supervision. It should ensure that appropriate action will be promptly taken to mitigate the damage, including notification to the transferring authority and, where appropriate given the circumstances of the incident, the individual concerned.

8) Data Retention: The proposed Regime should give the clear data retention limits, restrictions and safeguards. This data may only be processed under official authority or when authorized by State Party's law. Most importantly, it must raise the level of protection for individuals during data retention in the context of a criminal investigation or a law enforcement action. Oversight is ensured by independent national data protection authorities and data subjects can afford effective judicial recourse. There must be an obligation of data controller/processor to document data processing operations entails, in particular, that there will be a "trace" in case of unlawful processing. The retention periods will be subject to

periodic reviews and to ensure transparency, retention periods will have to be made publicly available or otherwise published. It is also specified that, where the Parties conclude an agreement on the transfer of "bulk data", such agreement must contain a specific provision on the applicable retention period. The data controller must also provide information about profiling.

9) Data Transfer: The new Regime must provide comprehensive, detailed and transparent rules for data transfers to third countries including the power to suspend data flows to a recipient in a third country or to an international organization who does not meet the adequacy standard.. While remains essentially tools, as well as certain derogations to transfer personal data outside the State Parties' territory, while reducing Red Tape. It should introduce some new tools for international transfers, Adequacy decisions, by providing more precise and detailed elements that must take into account when assessing the level of data protection provided in the legal order of a third country. The instrument should contain Onward Transfer principle but it include statements concerning the enforcement body, an arbitration right, disclosures to public authorities, and the legal person's liability for onward transfers.

10) Monitoring Body and Supervisory Authority: The instrument provisions on the independence, functions and powers of Collective; Universal, International or Regional, Data Protection Authority (DPA) must be expressed out in more detail and substantially enhanced. It should provide an effective monitor and sanctions by harmonizing the powers of national data protection supervisory authorities (DPAs). In the area of Criminal Matters, Supervision is ensured by independent national data protection authorities or domestic courts. To race up the changes of information technology, it should establish mechanisms regarding the enforcement bodies: ADR, Ombudsperson and old style DPA with greater competence. It should transform the oversight system from self-regulating to more responsive and proactive system, verification and annual re-verification process must proposed, the monitor compliance could be done via detailed questionnaires. Moreover, it should expand to the whole law enforcement sector the principle of independent oversight including effective powers to investigate and resolve individual complaints.

11) Redress Mechanism and Individual Remedy: The Regime should create One-Stop-Shop redress for data subject by addressing that any suffering individual can lodge their complaint to their own National DPA then the DPA will work internationally with other State

Party's DPA. In the case of Criminal Matters, it should remind State Members to make sure that individuals can afford effective judicial remedies. The direct accessible channel for individual such as ADR and Ombudsperson should be provided. It should also create an arbitration right for unresolved complaints for individual. Redress mechanism will inform a complainant of an access or surveillance matter has been properly investigated and obliged with the instrument, and proper remedies will be given. Remedy mechanisms must determine time period for responses by a subject organization.

12) Enforceability of Rights: The inventive Regime must expressly include the power to suspend data flows to a recipient in a third country or to an international organization in case of non-compliance. The local DPAs or Courts will be empowered to impose fines reaching up to EUR 20 million or up to 4% of the total worldwide annual turnover of a company. To bear in mind, in the scope of criminal matters, the capability of enforcement bases on particular State Party's enforcement institutions; National DPAs and the Domestic Courts. It should supply enforcement body which can inform a complainant of an access or surveillance matter, disclosures to public authorities. In the case of non-compliance it will be properly remedied. Moreover, the precautionary system such as "Flag list" for organizations which are subjected to DPA or Court orders from violation cases. To support the efficiency of enforcement, solid powers to investigate and resolve individual complaints must be confirmed as well as the material sanctions even it depends on domestic Courts.

Lastly, the instruments of the Regime must be subjected to periodic joint reviews, on critical provisions relate to individuals' rights; access, rectification, administrative and judicial redress.

The reforms of the EU and EU-US regime set up a new harmonized standard for liberal market-economy country to follow. Their regime could be transformed to International Treaty open for other state to ratify because it will save the time and budget consuming during negotiation and drafting phrases. International Community may use these set of standards as a point of departure to draft International Instrument on Personal Data Protection for sign and accession. Due to the technological hegemony of US IT Corporation on Cyberspace and the mature of EU-US single E-Market, it would be the incentive for other States to conform to their legal regime for boosting the economy of respective States. Thus, creating the International Treaty that meet the Adequacy Criterion of EU would be beneficial

for all liberal market regime countries and very persuasive for wider spread accession. The more inclusive approach would solve the problem on jurisdiction, and makes the compliance of personal data protection to different jurisdiction possible. The comprehensive considerations above could be embedded in as the baselines or components for initiating Universal Regime. The synthesis for Universal and International levels will be displayed in the next Chapter.

Table of 12 legal issues in 4 EU and EU-US Instruments

Issue / Instrument	EU General Data Protection Regulation	EU Directive onCriminal Matters	EU-US Privacy Shield	EU-US Umbrella Agreement
1. Legal Approval	1, 94 - 99	1, 58 - 65	Overview 1, 6	1, 5, 29
2. Definition and Scope	1, 2 – 4	1 - 3	Overview 8 - 9	2, 3, 27, 28
3. Content of Individual Rights	12 – 22	12 - 14, 16 - 18	II Principle 1-2, III Principle 8, 8f, 12	16.1, 16.3-5, 17, 20
4. Exemptions	23, 49, 89, 91	15, 38	Overview 5, III Principle 1-2, 8e, 9e, 13, 14	16.2, 20.2
5. Duty of Data Controller/Processor	24 – 31, 37 – 43	19 – 23, 26, 32 -34	Overview 6, III Principle 3-4, 8bcdghi	4, 11, 14, 20
6. Principle of Processing	5 – 11, 85 – 88, 91	4 - 11	II Principle 5, III Principle 9a-c, P.10a	6, 8, 13, 15
7. Data Security	32 – 36	27 - 31	II Principle 4,	9 - 10
8. Data Retention	10, 29 – 31, 90	24 - 26	III Principle 15,16	11 - 12
9. Data Transfer	44 – 50	35 - 40	II Principle 3, 7d III Principle 10bc	7
10. Supervisory Mechanism	51 – 59, 60 – 76, 90, 92, 93	41 – 51, 58	Overview 2, II Principle 7a(i), III Principle 5, 6, AnnexOmbudsperson	14, 18.2, 21, 22-23
11. Individual Remedy	65, 77 – 80, 82	48, 52 - 56	Overview 4, II Principle7a(iii),7bce III Principle 6,7, 11a-d AnnexArbitral,Ombus	18.1, 19.1, 19.3, 19.4
12. Enforcement/ Sanction	58, 65, 81 – 84	51, 57	Overview 3, II Principle 7a(ii), III Principle9cd, 11efg Annex Arbitral	18.3, 19.2, 23-26

Chapter 5 Universal approach on Personal Data Protection in Cyberspace

The goal of this Chapter is to crystallize the Universal Approach for supporting progressive realization of personal data protection internationally based on the International initiatives and comparative synthesis from the EU and EU-US approach. Eager to accomplish that goal, the first section will trace back to the root of the problem. Since protection of personal data deals with activities relating internet and Transnational IT Corporation, domestic law of single State cannot solve the highly trans-border complications. The Needs of International Regime to protect personal data on Cyberspace have been recognized by many reports and resolutions of International Organizations. The second section reveals the main concerns of UN Human Rights Council and many States on the Global Mass Electronic Surveillance undertaken by State Intelligence Agencies and in some cases with the coordination of IT Corporations. Accordingly, the third section will review the initiatives given by international governmental organizations and non-governmental movements on personal data protection. Then comparative synthesis from EU and EU-US regime will be brought to fill the loopholes in 3 main issues; Individual's Right of internet users around the world, obligation of the Transnational IT Corporation as a Data Controller/Processor and creating an implementation system of Personal Data Protection rules. The last section transforms all desires, protection of personal data in cyberspace globally, into benchmarks for initiating Universal Regime to take care of data subjects worldwide.

5.1. Background: The Needs of International Regime to protect Personal Data in Cyberspace

Protection of Personal Data in Cyberspace is not an exclusive EU and US regime problem. Of course, there are several initiatives, from intergovernmental and non-governmental organizations, trying to deal with this issue internationally. Some of them have already adopted useful documents to understand current shortcomings and they include the broad design of proposals to overcome them. The analysis in past chapters has shown how the new EU-US regime can be used to implement those proposals. Before jumping to the solutions, the essence problems from the activities in cyberspace will be analyzed first.

In the terms of Globalization Capitalism, "Google act upon reasons chosen by them. The liberal logic would be thus inverted but to a company that expects to be judged as doing no evil and, paradoxically, as being a champion of values of liberal nature".[1] State seems to be delight with the dynamics of business circle and gain benefit from personal data processing by Multinational IT Corporation. Even though the International Economic Organization, WTO, never has had a single case or precedent relevant to this issue yet but there is the provision that urges Member States to protect personal data.

Over the past decade it has been the shift towards the market-driven and technology determinism models of the Service Providers (SPs) like IT Corporation that has changed the face of the internet. If the next such shift is one that favors privacy and autonomy, that could be on behalf of all people. However, the evidences from US former contractor have shown the main threats to Cyber Security by Global Surveillance Programs relate to IT Corporation. The threats came from the National Authority who breach in to data system of IT Corporation or even cooperate with IT Corporation, instead of protecting Cyber Security for the Internet Citizen.

However, the International Community is struggling with the problem by initiating New Personal Data Protection and negotiating with various International Civil Societies to establish new Instrument on Personal Data Protection and harmonize the standard on international criminal cooperation matters. Still, there is no specific international instrument to handle these problems.

The initiatives of UNHRC and Civil Society Organizations have shown the preparation to counter-strike data processing of IT Corporation in some certain but the implementation of Personal Data Protection Regime stills questioning. Since there has been neither mechanism to fulfill the obligation to protect personal data of UN nor International preventive measure for monitoring IT Corporation's threats yet. Besides, there has been no international measure to handle the wide spread of data surveillance done by State Authority on internet users around the globe.

On international level, the Human Rights Council undertaken the mission of resolution 68/167 of the UN by approved the report from the Office of High Commissioner

[1] Thompson, Marcelo. "In Search of Alterity: On Google, Neutrality and Otherness." *Google and the Law*, Springer, New York, 2012, p. 360.

for Human Rights (OHCHR) on 30 June 2014, UN High Commissioner Report on the Right to Privacy in the Digital Age.[2] The report scope on the protection and promotion of the right to privacy in the context of mass electronic surveillance or digital communications interception and the collection of personal data, including a global scale surveillance.[3] OHCHR participated in a number of events and gathered information from a broad range of sources. On 24 February 2014, the High Commissioner delivered a keynote presentation at an expert seminar on "The right to privacy in the digital age", which was co-sponsored by Austria, Brazil, Germany, Liechtenstein, Mexico, Norway and Switzerland,[4] States whom were tapped by NSA due to US Global Internet Surveillances. Contributions to the resolution were received from 29 Member States from all regions, five international and/or regional organizations, three national human rights institutions, 16 non-governmental organizations and two private sector initiatives,[5] which were referred before in Report A/HRC/23/40.

In regional arena, since the US Global Internet Surveillances, there are significant signal which show the enthusiastic of EU to cope with the problem both by initiating new regulation and proposing new agreement with USA on personal data protection. Günther Oettinger, EU Commissioner for Digital Economy, said in the World Economic Forum 2015 that "We need a UN agency for data protection and data security"[6] for rebuilding trust among companies and consumers. The time for having personal data protection agency in UN Human Rights system has come. The set of Instruments, Umbrella Agreement between EU-US on Implementation and enforcement measures relate to personal data, had been launched after the negotiation between EU and US was settled in Mid-2016. As well as the EU-US Privacy Shield that US give in the mutual agreement to meet the EU demand base on Fundament Right to protection of personal data. The EU approach is effective due to the clear present doctrine of personal data protection in EU legal system, rule of law.

In terms of Precaution, personal data protection should be managed on the basis of rule of law, collective control, transparency, maximizing limited available resource and

[2] UN. *A/HRC/27/37*. 2014, para. 5.

[3] Ibid, para. 15.

[4] Ibid, para. 7.

[5] All contributions are available at www.ohchr.org/EN/Issues/DigitalAge/Pages/DigitalAgeIndex.aspx.

[6] Wearden, Graeme and Treanor, Jill. "UN Needs Agency for Data Protection, European Commissioner Tells Davos." *The Guardian*, 22 Jan. 2015, section Technology, www.theguardian.com/technology/2015/jan/22/un-agency-data-protection-davos-edward-snowden. Accessed 12 Nov. 2016.

reflexive mechanisms. Thus, the recognition of threats from IT Corporation and National Security Authority must be responded by harmonized international regulation and trans-national competence mechanism.

5.2. Recognition of problems relating personal data protection by International Community

The US Global Internet Surveillances also underscore the precarious position that companies, Trans-National Corporation, offering these services and technologies in one country is placed in other territory. Though the scope and quantity of data collected and held by an intermediary, IT Corporation, vary depending on the type of intermediary. Since IT Corporations offer many services to countless customers and locate its infrastructure cover vast area, governments have recognized the important role of them as Intermediary. Particularly in their ability to assist with state surveillance efforts by providing efficient access to a great number of user data and identifying potentially harmful or threatening content. Within this context, there is a shift from reactive government surveillance that is based on a request and authorized order, to partially privatized surveillance, with companies identifying and reporting potential threats, retaining information, and facilitating access to law enforcement. Indeed, the OHCHR in the Right to Privacy in the Digital Age report notes that the US Global Internet surveillance programs were facilitated in part by "strategic relationships between Governments, regulatory control of privacy companies, and commercial contracts."[7] The 2 dominant actors in this problem were recognized by International Organization respectively; IT Corporation and State Authority.

5.2.1. Problems from IT Corporation's activities

As individuals utilize intermediary platforms on a daily and routine basis, from searching for information on the internet, to posting updates to a social media account, to using voiceover-internet-protocol (VoIP) services to connect with friends and colleagues, or using the services of a cyber cafe, intermediaries host; IT Corporation, Data Controller and Data Processor, retain and have access to vast amounts of personal data of their users across

[7] UN. *A/HRC/27/37*. 2014, Preamble.

the world, irrespective of jurisdiction. In this context, company practices and a country's legal regulations have a far-reaching impact on the rights, specifically right to personal data protection, of both national and foreign users.[8]

When intermediaries, Service Providers, implement legal requirements for the blocking or filtering of content, they do so by employing different techniques and technologies such as key word filtering software, firewalls, image scanning, URL databases, technologies that enable deep packet inspection, etc.[9] Similarly, complying with legal mandates for interception or monitoring of communications also requires intermediaries to install and use technology on their networks. As pointed out by La Rue, technologies used for filtering also facilitate monitoring and surveillance as they have the ability to identify and track words, images, websites and types of content, as well as identify individuals using, producing or associated with the same.[10] For example, YouTube offers copyright holders the option of YouTube's "Content ID" system to manage and identify their content on the platform. Actions that copyright owners can choose from include muting audio that matches the music of copyrighted material, blocking a video from being viewed, running ads against a video, and tracking the viewer statistics of the video. These options can be implemented at a country-specific level.[11]

Instances such as the IT Corporations; Facebook, Google, Apple etc., demonstrate the complexity of issues related to intermediary liability and surveillance and raise questions about reasonable expectations regarding internet company practices and responses (particularly multinational companies), adequate national legislation, international guidelines, and appropriate public response. As noted in The Right to Privacy in the Digital Age, "the Guiding Principles on Business and Human Rights", endorsed by the Human Rights Council in 2011, provide a global standard for preventing and addressing adverse effects on human

[8] Hickok, Elonnai. "Intermediary liability and state surveillance." *Global Information Society Watch 2014: Communication Surveillance in Digital Age*, Centre for Internet and Society (CIS), India, 2014, p. 46.

[9] "Whitepaper: Understanding Web Filtering Technologies." *BLOXX*, www.bloxx.com/downloads/US/bloxx_whitepaper_webfilter_us.pdf. Accessed 16 Nov. 2016.

[10] La Rue, Frank. "Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression." *United Nations General Assembly*, 17 Apr. 2013.

[11] YouTube. "How Content ID Works." https://support.google.com/youtube/answer/2797370?hl=en. Accessed 16 Nov. 2016.

rights linked to business activity. The responsibility to respect human rights applies throughout a company's global operations regardless of where its users are located, and exists independently of whether the State meets its own human rights obligations." This is a high standard that intermediaries must adhere to. Some companies such as Google,[12] has policies in place for addressing requests from law enforcement as mentioned before in Chapter 3.

The cooperation between IT Corporation and State Authority is increasingly formalized: as telecommunications service provision shifts from the public sector to the private sector, there has been a "delegation of law enforcement and quasi-judicial responsibilities to Internet intermediaries under the guise of 'self-regulation' or 'cooperation'".[13] The enactment of statutory requirements for companies to make their networks "wiretap-ready" is a particular concern, not least because it creates an environment that facilitates sweeping surveillance measures.[14]

As pointed out by Frank La Rue in the Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, legal frameworks that hold intermediaries (rather than the individual) liable for content are needed, transfering the role of monitoring the internet to the intermediary.[15] Some jurisdictions do not have specific legal provisions addressing intermediary liability, but do issue court or executive orders to intermediaries for the restriction of content, as well as placing obligations – including technical obligations – on service providers via operating licenses. Legal provisions and orders pertaining to intermediary liability are not always limited to removing or disabling pre-defined or specified content. Requests for the removal of content can be accompanied with requests for user information including IP address and basic subscriber information. Some jurisdictions, such as India, have incorporated retention mandates for removed content and associated information in legal provisions addressing intermediary liability.[16]

Human Rights Council draw conclusions about corporate responsibilities for communication security, it is nonetheless clear that, given the threats to right to personal data

[12] Google, "Google Transparency Report." www.google.com/transparencyreport. Accessed 16 Nov. 2016.

[13] European Digital Rights. "The Slide from "Self-Regulation" to Corporate Censorship." Jan. 2011.

[14] UN. *A/HRC/27/37*. 2014, para. 42.

[15] La Rue, Frank. "Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression." *United Nations General Assembly*, 17 Apr. 2013.

[16] WIPO. *The Information Technology (Intermediaries Guidelines) Rules*. 2011, Rule 3(4).

protection online, IT Corporation actors should review the adequacy of their practices with regard to human right norms. At a minimum, companies should adhere to principles such as those laid out in the Guiding Principles on Business and Human Rights, the Global Network Initiative's Principles on Right to personal data protection and Privacy, the European Commission's ICT Sector Guide on Implementing the UN Guiding Principles on Business and Human Rights, and the Telecommunications Industry Dialogue Guiding Principles. Companies, like States, should construct the International Regime to avoid blocking or limiting the transmission of encrypted communications and permit anonymous communication.[17] Furthermore, the initiative to regulate corporation actors that supply technology to undermine encryption and anonymity would be beneficial to govern their products and customers with transparency principle. [18] Consequently, attention should be given to efforts to expand the availability of encrypted data-centre links, support secure technologies for websites and develop widespread default end-to-end encryption.

5.2.2. Problems caused by State Authority

The protection and promotion of the right to privacy in the context of domestic and extraterritorial surveillance and/or the interception of digital communications and the collection of personal data, including on a mass scale surveillance undertaken by State Agencies[19] had been emphasized by UN Human Rights Council Resolution. UN HRC approved the analysis and findings on the impacts of human rights in the context of mass surveillance, metadata collection and retention, and the recommendations to apply human rights to extraterritorial actions of government collects.[20] The resolution analysis brought dramatic global concerns on data protection on Internet since the US Global Internet Surveillances in June 2013 into the content.

One year after US Global Internet Surveillances in 2013, The Right to Privacy in the Digital Age: Report of the Office of the United Nations High Commissioner for Human

[17] UN. *A/HRC/29/32*. 2015, para. 62.

[18] Ibid, para. 61.

[19] UN. *A/HRC/23/40*. 2013, paras. 38-39.

[20] Ibid, para. 40.

Rights (OHCHR) was published.[21] The Report recognizes the relationship between service providers and surveillance and the increasing trend of privatized surveillance, noting: There is strong evidence of a growing reliance by Governments on the private sector to conduct and facilitate digital surveillance. On every continent, Governments have used both formal legal mechanisms and covert methods to gain access to content, as well as to metadata. This process is increasingly formalized: as telecommunications service provision shifts from the public sector to the private sector, there has been a "delegation of law enforcement and quasi-judicial responsibilities to Internet intermediaries under the guise of 'self-regulation' or 'cooperation'".[22] This report also explores how legal requirements, practices and policies pertaining to intermediary liability are feeding into this growing trend through the incorporation of requirements for intermediaries that facilitate surveillance for government.

The A/HRC/27/37 report's analysis and findings are of human rights in the context of mass surveillance, metadata collection and retention, and the application of human rights to extraterritorial actions of governments.[23] Report found that Mass surveillance by its very nature interferes with the right to privacy, and recommended that all stakeholders take steps to ensure that effective and independent oversight regimes and practices are in place, with attention to the rights of victims and to effective remedies.[24] On every continent, Governments have used both formal legal mechanisms and covert methods to gain access to content, as well as to metadata. The response from Non-governmental organizations on Internet Rights and Privacy is good, the report and discussions are underway about how best to take this work forward to ensure data privacy rights protection.[25]

Jurisdiction and the applicability of local law is a tension that arises in the context of intermediary liability and surveillance. Some facets of this tension include: to what extent do legal restrictions on content apply to multinational platforms operating in a country? To what extent can states access the communications passing or being stored in its territory? And to what extent do domestic protections of fundamental rights – including freedom of expression and privacy – apply to foreigners as well as nationals? The OHCHR in The Right to Privacy

[21] UN. *A/HRC/27/37*. 2014.

[22] Ibid, Recommendations.

[23] Ibid, para. 3.

[24] Ibid, para. 49.

[25] Ibid, para. 51.

in the Digital Age shed some light on these questions, drawing upon a number of international instruments and firmly asserting that any interference with the right to privacy must comply with the principles of legality, proportionality and necessity, regardless of the nationality or location of the individual.[26]

Tensions around mass surveillance of foreign citizens and political leaders, and a lack of legal constructs domestically and internationally to address these tensions, have led to questions of direction and the future of internet governance discussed at forums like NETmundial, where principles relating to surveillance and intermediary liability were raised.[27] Similarly, in March 2014, the US announced plans to relinquish the responsibility of overseeing the body tasked with regulating internet codes and numbering systems. This move has raised concerns about a backlash that could result in the division and separation of the internet, facilitating mass surveillance and content control.[28]

However, Data retention, Broad mandatory data retention policies limit an individual's ability to remain anonymous. A State's ability to require Internet service and telecommunications providers to collect and store records documenting the online activities of all users has inevitably resulted in the State having everyone's digital footprint. A State's ability to collect and retain personal records expands its capacity to conduct surveillance and increases the potential for theft and disclosure of individual information.[29] To fulfill right to personal data protection, States, international organizations, corporations and civil society groups should promote online security. Given the relevance of new communication technologies in the promotion of human rights and development, all those involved should systematically promote access to encryption and anonymity without discrimination.[30] Consequently, the prospect regime to tackle these problems is needed.

[26] Ibid.

[27] Powles, Julia. "Big Business Was the Winner at Netmundial." 28 Apr. 2014.

[28] Kelion, Leo. "Future of the Internet Debated at NetMundial in Brazil." *BBC*, 23/4/2014, <www.bbc.com/news/technology-27108869>, Accessed 16/11/2016.

[29] UN. *A/HRC/29/32. 2015*, para. 55.

[30] Ibid, para. 62.

5.3. Initiatives to support the progressive realization of right to personal data protection

While the Chapter 4 flash the light on the most advance legal regime for protection of personal data in EU-US regime, especially this section will search for the efforts in universal and international levels to push the protection of personal data to proper standard. Even though, the new EU-US regime may answer some of the requirements in EU and US E-Market but there are some areas else without the regulation. The section will study on previous international proposals, which have identified as the 'minimum' content of an International/Universal legal instrument, governing the issue of personal data protection in cyberspace. This is the case studies in this section and will be explained from their launching institution perspectives.

5.3.1. Agenda of International Governmental Organizations

UN General Assembly adopted on March 24th 2015 a resolution calling on the Human rights council to establish a special mandate on privacy. The Special Rapporteur on Right to Privacy had been created for the mandate 3 years period.[31] One of many mandates is to illustrate the problems and propose a recommendation to promote the progressive realization of Personal Data Protection, including principles and best practices at the national, regional and international levels. This Special Rapporteur appointment decision is the direct result of the turning point triggered by US Global Internet Mass Surveillances.

A year before resolution A/HRC/28/L.27 was approved, the Internet Rights and Principles Coalition (IRPC) Charter of Human Rights and Principles for the Internet was adopted, Contribution to the Net Mundial Global Multi-stakeholder Meeting on the Future of Internet Governance, 23-24 April 2014.[32]It was presented under the working group of United Nations Internet Governance Forum (IGF) which the representatives of States and International Civil Organization are participated.

The output of IGF efforts is the Charter launched by Internet Rights and Principles Dynamic Coalition, an open network of individuals and organizations, which contains 10

[31] UN. *A/HRC/28/L.27*. 24 Mar. 2015, pp. 3-4.

[32] UN Internet Governance Forum (IGF). *The Internet Rights and Principles Dynamic Coalition*. 2014, Introduction p. 1.

principles and 20 rights for Internet users. The Charter includes the Right to Privacy and Data Protection in Principle 5 on Privacy and Data protection and the 9th Right to Digital Data Protection.

The charter recognizes the important of PRIVACY AND DATA PROTECTION by confirming that everyone has the right to privacy online. This includes freedom from surveillance, the right to use encryption, and the right to online anonymity. Everyone also has the right to data protection, including control over personal data collection, retention, processing, disposal and disclosure.[33]

Furthermore, the Charter reaffirms the Right to Digital Data Protection as enshrined in Article 12 of the UDHR everyone has the right to privacy. It recalls the important aspect of this right is that everyone has the right to protection of personal data concerning him or her. In specific in the Internet, the right to protection of personal data includes:[34]

a) Protection of Personal data: Fair information practices should be enacted into national law to place obligations on companies and governments who collect and process personal data, and give rights to those individuals whose personal data is collected.

b) Obligations of data collectors: The collection, use, disclosure and retention of personal data must all meet transparent privacy-protecting standards. Everyone has the right to exercise control over the personal data collected about them and its usage. Whoever requires personal data from persons, shall request the individual's informed consent regarding the content, purposes, storage location, duration and mechanisms for access, retrieval and correction of their personal data. Everyone has a right to access, retrieve and delete the personal data collected about them.

c) Minimum standards on use of personal data: When personal information is required, only the minimum data necessary must be collected and for the minimum period of time for which this is required. Data must be deleted when it is no longer necessary for the purposes for which it was collected. Data collectors have an obligation to seek active consent and to notify people when their information has been forwarded to third parties, abused, lost, or stolen. Appropriate security measures shall be taken for the protection of personal data

[33] Ibid, p. 7.

[34] Ibid, p. 19.

stored in automated data files against accidental or unauthorized destruction or accidental loss as well as against unauthorized access, alteration or dissemination.

d) Monitoring by independent data protection authorities: Data protection should be monitored by independent data protection authorities, which work transparently and without commercial advantage or political influence.

The principles as seen in the Charter of Human Rights and Principles for the Internet have shown the relevant with the legal regime in Chapter 2: old regime, and 4: new regime, which had been reviewed before. In part a) Protection of Personal data, it has the same common ground with legal approval and contents of data subjects 'rights as every instrument expected their State Parties to undertake. While part b) Obligation and c) Minimum Standard are relevant with the basic duty and data processing requirements of either old and new regime on protection of personal data. The last part d), try to create the competence body to regulate the instrument as well as other instruments desire. The Charter is the great expectation of International Community to create a comprehensive legal baseline for further drive to create common Universal/International instrument in the near future.

5.3.2. Projects of International Civil Society Movements

There are two important and interesting movements relating protection of personal data globally: the International Conference of Data Protection and Privacy Commissioners (ICDPPC) and the International Internet Coalition (IIC).

The International Conference of Data Protection and Privacy Commissioners (ICDPPC is a global forum of field experts and the highest authorities and institutions guaranteeing data protection and privacy.[35] The ICDPPC is dedicated to identifying major challenges in the realm of privacy and data protection, and its main achievement in this field has been "The International Standards on the Protection of Personal Data and Privacy" (Madrid Resolution 2009).

In 2009, the ICDPPC experts' meetings took place in Barcelona in January 2009 and Bilbao in June 2009, as well as the annual ICDPPC conference held in Madrid in November of 2009. At the ICDPPC experts' meetings in January and June 2009, participants discussed

[35] ICDPPC. *Madrid Resolution*. 2009, presentation.

the development of a resolution on international privacy standards. In November 2009, the Joint Proposal for International Standards on the Protection of Privacy with Regard to the Processing of Personal Data (or "the Madrid Resolution") was unveiled.[36] In Madrid, on 6th of November 2009, The Joint Proposal on International Standards for the Protection of Privacy was positively welcomed by Protection Authorities of 50 countries gathered within the framework of the 31st International Conference of Data Protection and Privacy, through the adoption of the "Madrid Resolution",[37] The multiple approaches possible in the protection of personal data, integrating legislation from all five participating continents.

Madrid Resolution is a Non-Legal Binding Instrument, According to the director of the AEPD, the Madrid Resolution will, thus, become a "soft law" tool, widely demanded mainly by international companies, in order to respect the minimum data protection needs of citizens worldwide. [38]

The text's purpose is to define a series of principles and rights that guarantee the effective protection of privacy at an international level, as well as to ease the international flow of personal data, essential in a globalized world. Among the basic principles that must govern the use of personal data, and which have inspired the document, it founded those of loyalty, legality, proportionality, quality, transparency and responsibility; all of them are common to the different existing legal texts in the various regulations on the matter and enjoy wide consensus in their corresponding geographical, economic or legal application environments.[39]

The Joint Proposal of International Privacy Standards includes, in addition, in its articulation, the need for the existence of supervisory authorities, and for the different states to cooperate and coordinate their activities. In addition with the set of rights such as access, rectification, cancellation and objection and the way in which they can be exercised.[40] It also includes critical issues such as:

[36] ICDPPC. *Madrid Resolution.* 2009.

[37] Ibid, pp. 29-30.

[38] Ibid, purpose.

[39] Ibid, Explanatory Note p.32.

[40] Ibid, pp. 19, 30 - 31.

Rights of Data Subject: The document defines sensitive data as that data that affects the most intimate side of a person or whose misuse can originate an illegal or arbitrary discrimination, or may imply a severe risk for the said person, [41]and other legal terms relevant to Personal Data Protection.[42]

Obligation of Duty Bearer: It ensures security of personal data, through those measures that are considered appropriate in each case, or confidentiality, which affects the controller as well as anyone who participates in any of the stages in which personal data is managed.[43] In addition, in includes the requirements that must be met for the legal collection, preservation, use, revelation or erasure of personal data, such as, for example, the prior obtaining of the free, unequivocal and informed consent from the person providing the data. [44] A general rule, international personal data transfers may be performed when the State to which the data is transferred offers, at least, the level of protection foreseen in the document; or when whoever wants to transfer the data can guarantee that the addressee will offer the required level of protection, for example, through appropriate contractual clauses. [45]

Implementation Mechanism: The pro-active measures, which encourages States to promote a better compliance with the applicable laws regarding data protection matters, through instruments such as the establishment of procedures aimed at the prevention and detection of offences, or the periodic offering of awareness, education and training programs. [46]

The resolution of corporate was supported by the Council of Europe. A group of 10 large companies (Oracle, Walt Disney, Accenture, Microsoft, Google, Intel, Procter & Gamble, General Electric, IBM and Hewlett-Packard) have signed a declaration in which they proudly welcome the initiative from the 31st International Conference.[47]

[41] Ibid, p. 16.

[42] Ibid, p. 7.

[43] Ibid, p. 22.

[44] Ibid, pp. 19-20.

[45] Ibid, p. 17.

[46] Ibid, pp. 24 - 27.

[47] "Data protection authorities from over 50 countries approve the "Madrid Resolution" on international privacy standards." *The 31st International Conference of Data Protection and Privacy,* www.privacyconference2009.org/media/notas_prensa/common/pdfs/061109_estandares_internacionales_en.pdf. Accessed 20 Feb. 2015.

In this declaration, the signing companies encourage Data Protection and Privacy Authorities to continue insisting and collaborating in the development of transparent systems that will allow the taking on of responsibilities and that will provide accurate information to the citizen, granting him/her the power to decide. Also, recently, the group on data protection from the Council of Europe, in a meeting celebrated just a few months ago, decided to support the initiative approved by the data protection authorities to adopt these international privacy standards and, with this, contribute to expand and promote a worldwide framework for the protection of privacy. [48]

The Agencia Española de Protección de Datos (AEPD) as the main supporter to 2009 Privacy Conference established a Working Group which has been working since then to elaborate this Joint Proposal, assuming that all these common principles and approaches contribute valuable elements to the defense and promotion of privacy and personal information, with the aim of extending those criteria and incorporating applicable solutions.[49] The Working Group has been undertaking research and drafting further resolution for late years.

The second most interesting Non-Governmental Movement initiative related to International Personal Data Protection, as mentioned at the beginning of this section, is The International Internet Coalition (IIC), more than 600 Civil Society Organizations around the world until May 2014,[50] have endorsed the International principles on State Surveillance. The Principles officially launched at the UN Human Rights Council in Geneva in September 2013 by the host of Germany. The FINAL VERSION May 2014 has been posted at the Official Website of the Office of United Nations High Commissioner on Human Rights. The document pursues state to regard these principles:

Principle 1 LEGALITY: Any limitation to human rights must be prescribed by law. The State must not adopt or implement a measure that interferes with these rights in the absence of an existing publicly available legislative act, which meets a standard of clarity and

[48] Ibid.

[49] ICDPPC. *Madrid Resolution*. 2009, p. 34.

[50] International Coalition of Civil Organizations on Internet Freedom. *International Principles on the Application of Human Rights to Communications Surveillance*: *Background and Supporting International Legal Analysis*. 2014, Preamble.

precision that is sufficient to ensure that individuals have advance notice of and can foresee its application.[51]

Principle 2 LEGITIMATE AIM: Laws should only permit Communications Surveillance by specified State authorities to achieve a legitimate aim that corresponds to a predominantly important legal interest that is necessary in a democratic society. [52]

Principle 3 NECESSITY: Surveillance laws, regulations, activities, powers, or authorities must be limited to those which are strictly and demonstrably necessary to achieve a legitimate aim. [53]

Principle 4 ADEQUACY: Any instance of Communications Surveillance authorized by law must be appropriate to fulfill the specific Legitimate Aim identified. [54]

Principle 5 PROPORTIONALITY: Communications surveillance should be regarded as a highly intrusive act that interferes with human rights threatening the foundations of a democratic society. [55]

These principles require a State, at a minimum, to establish the following measures:

Principle 6 COMPETENT JUDICIAL AUTHORITY: Determinations related to Communications Surveillance must be made by a competent judicial authority that is impartial and independent. [56]

Principle 7 DUE PROCESS: Due process requires that States respect and guarantee individuals' human rights by ensuring that lawful procedures that govern any interference with human rights are properly enumerated in law, consistently practiced, and available to the general public.[57]

Principle 8 USER-NOTIFICATION AND THE RIGHT TO EFFECTIVE REMEDY: Those whose communications are being surveilled should be notified of a decision

[51] Ibid, paras. 14-18.

[52] Ibid, paras. 18-20.

[53] Ibid, para. 20.

[54] Ibid, para. 21.

[55] Ibid, para. 22.

[56] Ibid, paras. 22-23.

[57] Ibid, para. 24.

authorizing Communications Surveillance with enough time and information to enable them to challenge the decision or seek other remedies and should have access to the materials presented in support of the application for authorization. States should enact legislation criminalizing illegal Communications Surveillance by public or private actors. [58]

Principle 9 TRANSPARENCY: States should be transparent about the use and scope of Communications Surveillance laws, regulations, activities, powers, or authorities. [59]

Principle 10 PUBLIC OVERSIGHT: States should establish independent oversight mechanisms to ensure transparency and accountability of Communications Surveillance. [60]

Principle 11 INTEGRITY OF COMMUNICATIONS AND SYSTEMS: In order to ensure the integrity, security and privacy of communications systems, and in recognition of the fact that compromising security for State purposes almost always compromises security more generally, States should not compel service providers or hardware or software vendors to build surveillance or monitoring capability into their systems, or to collect or retain particular information purely for State Communications Surveillance purposes.[61]

Principle 12 SAFEGUARDS FOR INTERNATIONAL COOPERATION: In response to changes in the flows of information, and in communications technologies and services, States may need to seek assistance from foreign service-providers and States. [62]

Principle 13 SAFEGUARDS AGAINST ILLEGITIMATE ACCESS: States should also enact laws providing that, after material obtained through Communications Surveillance has been used for the purpose for which information was given, the material must not be retained, but instead be destroyed or returned to those affected. [63]

However, it is a non-legal binding document.

Those three initiatives from the UN Internet Governance Forum (IGF), the International Conference of Data Protection and Privacy Commissioners (ICDPPC) and the International Civil Society Coalition have given the prospect to draft and adopt an

[58] Ibid, paras. 25-26.

[59] Ibid, para. 27.

[60] Ibid, para. 28.

[61] Ibid, paras. 28-29.

[62] Ibid, paras. 29-31.

[63] Ibid, paras. 31-33.

International Legal Instrument to regulate relevant organizations which collect, process and transfer of personal data. For supporting that goal, further studies in detail to prevent the illegitimate wrongdoings must be done on specific issue.

There are some productive benchmarks from the EU-US legal regime could be adapted to assist the draft of International/Universal instrument on protection of personal data in cyberspace. Because of the long negotiation and drafting process of EU and the further reconciliation in complicated issues with the US, the set of rules from EU-US regime would be the best model for comparative legal studies. The comprehensive benchmarks in 12 issues will be synthesis below.

5.4. Comparative Synthesis from the perspective of the EU-US E-Market regime

Referencing to the 2016 EU and EU-US reformation process, this reform has tried to answer the same challenges that international community has confronted the worldwide internet users hold the nationality of some other countries which are not US citizen and the most of Mega IT Corporation who offer services in cyberspace are US Entities. The case of EU and US would be a suitable case study to be observed.

The legal scheme implemented for the trans-Atlantic exchange of personal information is, in effect, a craftwork legal solution constructed on a bi-lateral basis. As it has been already analyzed, it includes the EU GDPR and EU-US Data Privacy Shield for fundamental personal data exchanges and EU Directive on Criminal Matters and EU-US Umbrella Agreement for protection of natural persons with regard to criminal matters.

The EU-US regime covers 2 areas of E-Market which have persuasive factors: Most of competent organizations who may violate rights of data subject are under US jurisdiction such as IT Corporations and State Authorities, Their E-Market is highly attractive because the ratio of internet penetration is very high and the consumers have online purchasing power. Besides, the standard EU has set will oblige trade-counterparts around the world if they want to access EU E-Market, the regime would expand to them ultimately. Whereas, Non-EU countries might want to conform their legal policy to meet EU Standard, without separately negotiate mutual agreement, by initiating the International Regime or establishing the Universal Standard to harmonize Global E-Market regime.

To be more specific to EU-US predominant case study, on each side of the Atlantic, largely different provisions govern the respective processing once personal data have been transmitted. The EU-US example is a powerful case for the advantages of introducing a single international data protection instrument that would has saved both parties from a multitude of complex and hard-to follow arrangements and, ultimately, a significant waste of resources in the respective negotiation and drafting processes.[64] Nonetheless, these set of EU-US instruments have potential to set standard for International Data Protection Initiatives and other regional organizations since it covers vast majority states in the regime of liberal market economy countries.

5.4.1. Individual's Right to Personal Data Protection

EU internet users can represent internet user in other part of the world since they entitle the same rights approved by Universal Human Rights instruments such as UN Declaration on Human Rights. Furthermore, vast majority countries are State Parties of ICCPR. Thus what EU Nationals gained from US Entities should be provided to other internet users. Besides, the protection can bring in confident to online customer and generate more prosperity to Global E-Market. The personal data protection reform will allow people to regain control of their personal data. Two-thirds of Europeans (67%), according to a recent Eurobarometer survey, stated they are concerned about not having complete control over the information they provide online. Seven Europeans out of ten worry about the potential use that companies may make of the information disclosed.[65] The International data protection reform will strengthen the right to data protection, which is a fundamental right in the World Wide Web, and allow e-consumer/internet citizen to have trust when they give their personal data out.

[64] De Hert, Paul and Vagelis Papakonstantinou. "Three Scenarios for International Governance of Data Privacy: Towards an International Data Privacy Organization, Preferably a UN Agency." *ISJLP*, vol. 9, 2013, p. 294.

[65] European Commission. *Agreement on Commission's EU data protection reform will boost Digital Single Market*. Press release, Brussels, 15 Dec. 2015.

5.4.1.1. Legal Approval of Personal Data Protection

The international regime must introduce a single set of rules, to be applied uniformly across the world. While issues of interpretation can never be ruled out, even with regard to the same set of rules, this will eliminate the incentives and possibility for companies to artificially and strategically try to attach themselves to certain Member State with either more lenient rules or, more importantly, implementation deficits due to an inactive national data protection authority. It does not mean abandoning the territoriality principle in relation to competence altogether but it contains novel and inventive procedures for cooperation, mutual assistance, joint operations and a consistency mechanism.[66] One single e-market, one regime: The regulation will establish one single set of rules which will make it simpler and cheaper for companies to do business in the market.

The international regime will bring clear rules for better cooperation, Global Single common rules on data protection will enable police and criminal justice authorities to cooperate more effectively with each other based on mutual trust and legal certainty.[67] However, International Regime for data protection in criminal matters should not provide for a general data protection framework in the context of criminal law because of the nature of domestic type of criminal procedure implementation, voluntary/diversity chosen, and because the Regime for data protection in the police and justice sectors just sets minimum harmonization rules which open wide discretion to the Member States for its own fit.

The problem may arise from the architecture of the reform package on data protection itself, whether the establishment of Hard law or Soft law international instrument. The level of protection in the Soft law for data protection in the police and justice sectors should be lower than the one laid down in the Data Protection in General. The option of a Hard law also covering the area of criminal law enforcement might be unacceptable for most State Parties; that is why finally EU decided to adopt a Soft law with the same substance as the Regulation in General, but subject to the relevant limitations and exceptions,[68] and leaving more space for domestic implementation. On the contrary, international instrument

[66] EU. *General Data Protection Regulation.* 2016, Articles 60-76.

[67] European Commission. *EU Data protection reform on track: Commission proposal on new data protection rules in law enforcement area backed by Justice Ministers*. Press release, Luxembourg, 9 Oct. 2015.

[68] Maesa, Costanza D F. *Balance Between Security and Fundamental Rights Protection: an Analysis of The Directive 2016/680 for Data Protection in The Police and Justice Sectors and the Directive 2016/681 on the Use of Passenger Name Record (PNR).* 2016, p. 11.

for general personal data protection should be in a Hard Law form since it obliges IT Corporation, transfer data for economic purpose, in the prospect Single Global E-Market.

5.4.1.2. Definition and Scope of Personal Data Protection

The International Regime must apply to companies established outside the party territory that process data related to the activities of State Party's organizations. Non-Party companies will also be subject to the Treaty if they target State Party's residents by profiling, or proposing products or services.[69] There must be a single set of rules on data protection, directly applicable in all international party states, thereby mitigating the current fragmentation of national data protection laws and implementation by using the driving force of WTO GATTS article XX on personal data protection as a base. To accomplish, establishment of common rules on State Party territory, companies based outside of party's territory will have to apply the same rules when offering services in the member state.

The International Regime for data protection on criminal matters should have two faces. On one hand, it is innovative as its scope is now intended to cover all personal data processing undertaken in the context of police and judicial cooperation in criminal matters,[70] regardless of whether the processing takes place within or outside national borders. On the other hand, criminal law enforcement authorities, therefore, will no longer have to apply different sets of data protection rules depending on the origin of the personal data. The term should avoid different interpretations and provide a clear delimitation of the tasks of the scope of the regime.

By using EU GDPR and Directive on Criminal Matters, as baseline against criticism of its broad definition of "personal data", there is considered necessary in order to "future-proof" the instruments in the context of rapid technological change. Under the GDPR, any information related to a natural person who can be identified by ways likely to be used by the controller would be caught under the definition. In Directive, "personal data" is defined with respect to a person who is or can be directly or indirectly identified, particularly by

[69] "European General Data Protection Regulation finally adopted: are you ready?." *Data Protection, Privacy and Security Alert (US),* DLA Piper, 14 Apr. 2016, p. 1.

[70] Maesa, Costanza D F. *Balance Between Security and Fundamental Rights Protection: an Analysis of The Directive 2016/680 for Data Protection in The Police and Justice Sectors and the Directive 2016/681 on the Use of Passenger Name Record (PNR).* 2016, p. 10.

"reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity." Thus, the GDPR allows for the possibility of technological advances leading a controller to identify an individual through other sorts of data, which would then be protected as "personal data" under the GDPR.[71] Thus the definition in International Regime may use this definition to develop their term.

5.4.1.3. Content of Data Subjects' Right to Data Protection

The new rules must address the concerns by strengthening the existing rights and empowering individuals with more control over their personal data. Most notably, these include:

- **A clarified "right to be forgotten" or "right to erasure"**: allowing data subjects the right to require a controller to delete data files relating to them if there are no legitimate grounds for retaining it;[72]
- **The right to breach notification:** For example, companies and organizations must notify the national supervisory authority of serious data breaches as soon as possible so that users can take appropriate measures[73];
- **Right to be informed and access**: make it easier access of data subject to their own data. Individuals will have more information on how their data is processed and this information should be available in a clear and understandable way[74];
- **Right to access and rectification** - Any individual will be entitled to access their personal data – subject to certain conditions, given the law enforcement context – and request it to be corrected if it is inaccurate[75];

[71] Voss, W Gregory. "Preparing for the Proposed EU General Data Protection Regulation: With or without Amendments." *Bus. L. Today*, 2012.

[72] "European General Data Protection Regulation finally adopted: are you ready?." *Data Protection, Privacy and Security Alert (US),* DLA Piper, 14 Apr. 2016, p. 2.

[73] European Commission. *Agreement on Commission's EU data protection reform will boost Digital Single Market*. Press release, Brussels, 15 Dec. 2015.

[74] Ibid.

[75] European Commission. *Questions and Answers on the EU-US data protection "Umbrella agreement"*. Brussels, 1 Dec. 2016, p. 1.

- **Data portability**: Organizations must ensure data subjects can easily transfer their data files from one service provider to another.[76]

The Universal Regime must protect citizens' fundamental right to data protection when data is used by law enforcement authorities, it should be processed lawfully, fairly, and only for a specific purpose. All law enforcement processing under mandate must comply with the principles of necessity, proportionality and legality, with appropriate safeguards for the individuals. Supervision is ensured by independent national data protection authorities and effective judicial remedies must be provided.[77]

5.4.1.4. Exception to the exercise of Right to Personal Data Protection

Even in emergency situation, the clear safeguards and transparency obligations on government access is needed, The universal regime must set conditions for government that has given the assurance that the access of public authorities for law enforcement and national security is subject to clear limitations, safeguards and oversight mechanisms. Everyone in the jurisdiction of the treaty will benefit from redress mechanisms in this area.[78] The International Community must rule out indiscriminate mass surveillance on personal data transferred to third part under the International Agreement/Treaty. The requirement to Office of National Intelligence Authority for further clarification that bulk collection of data could only be used under specific preconditions and needs to be as targeted and focused as possible.[79] The International Treaty must detail the conditions and safeguards in place for the use of data under such exceptional circumstances, emergency situation.

The Personal Data Protection policies of self-certified companies should include information on the extent to which National law allows Public Authorities to collect and process data transferred under the Data Sharing Agreement. In particular companies

[76] "European General Data Protection Regulation finally adopted: are you ready?." *Data Protection, Privacy and Security Alert (US),* DLA Piper, 14 Apr. 2016, pp. 1-2.

[77] European Commission. *EU Data protection reform on track: Commission proposal on new data protection rules in law enforcement area backed by Justice Ministers*. Press release, Luxembourg, 9 Oct. 2015.

[78] European Commission. *European Commission launches EU-U.S. Privacy Shield: stronger protection for transatlantic data flows*. Press release, Brussels, 12 Jul. 2016.

[79] European Commission, *EU Commission and United States agree on new framework for transatlantic data flows: EU-US Privacy Shield.* Strasbourg, 2 Feb. 2016.

should be encouraged to indicate in their policies when they apply exceptions to the Principles to meet national security, public interest or law enforcement requirements. [80] It is crucial that the national security exception foreseen by the Data Sharing Agreement is used only to an extent that is strictly necessary to handle such emergency situation proportionately.

The laws must be sufficiently precise to indicate to citizens in what circumstances and on what terms the public authorities are empowered to gather information on their private lives and make use of it. Such information should "be accessible to the person concerned and foreseeable as to its effects", which means that it must be "formulated with sufficient precision to enable any individual – if need be with appropriate advice – to regulate his conduct".[81]

Ultimately, there is a need for establishment an oversight/redress possibility in the area of national intelligence for individuals through an independence quasi-judicial mechanism, Ombudsperson, within the Data Supervisory Authority.

5.4.2. Obligation of the Data Controller and Data Processor

Can US IT Corporation cases in EU be used with other parts of the world? This question would be the main curiosity of internet users and technocrats around the world. In today's digital economy, personal data has acquired enormous economic significance, in particular in the area of big data or metadata collected and processed by Giant US IT Corporation. By unifying Europe's rules on data protection, lawmakers are creating a business opportunity and encouraging innovation, not only for EU IT Corporations but also US ones. Creating clear and predictable obligation would be preferable for IT Corporation because the can plan how to do business in any E-Market worldwide. However, the other approach on adopting International instrument to cover the personal data protection related activities would be beneficial in term of setting common rule for Global E-Market. Hence, promoting the personal data protection in the area of law enforcement should be at stake as well.

[80] European Commission, *Restoring Trust in EU-US data flows - Frequently Asked Questions*. Brussels, 27 Nov. 2013, p. 4.

[81] Maesa, Costanza D F. *Balance Between Security and Fundamental Rights Protection: an Analysis of The Directive 2016/680 for Data Protection in The Police and Justice Sectors and the Directive 2016/681 on the Use of Passenger Name Record (PNR)*. 2016, p. 11.

5.4.2.1. Basic Duty of Data Controller and Processor

The Universal Regime must open-up diverse rules might fit for innovation. The rules must guarantee that data protection safeguards are built into products and services from the earliest stage of development (Data protection by design). Privacy-friendly techniques such as "pseudonomysation" will be encouraged, to reap the benefits of big data innovation while protecting privacy.[82] Moreover, the policy which put personal data protection as a fundamental ground for Data Controller/Processor (Data protection by default) would be better for enlargement the global e-market.

The encouragement of transparency governance will make organizations have increased responsibility and accountability on how they control and process personal data. The needs of increased transparency obligations will oblige them to make privacy notices which include much more detailed information.[83] Public and Private organizations processing data on behalf of other companies/authorities will be required to comply with a number of specific personal data protection related obligations. They must be liable to sanctions if they fail to meet the criteria.

The verified companies and certified authorities should publicly disclose their privacy policies. The Privacy policies of verified organizations' websites should always include a link to the National Data Protection Authority website which lists all the 'current' members of the scheme. The policy should entail personal data conditions of any contracts they conclude with third party e.g. subcontractors, cloud computing services.[84] Obvious emblems on the website of the National Data protection Authority all companies which are current members of the scheme and the watching list of threaten organization.

The controller and the processor must appoint a data protection officer (DPO) who has expert knowledge on data protection law.[85] The DPO will report to the highest

[82] European Commission. *Agreement on Commission's EU data protection reform will boost Digital Single Market*. Press release, Brussels, 15 Dec. 2015.

[83] DLA Piper. "EU General Data Protection Regulation - Key Changes." www.dlapiper.com/en/uk/focus/eu-data-protection-regulation/key-changes/. Accessed 14 Jan. 2017, p. 1.

[84] European Commission. *Restoring Trust in EU-US data flows - Frequently Asked Questions*. Brussels, 27 Nov. 2013, p.4.

[85] Voss, W Gregory. "Preparing for the Proposed EU General Data Protection Regulation: With or without Amendments." *Bus. L. Today*, 2012.

management level and make a periodic report of risks and threats they have found and warned.

5.4.2.2. Condition and Requirement of Data Collection and Processing

The Universal Regime should require a more active consent based model to support lawful processing of personal data; wherever consent is required for data to be processed, consent must be explicit, rather than implied.[86]

The stronger protection for data processing that presents "specific risks," such as that which involves certain sensitive information, triggers the requirement for a data protection impact assessment. This assessment, which must describe the processing foreseen, shall assess risks to data subject rights, means of addressing these and those designed to protect personal data, and demonstrate compliance with the Regime. The data protection impact assessment is to be accomplished by or on behalf of the controller,[87] and the International Data Authority may adopt further criteria by delegated acts.

The common international regime is needed to slash red tape for state authorities, Police and criminal justice authorities will no longer have to apply different sets of data protection rules according to the origin of the personal data, saving time and budget. The new rules will apply to both domestic processing and cross-border transfers of personal data. Having more harmonized laws in all Treaty Party States will make it easier criminal enforcement officer to coordination.[88] However, the rules in the legal instrument must take account of the specific requirements of the judicial and criminal justice sector and respect the different legal cultures in State Parties.

Nonetheless, data controllers or processors will be required to report data breaches to the relevant data protection agency "without undue delay," and where feasible of notice of such a breach. Notifications after such time period will need to be justified. Processors must inform controllers of breaches immediately after their establishment, and the

[86] DLA Piper. "EU General Data Protection Regulation - Key Changes." www.dlapiper.com/en/uk/focus/eu-data-protection-regulation/key-changes/. Accessed 14 Jan. 2017, p. 1.

[87] Voss, W Gregory. "Preparing for the Proposed EU General Data Protection Regulation: With or without Amendments." *Bus. L. Today*, 2012.

[88] European Commission. *EU Data protection reform on track: Commission proposal on new data protection rules in law enforcement area backed by Justice Ministers*. Press release, Luxembourg, 9 Oct. 2015.

controller must inform the data subject if the breach will likely have a negative effect on the protection of the subject's personal data or privacy, unless the controller can prove that the data was rendered "unintelligible" to unauthorized persons.[89]

5.4.2.3. Data Security

There are 2 main measures that Universal Regime should implant. Firstly, Risk-based approach: the rules must avoid a burdensome one-size-fits-all obligation and rather tailor them to the respective risks. Secondly, Impact Assessments: IT Corporations will have obligation to carry out an impact assessment no matter how low risk there is.[90] The development of apparel Cybersecurity Strategy of many regional organizations and economic bloc may support the same mission to maintain stability of Internet and trust among online citizen. Thus, the Privacy impact assessment (PIA) will become a mandatory prerequisite before processing personal data for operations that are likely to present higher privacy risks to data subjects due to the nature or scope of the processing operation. [91]

The rule must demand organizations to notify the local supervisory authority, and (in some cases) data subjects, of significant data breaches. [92] There must be an Authority to announce Information in case of data security breaches. A mechanism will be put in place so as to ensure notification of data security breaches to the competent authority and, where appropriate, the data subject.[93]

5.4.2.4. Data Retention

This Universal Regime should complement existing EU, EU-US and State Parties agreements between IT Corporation and law enforcement authority and among law

[89] Voss, W Gregory. "Preparing for the Proposed EU General Data Protection Regulation: With or without Amendments." *Bus. L. Today*, 2012.

[90] European Commission. *Agreement on Commission's EU data protection reform will boost Digital Single Market*. Press release, Brussels, 15 Dec. 2015.

[91] DLA Piper. "EU General Data Protection Regulation - Key Changes." www.dlapiper.com/en/uk/focus/eu-data-protection-regulation/key-changes/. Accessed 14 Jan. 2017, p. 2.

[92] Ibid.

[93] European Commission. *Questions and Answers on the EU-US data protection "Umbrella agreement"*. Brussels, 1 Dec. 2016, p. 1.

enforcement authorities themselves. Since it creates clear harmonized data protection rules and set a high level of protection for future agreements in the field of Data Retention; purposes, time period and competent authority.[94] The International Instrument should provide the following protections to make sure that everyone's data are protected when collected, processed and shared the retained data between organizations.

The rules must give clear limitations on data use. Personal data may only be used for the purpose of preventing, investigating, detecting or prosecuting criminal offences, and may not be processed beyond compatible purposes. Organization must be subject to the prior consent of the competent authority of the country which had originally retained personal data. The limit of Retention periods must be written obviously**,** Individuals' personal data may not be retained for longer than necessary or appropriate. These retention periods will have to be published or otherwise made publicly available. The decision on what is an acceptable duration must take into account the impact on people's rights and interests.[95]

5.4.2.5. Data Transfer

The tightening of conditions for the onward transfers of data to third parties will guarantee the same level of protection in case of a transfer from a registered company[96] must be prerequisite by International Regime. The Track and Trace-back system on the verified organizations (Accountability Principle – Nationality based) should be brought in to the Regime and make it a liability for Nationality State of the Head Quarter of such organizations to control their activities.

The International Regime should provides for general principles and clear rules for the transfer of personal data by police and criminal justice authorities outside the treaty mandate, to ensure that these transfers take place with an adequate level of data protection (Adequacy Principle – Territorial based). The international regime must provide

[94] European Commission. *Questions and Answers on the EU-US data protection "Umbrella agreement"*. Brussels, 1 Dec. 2016, p. 1.

[95] Ibid.

[96] European Commission. *European Commission launches EU-U.S. Privacy Shield: stronger protection for transatlantic data flows*. Press release, Brussels, 12 Jul. 2016.

robust rules on personal data exchanges at national, regional and international level[97] so it would be easier and safer international cooperation.

5.4.3. Implementation of Personal Data Protection

The implementation phase has started: International community will countdown years to ensure data processing activities are in line with the newly adopted rules of big liberal free market bloc like EU, US. This means International cooperation needing to act now. It makes sense to undertake a snapshot assessment of the impact of the EU and EU-US Regime on the IT Corporation and Intelligence Authority, so that steps can be taken to identify and implement any necessary changes. Any assessment ought to be tailored to the specific needs of the data subjects but is likely to focus on key issues such as appointment of a Data Protection Authority/Officer and Monitoring body or providing individual redress and putting a sanction on non-compliance organization. Nonetheless, even EU new regime, it permits national legislators to diverge to a considerable extent from certain of the GDPR's provisions, including the provisions covering the situation at issue on conflict of applicable law in different jurisdictions. Consequently, the scenario will come down to the critical question on, why leaving the implementation to domestic court around the world is not enough? And should other citizen have the same redress rights as US&EU Nationals? Since the main service providers in cyberspace are US IT Corporation and the most dangerous threats are coming from US National Security Agency.

5.4.3.1. Monitoring Body and Supervisory Authority

The Universal Regime should contain novel and inventive procedures for cooperation, mutual assistance, joint operations and a consistency mechanism. Moreover, all national data protection authorities have to present activity reports periodically, which will be published. All of this aims at ensuring consistency in the application of the regulation by the national authorities. It also seeks to encourage the national supervisory authorities to take an active stance and aims to mobilize all of them to an optimal extent. It must provide the

[97] European Commission. *EU Data protection reform on track: Commission proposal on new data protection rules in law enforcement area backed by Justice Ministers*. Press release, Luxembourg, 9 Oct. 2015.

harmonized rule, to apply in uniformity by supervisory authorities across the world to eliminate the problems on fragmented territories[98] including the provisions covering the situation at issue on conflict of applicable law in different jurisdictions.

The regime must support the better cooperation between law enforcement authorities with the new Data Protection Directive for Police and Criminal Justice Authorities, law enforcement authorities in Party States will be able to exchange information necessary for investigations more efficiently and effectively, improving cooperation in the fight against terrorism and other serious crime among state party. The Data Protection on Criminal Matters part will take account of the specific needs of legal enforcement.[99] Moreover, it must respect the different legal traditions in State Parties and is fully in line with the International Treaties of Human Rights.

The needs of establishment the One-stop-shop, businesses and individuals will only have to deal with one single supervisory authority. Furthermore, a global data protection authority which will act as the lead regulator for compliance issues among the State Party, where the organization has multiple points of presence around the world.

5.4.3.2. Redress Mechanism and Individual Remedy

The Universal Regime must push forward a stronger remedy mechanism, better protection of citizens 'data Individuals' personal data will be better protected, when processed for any law enforcement purpose including prevention of crime. It must protect everyone, regardless of whether they are a victim, criminal or witness. Supervision is ensured by independent national data protection authorities, and effective judicial remedies must be provided. The Data Protection on Criminal Matters must provide clear rules for the transfer of personal data by law enforcement authorities outside the territory, to ensure that the level of protection of individuals guaranteed in the regimes' jurisdiction is not undermined.[100] The

[98] Gryffroy, Pieter. *Taking a look at two cases in the margin of the CJEU's "Privacy Spring", before and after the General Data Protection Regulation: Weltimmo and Bara.* 2016, p. 4.

[99] European Commission. *Agreement on Commission's EU data protection reform will boost Digital Single Market*. Press release, Brussels, 15 Dec. 2015.

[100] European Commission. *Agreement on Commission's EU data protection reform will boost Digital Single Market*. Press release, Brussels, 15 Dec. 2015.

oversight body of such mission should be created in a form of independence Quasi-Judicial organization or impartial court.

Even trying to create international regime but it is the duty of the national courts in cooperation with the international instrument on personal data protection to ensure the uniform interpretation of the International Personal Data Protection provisions[101] throughout the territory of state party.

The One-stop-shop for individual complainant as mentioned above would be important path for effective remedy. This is estimated to save billions per year and provide greater opportunity for internet user to contact with oversight mechanism. The appointment of assistant or attorney for local victim to appeal in court or One-stop-shop must be initiated for free or pro-bono basis (founding trust fund to collect budget from the income of processing organizations or from fines).

There must be an effective and accessible data personal protection remedy for individual internationally. The accessible and affordable dispute resolution mechanisms is Ideal, the complaint will be resolved by the company/authority itself; or free of charge Alternative Dispute resolution (ADR) solutions will be offered. Individuals can also go to their national Data Protection Authorities (DPA), who will work with the international Data Protection Authority to ensure that complaints by State Party's citizens are investigated and resolved. If a case is exhaustion of domestic remedy, as a last resort there will be an arbitration mechanism.[102] The National DPA should monitor more systematically ADR providers regarding the transparency and accessibility of information they provide concerning the procedure they use and the follow-up they give to complaints.[103] Furthermore, redress possibility in the area of national security for State Party citizen must be handled by an Ombudsperson independent from the national intelligence services who involved.

However, the most critical part would be the judicial redress and enforceability of rights of the Aliens in other jurisdiction, for example Spanish victim in US

---

[101] Gryffroy, Pieter. *Taking a look at two cases in the margin of the CJEU's "Privacy Spring", before and after the General Data Protection Regulation: Weltimmo and Bara.* 2016, p. 3.

[102] European Commission. *European Commission launches EU-U.S. Privacy Shield: stronger protection for transatlantic data flows*. Press release, Brussels, 12 Jul. 2016.

[103] European Commission. *Restoring Trust in EU-US data flows - Frequently Asked Questions*. Brussels, 27 Nov. 2013, p. 4.

Court. Since Foreign Citizens will have the right to seek judicial redress before Domestic courts of other Nation. In case of the State Party authorities deny access or rectification, or unlawfully disclose their personal data.[104] This provision of the International Instrument depends on the adoption by such Party Legislator of the State's Judicial Redress Act has been launched.

5.4.3.3. Enforceability of Right

Universal Regime must impose that non-compliance could lead to solid sanctions. The revised EU enforcement regime is underpinned by power for regulators to levy financial sanctions can be substantial, with administrative fines authorized of up to a maximum of 20 million euros or 4% of total worldwide global turnover of the prior financial year, whichever is higher. The use of damage fine would be a real cost for IT Corporation to trigger the change in their policy and practice.

The method of periodic report for conduct regular updates and reviews of participating companies, to ensure that companies follow the rules they submitted themselves to. If companies do not comply in practice they face sanctions and removal from the list.[105] The Trust-Mark emblem would be recruited to supplement the action and procure ambitious international IT Corporation to participate in order to market their services in global market. In compound with Annual joint review mechanism**,** the mechanism will monitor the functioning of the Treaty, including the commitments and assurance as regards access to data for law enforcement and national security purposes.[106] The International and National Data Protection Authority will conduct the review and associate national intelligence experts from the State Party Authorities. The Commission will draw on all other sources of information available and will issue a public report to the Director or High level Commission of the Treaty.

---

[104] European Commission. *Questions and Answers on the EU-US data protection "Umbrella agreement".* Brussels, 1 Dec. 2016, p. 1.

[105] European Commission. *EU Commission and United States agree on new framework for transatlantic data flows: EU-US Privacy Shield.* Strasbourg, 2 Feb. 2016.

[106] European Commission. *European Commission launches EU-U.S. Privacy Shield: stronger protection for transatlantic data flows*. Press release, Brussels, 12 Jul. 2016.

Moreover, the recognition of investigative power of domestic and international supervisory authority must be landed as a procedure to point out wrongdoings internationally. Following the certification or recertification of IT Corporations under International Data Protection Treaty, a certain percentage of these IT Corporations should be subject to ex officio investigations of effective compliance of their data protection policies (going beyond control of compliance with formal requirements). Whenever there has been a finding of non-compliance, following a complaint or an investigation, the IT Corporation should be subject to follow-up specific investigation[107] thereafter.

The time is counting down to the point that E-Market enlargement is non-avoidable so the harmonization of legal regime to regulate International market is needed. National data protection authorities, as well as the Regional and International data protection bodies which will be established in the future, must issue rules and interpretations to assist data controller/processor organizations to prepare themselves before converge to harmonized global e-market.

5.5. Benchmarks for the development of a specific Universal Regime

Taking into account the results of the research, the needs to create International/Universal regime is obvious if building trust in E-Market is the aim. Since the court decision in diverse cases used the principle of territoriality and "Adequacy Principle" to effectively address the issue, there are some companies that might be inclined to artificially pick which national law to comply with and which national data protection authority to deal with. The EU and EU-US regimes will change that status quo by providing for a single set of rules, to be applied in uniformity by supervisory authorities across the EU and also extraterritorial.[108] This should eliminate the jurisdiction problems presented in many past cases and will create a common future for Global Single E-Market

[107] European Commission. *Restoring Trust in EU-US data flows - Frequently Asked Questions*. Brussels, 27 Nov. 2013, p. 4.

[108] Gryffroy, Pieter. *Taking a look at two cases in the margin of the CJEU's "Privacy Spring", before and after the General Data Protection Regulation: Weltimmo and Bara.* 2016, p. 4.

Despite the fact that within some two decades of intensive application, only small portion of countries have managed to pass EU *adequacy* criterion,[109] which allows personal data transfers to them, the EU has been extremely active in exporting its data protection model.[110] The new European data protection model and EU-US regime present a ready-made solution of substantial depth that can be tempting to countries with no previous data protection experience. If reaching the standard of EU, like the case of US and EU relationship, is the goal. So the main elements of the new data protection regime should consist of these elements: [111]

Empowerment of individuals' right

- Right of data subjects to know how their personal data are handled and by whom.
- Data portability: transferability of personal data between service providers.
- "Right to be forgotten" is clarified and codified through the introduction of a "right to erasure".
- Breach Notification: Information about when personal data has been hacked, if the breach is likely to result in a high risk to the individual's rights and freedoms.
- Allow Non-profit organizations to represent individuals in exercising their rights with regard to administrative and judicial remedies.

[109] Kuner, Christopher. "Developing an Adequate Legal Framework for International Data Transfers. Reinventing Data Protection?." *Springer*, 2009, pp. 262-73.

[110] Greenleaf, Glenn. "The Influence of European Data Privacy Standards outside Europe: Implications for Globalisation of Convention 108." *INT'L DATA PRIVACY LAW* 2 (Issue 2, 2012), pp. 68-92.

[111] Look at these documents; European Commission. *Agreement on Commission's EU data protection reform will boost Digital Single Market*. Press release, Brussels, 15 Dec. 2015; "European General Data Protection Regulation finally adopted: are you ready?." *Data Protection, Privacy and Security Alert (US)*, DLA Piper, 14 Apr. 2016; European Commission. *European Commission launches EU-U.S. Privacy Shield: stronger protection for transatlantic data flows*. Press release, Brussels, 12 Jul. 2016; European Commission, *EU Commission and United States agree on new framework for transatlantic data flows: EU-US Privacy Shield.* Strasbourg, 2 Feb. 2016; European Commission. *Restoring Trust in EU-US data flows - Frequently Asked Questions*. Brussels, 27 Nov. 2013; European Commission. *EU Data protection reform on track: Commission proposal on new data protection rules in law enforcement area backed by Justice Ministers*. Press release, Luxembourg, 9 Oct. 2015; European Commission. *Questions and Answers on the EU-US data protection "Umbrella agreement"*. Brussels, 1 Dec. 2016; European Data protection Supervisor. *Opinion 1/2016*. 12 Feb. 2016.

New rules for businesses competitiveness

- One-stop-shop: businesses with establishments in more than one Member State will in many cases have to deal with one supervisory authority (lead supervisory authority) only.
- Domestic rules on State territory: companies based outside of destination country will have to apply the same rules when offering services in the offshore country.
- Risk-based approach: no one-size-fits-all obligation, obligations now tailored to potential risks; Data protection by default.
- Data protection by design: the regulation guarantees that data protection safeguards are built into data processing from the earliest stage of development; producers of products and services are encouraged to take into account the right to data protection when developing new products and services that are based on or intended to process personal data.
- Obligation to notify data breaches to supervisory authorities, in some instances also to individuals.
- No more obligations to notify insignificant data processing to supervisory authorities every times.
- Businesses are exempt from the obligation to appoint a data protection officer insofar as data processing is not their core business activity and this does not require regular and systematic monitoring of data subjects on a large scale, or the core business activities do not consist of processing on a large scale special category of data. Other Regional or national law may however extend this obligation.
- Businesses will have no obligation to carry out an impact assessment unless there is a high risk to individuals' rights and freedoms.

Data protection in the area of law enforcement efficiency

- Law enforcement authorities (LEAs) can exchange information more efficiently and effectively.
- LEAs must comply with the principles of necessity, proportionality and legality when processing personal data.
- Supervision must be ensured by independent national data protection authorities.

- Effective judicial remedies must be provided.
- Rules for transferring personal data to third countries are clarified.
- Member States may introduce a higher level of protection into their national laws.

After research through many proposals from relevant competent organizations, there are some requirements that could be crystals as the best practice elements. These remarks should be brought to oblige data controller/processor in order to support the progressive realization of right to personal data protection. For transforming this universal best practice to be the enforceable policy, these measures should be adapted for drafting a new legal instrument to regulate the duty bearer organization. The prospect measures are as follows: [112]

Progressive Realization and Obligation to Transparency

1) State must publish the personal data protection or privacy policy of verified organizations

2) Organization, Legal Persons such as state authority, business enterprises and non-governmental organizations, must put the link to the supervisory and oversight authority website, which lists all the 'current' members of the scheme, on the privacy policies of verified organizations' websites

3) Organization must announce privacy conditions of any contracts verified organizations conclude with subcontractors, e.g. cloud computing services. (Data Controller and Data processor)

4) State must show the clearly flag of all organizations which are not current members of the scheme on the website of the supervisory and oversight authority.

Supervisory and Redress

5) State and Organization must appoint the supervisory and oversight authority to monitor more systematically ADR providers regarding the transparency and accessibility of information they provide concerning the procedure they use and the follow-up they give to complaints.

[112] European Commission. *Q&A: Guidance on transatlantic data transfers following the Schrems ruling*. Fact Sheet, Brussels, 6 Nov. 2015.

6) Organization must include a link to the alternative dispute resolution (ADR) provider on the verified organizations' websites of personal data protection policies.

7) Organization must provide the ADR which is readily available and affordable.

Implementation and Enforcement

8) Following the verification or recertification of organizations under International Agreement, a certain percentage of these organizations should be subject to ex officio investigations of effective compliance of their personal data protection policies (going beyond control of compliance with formal requirements).

9) Whenever there has been a finding of non-compliance, following a complaint or an investigation, the organization should be subject to follow-up specific investigation once again after 1 year.

10) In case of doubts about an organization's compliance or pending complaints, the Supervisory or Oversight Authority should inform the competent State data protection authority.

11) Even there are false claims of International Agreement adherence, still need to continue investigation.

Exceptions and Access by State Authorities

12) Personal data protection policies of verified organizations must include information on the extent to which Domestic law allows public authorities to collect and process data transferred under the International Agreement. In particular organizations should be encouraged to indicate in their personal data protection policies when they apply exceptions to the Principles to meet national security, public interest or law enforcement requirements.

13) The national security exception must be oversight and only use by the prerequisite condition of International Agreement. Exemption is used only to an extent that is strictly necessary and proportionate.

In summary, there is a need to providing a single set of rules to be applied in uniformity by supervisory authorities across the world. This would eliminate the problems

present in many past cases including the provisions covering the situation at issue on conflict of applicable law in different jurisdictions. Furthermore, the more “Accountability Principle” approach may be introduced to trace and track the activity of Trans-National IT Corporations and National or International Intelligence Agencies because of the different competences on the implementation ability among various States. Conclusively, the recognition of investigative power of domestic and international supervisory authority must be landed as a procedure to point out wrongdoings internationally. Whenever there has been a finding of non-compliance did by either private or public entities, following a complaint or an investigation, such IT Corporation and State Authority should be subject to follow-up specific investigation thereafter.

Chapter 6 Conclusions and Recommendations

The uses of personal data from internet are no longer performed locally, or even within well-scoped physical territories. Besides, trans-border personal data processing became personalized. Domestic data controllers are no longer needed to transmit their data subjects' data across borders to other data controllers in order for trans-border exchanges to occur. At present, Social Network applications enable users to upload their personal data to the "Account" or "Webpage", going to and from unidentified destination. With regard to data protection, it must be decided how, if at all, data can be protected to the same extent in the cyberspace as in the "real" world. It is usual that attempts to create a safe online society result in even harder than in an offline environment because the amount of processed data is far greater than the past. Within this general context of problems and challenges, our research makes possible to obtain some conclusions and to formulate some recommendations that can help to their solution and management.

6.1. Conclusions

6.1.1. Personal Data Protection under the EU and EU-US E-market legal regime prior 2013 reforms: main deficiencies/shortcomings and problems

Even though, the goal of this research is to harmonize the provision and implementation of Personal Data Protection, for creating International Regime, but at the starting point show the overlap and insufficient of the old instruments. Specially, the old set of personal data protection laws, which was enacted before the reformation process of EU and US, had been heavily based on the implementation at the domestic level.

6.1.1.1. Predominance of the US Entities and its effects on Global Netizen

Most prominently, the discontents US system brought to the personal data protection recourse came from the directly clash with the State intelligence operation in National Security realm. The intention of US government to conduct mass electronic surveillance on activities relate to terrorism, especially on foreigner who is out of the full US

constitutional protection, may put further complicated situations for internet users around the world. Since most of dominant IT Corporations are subjected to US or transfer personal data to the servers in US territory, the different standard would be the main threat to Non-US citizen internet users.

US IT Corporation are subjected to US domestic laws whereas Rights of Global Neitizen are in the realm of US jurisdiction when such data transferred to US territory or entity and it may be compromised by the exercise of US Authorities.

Data Controller, US IT Corporation, has obligation to secure their data system and notify data subjects and State Data Protection Authority (DPA), when data breach happen. US DPA, Federal Trade Commission under Ministry of Commerce, has a duty to provide preparatory and supporting advices especially when there were wide spread of massive electronic data surveillance by US National Security Agency. Before the revelations on June 5th of 2013, both US DPA and IT Corporation had done nothing. To meet the Adequacy Criterion of EU, the transfer of data across Atlantic had been under provision of EU-US Safe Harbor Agreement, legalizing trans-border data flows.

The effectiveness of the enforcement regimes in various countries is on the extent of judicial interpretation and on other comparative aspects of data protection laws. There are processing dispute resolution procedures in EU but not in the Safe Harbor Agreement. The mass transfer of data of Non-US citizens to US companies and authorities and the lack of appropriate redress mechanism for them is an issue of extreme concern.

The EU data protection regulators had launched an investigation into Google's data retention and privacy practices, which was extended to cover other search engines as well. In 2012 the EPIC appealed to the United States District Court for the District of Columbia seeking disclosure of any communications between National Security Agency (NSA) and Google Inc. regarding encryption and cyber security. Many cases lead to the revelation of the cooperation between NSA and IT Corporation which impact to Personal Data Protection.

As NSA‘s PRISM project collect data from the most powerful IT Corporations of the world such as Google, Yahoo, Facebook etc., the identification of place time and activity of people could be tracked and traced orderly from the Big Data Collection that gathering from Cyberspace globally including Non-US Citizen outside US territory.

Since the US Courts have made decisions which set the precedent on Data Collecting and Sharing of IT Corporation and State Authority because they are the subjects under US jurisdiction. On December 16, 2013, the U.S. District Court ruled in *Klayman v. Obama*, that the NSA's bulk collection of domestic telephone call detail records likely violated the Fourth Amendment (right to privacy and personal data protection). This case celebrated the full constitutional rights enjoyment of US citizen but the protection for Non-US citizen stills remain.

On other side of Atlantic, Court of Justice of European Union CJEU had launched a series of decisions relating personal data protection by IT Corporation and State especially the case of US nationality Entities. Since there was the *LIBE Report on Mass Electronic Surveillance*, the MUSCULAR program, which collects more than twice as many data points compared to PRISM. The MUSCULAR program requires no warrants and operates by the coordination with UK,; so UK as EU Member State, have made direct breach on personal data of data subjects around the world.

Facebook's user, who claims his data was breached by US Agencies, filed the case called Schrems Case after his name. The CJEU ruling found that U.S. national security, public interest, and law enforcement requirements have "primacy" over the Safe Harbor principles, and that US undertakings are bound to disregard, without limitation, the protective rules laid down by that scheme where they conflict with such requirements. Consequently, the CJEU observed that the Safe Harbor scheme "enables interference" by US authorities "with the fundamental rights of the persons whose personal data is or could be transferred from the EU to the US."

The CJEU concluded that Safe harbor and US legislation do not providing for any possibility for an individual to pursue legal remedies in order to have access to personal data relating him or to obtain the rectification or erasure of such data compromises the essence of this fundamental right, which is an important component of the rule of law. Thus, the Safe Harbor Decision did not contain sufficient remedy measure for individual in case of violation by IT Corporation or State National Authority.

Therefore, CJEU invalidated Safe Harbor on 6 October 2015. EU and the US need to renegotiate new agreement to regulate data flows between both sides of Atlantic.

In conclusion, the difficulties come from the failure of US legal system for protecting personal data of data subjects. The inadequacy of US system brought deteriorates to the personal data protection. The program of US government to conduct mass electronic surveillance on activities relate to terrorism, especially on foreigner who is out of the full US constitutional protection, may put further obscure scenarios for internet users globally.

6.1.1.2. Different standards and the difficulties from fragmented jurisdiction

Personal Data protection has been recognized in diverse instruments from International Organization to EU Regional Bloc then Bilateral EU-US agreement. Accordingly, the legal binding consequence of each agreement is different because the legal nature of each one is up to the manner of its launching institution. Differences in the legal nature of data protection law between cultures and legal systems have made it more difficult to reach an international consensus on the subject.

The commons and differences of definition and scope written in various sources, brings complicates to the implementation of personal data protection. Many activities in the public or the private sector are under scope of personal data protection instruments which cover large amount of information. But it has brought troubles to individual for exercising their right in other countries. However, the different scopes are on actor and jurisdiction as most powerful actor who control and process personal data, IT Corporation; Multi-National Legal Person, is under the appliance of the Law of specific territory but their activities are trans-border.

The instruments recognizing right to personal data had been creating for decades so there is some out-of date provisions maintain in those legal documents. The more advance in technology the more complexity it brought into legal atmosphere. The implementation of data subjects' right to personal data protection is increasingly complicated because the nature of data which is decentralized to various kinds of organizations.

The '*fairly and lawfully*' principle provides a 'lens' through which the other provisions in the Data Protection Directive should be interpreted. Since the data processor has no direct obligation to data subject, it will impact how data protection issues are addressed in

data processing business and data sharing on preventing and suppressing crime and terrorism especially when the Third Party is the Subject to Different Jurisdiction.

The jurisdiction of EU laws and extraterritorial application of EU data protection law was re-affirmed more strongly in *Google Spain Case.* In finding that EU data protection law did apply in such a case, the Court noted that the Directive should be interpreted to have 'a particularly broad territorial scope'. The CJEU also held that the right to delete data under the EU Data Protection Directive applies to the results of Internet search engines ('right to be forgotten' or 'right to erasure'). These precedents give a path for EU internet users to exercise their rights with Trans-Border IT Corporations even such Legal Persons are not EU nationals.

In the European Union, various legal instruments and obligations provide individuals and regulators with a framework that allows the assertion of rights with regard to EU-based data processing. Thus, EU data protection authorities are obliged to cooperate with each other, and often do so in practice. Court decisions from one EU Member State can also be enforced in another Member State with relative ease. However, the same legal instruments do not apply to situations where a non-EU country is involved, meaning that such enhanced regulatory cooperation and ease of enforcement are not possible to fulfill. The difficulty of asserting legal rights abroad is not unique to data protection, but results from the fact that there is no global legal framework for the assertion of consumer rights in Cyberspace, or for the recognition and enforcement of court decisions in other countries.

6.1.1.3. Vague exemptions and lack of supervisory over data surveillance in criminal procedure

As well as other human rights, the right to personal data protection is not absolute; it can be restricted in certain situations and due to other rights. Most often deal with the relationship between state of emergency and personal data protection. The state authorities and courts must weigh up the reasons for accessing certain data and the potential effect on an individual of such state surveillance. A necessary precondition and proportionate solution must be provided, in which state/public interests as well as the interests of the data subject are taken into consideration. Nonetheless, US most influence IT Corporations are a subject under US national security laws; Patriot Act, Homeland Security Act and Foreign

Intelligence Surveillance Act which may compromise the full enjoyment of personal data protection,,

Most data protection instruments impose a similar obligation on public authorities and private parties. After all, fundamental human rights primarily aim to limit the actions of public authorities in order to protect the activities of private parties, including the processing of personal data, from state interference. However, the effectiveness of access control of national security exceptions is relevant to the existence of any back doors or other means for accessing unencrypted personal data opened by Service Provider, IT Corporation.

In *Elecronic Privacy Information Center v. National Security Agency*, the D.C. Circuit held that the NSA's *Glomar* response (remain silent when face inquiry) sufficiently satisfied the exemption requirements of the Freedom of Information Act because threat assessment is an undisputed NSA function and, therefore, the NSA was not required to confirm or deny existence of any responsive records. This case affirmed the exemption power of national Security to exercise secrecy mission above the protection of civil rights.

Problems have emerged from set of Security Laws were left to the interpretation in secret proceedings, such as the *Foreign Intelligence Surveillance Court* (FISC and the higher Review court FISCR) whose judges are appointed solely by the Chief Justice of the Supreme Court. It appears that the FISA courts agree with the government's argument that it is common in investigations for some indefinitely large corpus of records to be considered "relevant", in order to discover the actual evidence. Accordingly, the lack of Supervision and Oversight are the main threat to protection of personal data worldwide since it relies on US Administrative related Court decisions. Further, the Non-US Citizen has no right to appeal in US Court for such violations.

In the *Digital Rights Ireland Case*, it can be pointed particularly on the principle of purpose limitation, on the right to access of individuals to their personal data and on the control by independent data protection authorities. However, data retention needs a shred of evidence to suggest that their conduct might be connected to a serious crime and no one is exempted from this rule; it even applies to those whose communications are subject to professional secrecy, according to national rules. Aftermath, the Data Retention Directive was invalidated by CJEU on 8th April 2014 since it did not meet the EU principle of proportionate and necessary exemptions.

6.1.2. Improvements and limits in Personal Data Protection after the 2013 reforms of the EU and EU-US E-Market legal regime.

After all benchmarks the US and EU Courts had been made in past cases, the US Government and EU Legislation Unit have launching set of laws in the interest of reformation.

The US and EU appointed committee to create changes for better solution to handle the problems. Accordingly, EU approves General Data Protection Regulation (GDPR) and Directive on judicial and criminal matters then brought US to sign agreement to implement those standards which are EU-US Privacy Shield for general data protection and EU-US Umbrella Agreement on judicial and criminal matters. These reforms took place since April of 2016 and will be full implementation in 2018.

Nevertheless, the starting point of these set of reforms can be traced back to the changes triggered by the US since late 2013 due to the International pressure on Global Mass Electronic Surveillance Programs of US Government, especially from EU the main E-Market trading counterparts.

6.1.2.1. Responses of the US relating personal data protection for Non-US citizen Data Subject

There are initiatives from US and EU to address the problem of personal data protection in digital age. The US Government had launched a set of laws to reform their surveillance activity and provide Non-US citizen stronger protection of their personal data.

In March 2014, the US government adopted six privacy principles to govern surveillance. This US Framework declared by President Obama Presidential Policy Directive 28 (PPD-28), to better protect personal data of all persons including non-U.S citizens worldwide.

The critical improvement is the Judicial Redress Act, extends to EU citizens the same rights that U.S. citizens enjoy under the Privacy Act of 1974 with respect to the data protection obligations of U.S. government agencies. Additionally, the Judicial Redress Act give EU citizen access to U.S. courts to enforce privacy rights in relation to personal data transferred to the U.S. for law enforcement purposes.

The EU GDPR applies to organizations established in a third country if they are offering goods and services, or monitoring the behavior of individuals, in the EU. It also introduces some new tools for international transfers, Adequacy decisions, the GDPR provides more precise and detailed elements that must take into account when assessing the level of data protection provided in the legal order of a third country.

In Privacy Shield, redress mechanism will inform a complainant of an access or surveillance matter has been properly investigated and obliged with US law. In the case of non-compliance it will be properly remedied. EU citizens are capable to lodge complaints directly to their local DPAs. Remedy mechanisms determine period for responses by a subject organization. Privacy Shield also creates a new arbitration right for unresolved complaints.

However, the Umbrella Agreement does not provide for equal rights and remedies for EU- and US nationals in the USA; but worse, non-EU citizens living in EU Member States who are not nationals of the Member State concerned and whose data may have been sent to the USA, are completely denied judicial redress in the USA under the Umbrella Agreement.

6.1.2.2. Harmonization of Trans-Atlantic legal standards

The GDPR applies to organizations established in a third country if they are offering goods and services, or monitoring the behavior of individuals, in the EU. It provides for an effective sanctions regime by harmonizing the powers of national data protection supervisory authorities (DPAs). They will be empowered to impose fines reaching up to EUR 20 million or up to 4% of the total worldwide annual turnover of a company.

The EU-US Privacy Shield core principles are the same as Safe Harbor by harmonize the data protection within EU-US Single E-Market. Privacy Shield includes statements regarding the enforcement body, a new arbitration right, disclosures to public authorities, and the company's liability for onward transfers.

EU Directive on Criminal and Judicial Matters includes harmonized rules for international transfers of personal data in the context of criminal law enforcement cooperation. Meanwhile, it will enable the police and judicial authorities to cooperate more effectively, amongst Member States as well as between Member States and their international

partners, to combat crime and terrorism. It urges State to provide independent national data protection authorities that individuals can afford effective judicial remedies.

EU-US umbrella Agreement protections and safeguards will apply to all data exchanges taking place in the context of transatlantic law enforcement co-operation in criminal matters in every level. The provision covers all the substance EU data protection principles; processing standards, safeguards and individual rights. Agreement provides data subject judicial redress rights concerning US domestic law reforms to support EU Citizen. Nevertheless, it contains some inferiors and threats to data protection standard of EU; different definition, oversight and rights of data subject to claim remedy especially Non-EU Citizen even they live in EU territory.

6.1.2.3. Balancing the interests between data subject and State Authority concerning criminal matters

Following a review by an independent panel appointed by President Obama, the US executive branch made significant changes to improve the compliance of its foreign intelligence practices with international human rights law. These include more specific definitions of the purposes for which surveillance can be undertaken.

Since March 2014, the US government adopted Directive 28 (PPD-28), US Framework, to govern surveillance with six privacy principles. It imposes important limitations for intelligence operations. It specifies that data collection by the intelligence services should be targeted. Additionally, the PPD-28 limits the use of bulk collection of data to 6 purposes; detect and counter threats from espionage, terrorism, weapons of mass destruction, threats to the Armed Forces or transnational criminal threats. The six principles endorsed by the US are (1) rule of law, (2) legitimate purpose, (3) non-arbitrariness, (4) competent external authority, (5) meaningful oversight, and (6) increased transparency and democratic accountability. However, there are stills some overlaps between the US Framework and the Principles that US practice may fail to comply since the old court precedent, Glomar Response, is remained.

Furthermore, US reviews the USA Freedom Act which would preventing bulk collection by requiring a nexus to an investigation, bringing clarity to Section 215 of Patriot Act, increasing FISC oversight and introducing a special advocate, increasing the ability of

companies to disclose government national security data requests, and increasing the power of internal oversight bodies, as well as adding external checks.

The critical improvement is the Judicial Redress Act, extends to EU citizens enjoy under the Privacy Act of 1974 with respect to the data protection obligations of U.S. government agencies. However, the limited application of the Judicial Redress Act because there are many exemptions and the legal uncertainty regarding the agencies to which the Judicial Redress Act will apply, do not satisfy the requirement to offer an effective redress mechanism to all individuals concerned in national security intelligence surveillance cases. Additionally, the Judicial Redress Act give EU citizen access to U.S. courts to enforce privacy rights in relation to personal data transferred to the U.S. for law enforcement purposes. Stills Non-EU citizen are not entitled to enjoy these rights.

GDPR provide comprehensive, detailed and transparent derogations to transfer personal data outside the EU, the reform clarifies those rules in many ways. The provisions on the independence, functions and powers of EU DPAs are expressed out in more detail and substantially enhanced. This expressly includes the power to suspend data flows to a recipient in a third country or to an international organization.

Privacy Shield scopes clear data retention limits, restrictions, safeguards, and oversight mechanisms for access by state agencies for law enforcement and national security purposes. It transforms the oversight system from self-regulating to more responsive and proactive system, certification and annual recertification process remain, but the Department of Commerce will monitor compliance via detailed questionnaires. Moreover, the Federal Trade Commission will maintain a “Flag list” for organizations that are subject to FTC or court orders in Privacy Shield cases.

EU Directive on criminal matters provides transparent, detailed and comprehensive rules for personal data transfers to third countries including the power to suspend data flows to a recipient in a third country or to an international organization who does not meet the adequacy standard. The new Directive will raise the level of protection for individuals; victims, witnesses, and suspects of crimes are protected in the context of a criminal investigation or a law enforcement action. Supervision is ensured by independent national data protection authorities.

The EU-US Umbrella Agreement does not contain a general human rights clause prohibiting the "sharing" or "onward transfers" of data on EU persons, provided subject to the Agreement, with or to other agencies, in the USA or elsewhere, in circumstances in which this could lead to serious human rights violations, including arbitrary arrest and detention, torture or even extrajudicial killings or "disappearances" of the data subjects or others. It also expands to the whole law enforcement sector the principle of independent oversight including effective powers to investigate and resolve individual complaints. Nonetheless, in terms of transparency and oversight, it falls short of fundamental European data protection and human rights requirements because the data subjects cannot file their appeal in FISC.

The reforms of EU and EU-US regime set a new harmonized standard for liberal market economy country to follow. It could be transformed to International Treaty open for other state to ratify. International Community may use these set of standards as a foundation to draft International Instrument on Personal Data Protection for sign and accession. The more inclusive approach, would solve the problem on jurisdiction, and make the compliance of personal data protection to different jurisdiction possible.

6.2. Recommendations on drafting International Regime for Personal Data Protection

Due to the speedy widespread of Internet penetration in the last two decades, a new situation has now arisen whereby Multi-National IT Corporations collect a large amount of personal data either directly, though the user putting their data in Social Network or indirectly people using an search engine or tab bar that allow much information to be found out about them. Many private entities, including giant IT Corporations or State Agencies, have their own "Rule" and different structures for self-regulating their information system. But these are policies the organizations have themselves seen proper to enact and are mainly based on the self-verified of such Entities. Furthermore, domestic legislation is enacted regardless of the fact that the companies are multi-nationals and it may be tough to seek a direct link to a given jurisdiction in a specific case. Not withstand, laws could, in fact, prove hard to apply efficiently due to deadlocks relating jurisdiction.

6.2.1. Single set of common rules

While data protection legislation has a cross-border dimension, its subsequent development acquired distinct national and regional characteristics. In order to accommodate the international cooperation of fundamentally different data protection legal systems, a series of initiatives have been undertaken, particularly during the last decade.

The interesting legal scheme implemented for the trans-Atlantic exchange of personal information is, in effect, a patchwork legal solution constructed on EU-US bilateral basis. It includes the Privacy Shield for fundamental personal data exchanges and Umbrella Agreement for protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties.

On each side of the Atlantic, largely different provisions govern the respective processing once personal data have been transmitted. The EU-US example is a powerful case for the advantages of introducing a single international data protection instrument that would has saved both parties from a multitude of complex and hard-to follow arrangements and, ultimately, a significant waste of resources in the respective negotiation and drafting processes. Nonetheless, these set of EU-US instruments have potential to set standard for International Data Protection Initiatives and other regional organizations since it covers vast majority states in the regime of liberal market economy countries.

To providing a single set of rules, to be applied in uniformity by supervisory authorities across the world would eliminate the problems present in many past cases including the provisions covering the situation at issue on conflict of applicable law in different jurisdictions.

6.2.2. Regulate the high capacity trans-border entity

Since the court decision in many cases used the principle of territoriality and “Adequacy Principle” to effectively address the jurisdiction, so the issue that some IT Corporations might be tended to artificially select which national law to comply with and which national data protection authority to deal with. The more “Accountability Principle” may be introduced to trace and track the activity of Trans-National IT Corporations and

National or International Intelligence Agencies because of the different competences on the implementation ability among various States.

6.2.2.1. Regulate Trans-National IT Corporation

For employing Adequacy Principle, the Data protection related trust-marks, particularly web seals, flag, constitute the practical extension of self-regulatory attempts by trade-counterparts in E-Market. By affixing web seals onto Internet pages, members verify compliance to the data protection standards and best practices more or less in the same way that notification of the processing to data protection authorities confirms its lawfulness in the E-Market. Look at the Model of US, the web seal program TRUSTe (originally E-Trust) and used in an attempt to convince the EU on the *adequacy* of its data protection, and later used in negotiations for the conclusion of the Safe Harbor Agreement and then Privacy Shield that open for company to register. Privacy Shield is controlled and guaranteed by US Federal Trade Commission.

By adapting the Accountability Principle of OECD Model, international and regional organizations have released various legal statuses and effectiveness personal data protection law. These codes of practice come in various formats and types. They range from self-regulatory instruments of voluntary compliance without any monitoring or enforcement mechanisms, to strict sets of rules introduced in cooperation with national data protection authorities and even ratified by law in strict EU-like data protection systems. In effect, these are universal codes of practice adopted by multinational groups of companies and ratified by the competent national data protection authorities, which define the group's global data protection policy with regard to the international transfers of personal data within the same corporate group to entities located in countries that may not provide an *adequate* level of protection, as per EU standards.

6.2.2.2. Regulate State Intelligence Agency

The Data Protection for Police and Criminal Justice Authorities part, especially national and international intelligence units counter organized crime and terrorism, will take account of the specific needs of legal enforcement. It must protect everyone, regardless of whether they are a victim, criminal or witness, and the proposed International

Intelligence Codex must be under serious considerations. All law enforcement processing in the State Party must comply with the principles of necessity, proportionality and legality, with appropriate safeguards for the individuals. Oversight is ensured by independent national data protection authorities, and effective judicial remedies must be provided. Moreover, Rules for transferring personal data to third countries are clarified and Member States may introduce a higher level of protection into their own national laws. However, it must respect the different legal traditions in State Parties and is fully in line with the International Treaties of Human Rights.

6.2.3. Establish an International Data Protection Institution

The Universal or International regime should contain novel and inventive procedures for cooperation, mutual assistance, joint operations and a consistency mechanism. Moreover, all national data protection authorities have to present activity reports annually, which will be made public. All of this aims at ensuring consistency in the application of the regulation by the national authorities. Universal Regime must impose that non-compliance could lead to heavier and material sanctions. If companies do not comply in practice they face sanctions and removal from the list, such as Trustmark Emblems.

Universal Regime should settle the One-stop-shop, businesses and individuals will only have to deal with one single supervisory authority. The One-stop-shop for individual complainant would be important path for effective remedy and provide greater opportunity for internet user to contact with oversight mechanism. The accessible and affordable dispute resolution mechanisms is Ideal, the complaint will be resolved by the company/authority itself; or free of charge Alternative Dispute resolution (ADR) solutions. ADR should be offered if a case is exhaustion of domestic remedy, as a last resort there will be an arbitration mechanism. Furthermore, redress possibility in the area of national security for State Party citizen must be handled by an Ombudsperson independent from the national intelligence services who involved.

The Data Protection for Police and Criminal Justice Authorities part needs of Supervision by independent national data protection authority or non-partial court, and effective judicial remedies for suffering data subjects must be provided.

The recognition of investigative power of domestic and international supervisory authority must be landed as a procedure to point out wrongdoings internationally. Whenever there has been a finding of non-compliance, following a complaint or an investigation, the IT Corporation should be subject to follow-up specific investigation thereafter.

Bibliography

1. Book

Bennett, Colin J and Raab, Charles D. *The Governance of Privacy: Policy Instruments in Global Perspective.* 2006.

Brin, David. *The Transparent Society: Will Technology Force Us to Choose between Privacy and Freedom?*. Basic Books, 1999.

Bygrave, Lee A and Michaelsen, Terje. *Governors of Internet.* Oxford University Press, 2009.

Cavanagh, Allison. *Sociology in the Age of the Internet.* Tata McGraw-Hill Education, Delhi, 2010.

Concurring, Harlan J. *Comment on Case 389 U.S. 347 Katz v. United States*. 1967.

Crofton, Isaak. *Crypto Anarchy*. Lulu, 2015.

DLA Piper. *European General Data Protection Regulation finally adopted: are you ready? Data Protection, Privacy and Security Alert (US),* 14 Apr. 2016.

Fokus, Fraunhofer. (Hoepner, P and Strickand, L and Löhe, M.). *Historical Analysis on European Data Protection Legislation*. 2012.

Foucault, Michel. *Security, Territory, Population (Michel Foucault: Lectures at the College De France)*. Burchell, Graham. Trans. Palgrave Macmillan, London, 2007.

Fuchs, Christian. *Internet and Society: Social Theory in the Information Age.* Routledge, London, 2007.

Galetta, Antonella and De Hert, Paul. *A European perspective on data protection and access rights.* Vrije Universiteit, Brussels, 2013.

Goldsmith, Jack and Wu, Tim. *Who Controls the Internet?: Illusions of a Borderless World.* Oxford University Press, UK, 2006.

Gryffroy, Pieter. *Taking a look at two cases in the margin of the CJEU's "Privacy Spring", before and after the General Data Protection Regulation: Weltimmo and Bara*. 2016

Hogan Lovells. *Legal Analysis of the EU-US Privacy Shield*. 2016.

Hunton&Williams. *Overview of the EU General Data Protection Regulation*. 2016.

Hustinx, Peter. *EU Data Protection Law: The Review of Directive 95/46/EC and the Proposed General Data Protection Regulation*. 2014.

Kerschischnig, Georg. *Cyberthreats and International Law.* Eleven International Publishing, 2012.

Lloyd, Ian J. *Information Technology Law.* Oxford University Press, UK, 2011.

Lloyd, Ian J. *Legal Aspects of the Information Society*. Lexis Law Pub, London, 2000.

Loader, Brian. *The Governance of Cyberspace: Politics, Technology and Global Restructuring.* Psychology Press, Brighton, 1997.

Lyon, David. *Surveillance Studies: An Overview*. Polity Press, Cambridge, 2007.

Maesa, Costanza D F. *Balance Between Security and Fundamental Rights Protection: an Analysis of The Directive 2016/680 for Data Protection in The Police and Justice Sectors and the Directive 2016/681 on the Use of Passenger Name Record (PNR)*. 2016.

Marx, Karl. *Capital: A Critique of Political Economy.* International, New York, 1867.

Morningstar, Chip and Randall, Farmer R. "The Lessons of Lucasfilm's Habitat." *The New Media Reader*. Ed. Wardrip-Fruin and Nick Montfort: The MIT Press, Massachusetts, 2003.

Nowak, Manfred. *United Nations Covenant on Civil and Political Rights: Ccpr Commentary.* Engel, Lancaster, 1993.

Peters, Sarah. *2009 Csi Computer Crime and Security Survey.* Computer Security Institute, 2009.

Polanyi, Karl. *The Great Transformationthe Political and Economic Origins of Our Time.* Farrar&Rinehart, New York, 1944.

Spinello, Richard A. *Cyberethics: Morality and Law in Cyberspace.* Jones & Bartlett Publishers, Massachusetts, 2014.

Terranova, Tiziana. *Network Culture: Politics for the Information Age.* Pluto Press, London, 2004.

Vaidhyanathan, Siva. *The Googlization of Everything: (and Why We Should Worry).* University of California Press, 2012.

2. Article

Ackerman, Spencer. "Nsa Illegally Collected Thousands of Emails before Fisa Court Halted Program." *The Guardian, August*, vol. 21, 2013.

Akdeniz, Yaman. "Governing Racist Content on the Internet: National and International Responses." *UNBLJ*, vol. 56, 2007.

Arthur Cox. "Data Protection Update – New Legislation." *Technology & Innovation*, 2016

Avet, Traci. "Who's Afraid of Google?." *Library Journal*, vol. 131, no. 10, 2006.

Balkin, Jack M. "Digital Speech and Democratic Culture: A Theory of Freedom of Expression for the Information Society." *NYUL rev.*, vol. 79, 2004.

Barlow, John Perry. "A Declaration of the Independence of Cyberspace (Feb. 8, 1996)." *Davos, viewed*, vol. 10, 2013.

Basu, Subhajit and Jones, Richard. "Regulating Cyberstalking." *Journal of Information Law & Technology*, vol. 22, 2007.

Battelle, John. "The Search: How Google and Its Rivals Rewrote the Rules of Business and Transformed Our Culture." 2005.

Bender, David and Larry Ponemon. "Binding Corporate Rules for Cross-Border Data Transfer." *Rutgers JL & Urb. Pol'y*, vol. 3, 2006.

Berman, Paul S. "Law and Society Approaches to Cyberspace." *Law and Society Approaches to Cyberspace*, Ashgate Publishing, Aldershot, 2007.

Bignami, Francesca. "The Us Legal System on Data Protection in the Field of Law Enforcement. Safeguards, Rights and Remedies for Eu Citizens." 2015.

Blackmer, WS. "Gdpr: Getting Ready for the New Eu General Data Protection Regulation." *Information Law Group, InfoLawGroup LLP, Retrieved*, vol. 22, no. 08, 2016, p. 2016.

Boehm, Franziska. "Confusing Fundamental Rights Protection in Europe: Loopholes in Europe's Fundamental Rights Protection Exemplified on European Data Protection Rules." *University of Luxembourg, Law Working Paper Series, Paper no. 2009-01*, 2009.

Bowden, Caspar. " Directorate General For Internal Policies." *The Us Surveillance Programmes and Their Impact on Eu Citizens' Fundamental Rights,* 2013.

Brown, Ian. "The Feasibility of Transatlantic Privacy-Protective Standards for Surveillance." *International Journal of Law and Information Technology*, vol. 23, no. 1, 2015.

Bryan, Cathy and Tatam, James. "Political Participation and the Internet." *Liberating Cyberspace: Civil Liberties, Human Rights & the Internet.* Pluto Press, London, 1999.

Bumiller, Elisabeth. "Pentagon Expanding Cybersecurity Force to Protect Networks against Attacks." *The New York Times*, vol. 27, 2013.

Bygrave, Lee A. "Privacy Protection in a Global Context–a Comparative Overview." *Scandinavian Studies in Law*, vol. 47, 2004, pp. 319-348.

Carroll, J M. "The Problem of Transnational Data Flows." *Policy issues in data protection and privacy, Proceedings of the OECD seminar*, vol. 24, 1974.

Carter, Dave. "Economic Regeneration and the Information Economy." *The governance of cyberspace: Politics, technology and global restructuring*, vol. 136, 1997.

Cate, Fred H. "The Failure of Fair Information Practice Principles." *Consumer Protection in the Age of the Information Economy,* 2006.

Cathy, Bryan. and James, Tatam. "Political Participation and the Internet." *Liberating Cyberspace: Civil Liberties, Human Rights & the Internet.* Pluto Press, London, 1999.

Chander, Anupam and Sunstein, Cass. "Whose Republic?." *JSTOR*, 2002.

Chazen, Joshua R. "Electronic Privacy Information Center V. National Security Agency: How Glomar Responses Benefit Businesses and Provide an Epic Blow to Individuals." *J. Bus. & Tech. L.*, vol. 9, 2014

Clarke, Roger. "Information Technology and Dataveillance." *Communications of the ACM*, vol. 31, no. 5, 1988.

Cohen, Julie E. "Examined Lives: Informational Privacy and the Subject as Object." *Stanford Law Review*, 2000

Coudert, Fanny. "The Directive for Data Protection in the Police and Justice Sectors: Towards Better Data Protection?" 2016.

De Hert, Paul and Papakonstantinou, Vagelis. "Three Scenarios for International Governance of Data Privacy: Towards an International Data Privacy Organization, Preferably a UN Agency." *ISJLP*, vol. 9, 2013.

De Hert, Paul and Schreuders, Eric. "The Relevance of Convention 108." *Proceedings of the Council of Europe Conference on Data Protection,* Warsaw, 2001.

De Hert, Paul. "The Right to Protection of Personal Data. Incapable of Autonomous Standing in the Basic EU Constituting Documents?." *Utrecht Journal of International and European Law*, vol. 1, no. 31, 2015.

De Montjoye, Yves-Alexandre et al. "Unique in the Crowd: The Privacy Bounds of Human Mobility." *Scientific reports*, vol. 3, 2013.

Donohue, Laura K. "Bulk Metadata Collection: Statutory and Constitutional Considerations." *Harvard Journal of Law and Public Policy*, vol. 37, no. 3, 2014.

Dowling Jr, Donald C. "Preparing to Resolve Us-Based Employers' Disputes under Europe's New Data Privacy Law." *J. Alt. Disp. Resol.*, vol. 2, 2000.

Dowling Jr, Donald C. "International Data Protection and Privacy Law." *Practising Law Institute treatise International Corporate Practice*, 2009.

Drummond, David. "A New Approach to China." *The official Google blog*, vol. 12, 2010.

Easterbrook, Frank H. "Cyberspace and the Law of the Horse." *U. Chi. Legal F.*, 1996.

Eberlein, Burkard and Newman, Abraham L. "Escaping the International Governance Dilemma? Incorporated Transgovernmental Networks in the European Union." *Governance*, vol. 21, no. 1, 2008.

Escudero-Pascual, Alberto and Hosein, Ian. "Questioning Lawful Access to Traffic Data." *Communications of the ACM*, vol. 47, no. 3, 2004.

Fahey, Elaine and Curtin, Deirdre. *A Transatlantic Community of Law: Legal Perspectives on the Relationship between the EU and US Legal Orders*. Cambridge University Press, UK, 2014.

Farrell, Henry. "Constructing the International Foundations of E-Commerce—the EU-US Safe Harbor Arrangement." *International Organization*, vol. 57, no. 02, 2003.

Farrell, Maria. "Communications data retention in the UK." *E-commerce Law and Policy*, Vol. 3, 2001.

Flynn, Cathal. "Data Retention, the Separation of Power in the Eu and the Right to Privacy: A Critical Analysis of the Legal Validity of the 2006 Directive on the Retention of Data." *UC Dublin L. Rev.*, vol. 8, 2008.

Fuster, Gloria González et al. "From Unsolicited Communications to Unsolicited Adjustments." *Data Protection in a Profiled World*, Springer, 2010.

Garcia, Michael J. "International Law and Agreements: Their Effect Upon Us Law." *Washington: Congressional Research Service, marzo*, 2013.

Gavilán, Elisa U. "Derechos Fundamentales Versus Vigilancia Masiva. Comentario a La Sentencia Del Tribunal De Justicia (Gran Sala) De 6 De Octubre De 2015 En El Asunto C-362/14 Schrems." *Revista de Derecho Comunitario Europeo*, no. 53, 2016.

Gellman, Barton and Laura Poitras. "Us, British Intelligence Mining Data from Nine Us Internet Companies in Broad Secret Program." *The Washington Post*, vol. 6, 2013.

Ghosh, Devdeep. "The Information Technology (Intermediaries Guidelines) Rules, 2011: A Disaster on All Fronts." 2013.

Ginsburg, Jane C. "Copyright and Control over New Technologies of Dissemination." *Columbia Law Review*, 2001.

Greenleaf, Graham. "'Modernising'data Protection Convention 108: A Safe Basis for a Global Privacy Treaty?" *Computer law & security review*, vol. 29, no. 4, 2013.

Greenleaf, Graham. "Sheherezade and the 101 Data Privacy Laws: Origins, Significance and Global Trajectories." *Journal Of Law, Information & Science*, 2013.

Greenleaf, Graham. "The Influence of European Data Privacy Standards Outside Europe: Implications for Globalization of Convention 108." *International Data Privacy Law*, 2012.

Greenwald, Glenn and Ewen MacAskill. "NSA Prism Program Taps in to User Data of Apple, Google and Others." *The Guardian*, vol. 7, no. 6, 2013.

Grimm, Dieter. "Der Datenschutz vor einer Neuorientierung" *Juristenzeitung*, 2013.

Grimmelmann, James. " What Is Pay per Click (PPC)?."." *Iowa L. Rev.*, vol. 93, 2007.

Guadamuz, Andres. "Law and Society Approaches to Cyberspace." *HeinOnline*, 2010.

Hamari, Juho et al. "The Sharing Economy: Why People Participate in Collaborative Consumption." *Journal of the Association for Information Science and Technology*, vol. 67, no. 9, 2016.

Harrison, Ann. "Creative Commons redefines intellectual property use", *Network World Peer-to-Peer Newsletter,* 29 May 2002, www.networkworld.com/newsletters/fileshare/2002/01366104.html. Accessed on 21 Nov. 2012.

Hickok, Elonnai. "Intermediary liability and state surveillance." *Global Information Society Watch 2014: Communication Surveillance in Digital Age*, Centre for Internet and Society (CIS), India, 2014.

Huey, Laura and Richard Rosenberg. "Watching the Web: Thoughts on Expanding Police Surveillance Opportunities under the Cyber-Crime Convention." *Canadian Journal of Criminology and Criminal Justice*, vol. 46, no. 5, 2004.

Hurwitz, Roger. "Depleted Trust in the Cyber Commons." *DTIC Document*, 2012.

Hustinx, Peter. "The Moment of Truth for the Data Retention Directive." Presentation at The Taking on the Data Retention Directive'Conference, Brussels, 2010.

Hustinx, Peter. "Recent developments in the European Union." *30 years after: the impact of the OECD Privacy Guidelines,* Joint ICCP-WPISP Roundtable, Paris, 2010.

Introna, Lucas D and Helen Nissenbaum. "Shaping the Web: Why the Politics of Search Engines Matters." *The information society*, vol. 16, no. 3, 2000.

Kang, Jerry. "Cyber-Race." *Harvard Law Review*, 2000.

Kennedy, John B. “Slouching towards Security Standards: The Legacy of California’s SB 1386.” *Privacy Law Institute (Seventh Annual)*, 2006

Kerr, Orin S. “The Fourth Amendment and the Global Internet.” *GWU Law School Public Law Research Paper No. 2014-30*, 2014.

Kirby, Michael. "The History, Achievement and Future of the 1980 Oecd Guidelines on Privacy." *International Data Privacy Law*, vol. 1, no. 1, 2011.

Klang, Mathias and Murray, Andrew. “Internet Service Providers and Liability.” *Human Rights in the Digital Age.* Psychology Press, Brighton, 2005.

Kokott, Juliane and Sobotta, Christoph. "The Distinction between Privacy and Data Protection in the Jurisprudence of the Cjeu and the Ecthr." *International Data Privacy Law*, vol. 3, no. 4, 2013.

Konstadinides, Theodore. "Destroying Democracy on the Ground of Defending It? The Data Retention Directive, the Surveillance State and Our Constitutional Ecosystem." *European Law Review*, vol. 36, 2011.

Koops, Bert-Jaap and Sluijs, Jasper P. "Network Neutrality and Privacy According to Art. 8 Echr." *European Journal of Law and Technology,* vol. 2, no. 3, 2012.

Kuczerawy, Aleksandra and Coudert, Fanny. "Privacy Settings in Social Networking Sites: Is It Fair?." *IFIP PrimeLife International Summer School on Privacy and Identity Management for Life*, Springer, 2010.

Kuner, Christopher. "An International Legal Framework for Data Protection: Issues and Prospects." *Computer law & security review*, vol. 25, no. 4, 2009.

Kuner, Christopher. "Developing an Adequate Legal Framework for International Data Transfers." *Reinventing Data Protection?*, Springer, 2009.

Kuner, Christopher. "European Data Protection Law." *Corporate Compliance and Regulation,* Oxford University Press, UK, 2007.

Kuner, Christopher. "Regulation of Transborder Data Flows under Data Protection and Privacy Law: Past, Present, and Future." *TILT Law & Technology Working Paper No. 016/2010*, 2010.

Lescroël, Amélie et al. "Antarctic Climate Change: Extreme Events Disrupt Plastic Phenotypic Response in Adélie Penguins." *PloS one*, vol. 9, no. 1, 2014.

Litman, Jessica. "Sharing and Stealing." *Hastings Communications and Entertainment Law Journal*, vol. 27, 2003.

Lopez-Tarruella, Aurelio. "Introduction: Google Pushing the Boundaries of Law." *Google and the Law*, Springer, New York, 2012.

LoPucki, Lynn M. "Human Identification Theory and the Identity Theft Problem." *Tex. L. Rev.*, vol. 80, 2001

Maras, Marie-Helen. "The Economic Costs and Consequences of Mass Communications Data Retention: Is the Data Retention Directive a Proportionate Measure?." *European Journal of Law and Economics*, vol. 33, no. 2, 2012

Masing, Johannes. "Herausforderungen Des Datenschutzes." *Neue Juristische Wochenschrift*, vol. 65, no. 33, 2012.

McAllister, Neil. "Senate Votes to Continue Fisa Domestic Spying through 2017-All Proposed Privacy Amendments Rejected." *The Register, December 29th*, 2012.

Medine, David et al. "Report on the Telephone Records Program Conducted under Section 215 of the USA Patriot Act and on the Operations of the Foreign Intelligence Surveillance Court." *Privacy and Civil Liberties Oversight Board, January*, vol. 23, 2014.

Mendel, Toby et al. *Global Survey on Internet Privacy and Freedom of Expression.* UNESCO, Paris, 2012.

Metcalf, Katrin N. "Legal Aspects of Privacy Law and Data Protection." *The Right to Privacy as a Human Right and Everyday Technologies*, Institute of Human Rights NGO, 2014.

Michael, Katina et al. "Planetary-Scale Rfid Services in an Age of Uberveillance." *Proceedings of the IEEE*, vol. 98, no. 9, 2010.

Milanovic, Marko. "Human Rights Treaties and Foreign Surveillance: Privacy in the Digital Age." *Harv. Int'l LJ*, vol. 56, 2015.

Minsky, Marvin et al. "The Society of Intelligent Veillance." *Technology and Society (ISTAS), 2013* IEEE International Symposium, 2013.

Mitrou, Lilian. "The Impact of Communications Data Retention on Fundamental Rights and Democracy: The Case of the Eu Data Retention Directive." *Haggerty/Samatas*, 2010.

Mnookin, Jennifer L. "Virtual (Ly) Law: The Emergence of Law in Lambdamoo: Mnookin." *Journal of Computer Mediated Communication*, vol. 2, no. 1, 1996.

Moraes, Claude. "Working Document on the US and EU Surveillance programmes and their impact on EU citizens fundamental rights." *LIBE Committee Inquiry on electronic mass surveillance of EU citizens*, Justice and Home Affairs, 2013.

Nakashima, Ellen. "Banks Seek Nsa Help Amid Attacks on Their Computer Systems." *Washington Post*, vol. 11, 2013.

Narayanan, Arvind and Vitaly Shmatikov. "Myths and Fallacies of Personally Identifiable Information." *Communications of the ACM*, vol. 53, no. 6, 2010

Narayanan, Arvind and Vitaly Shmatikov. "Robust De-Anonymization of Large Sparse Datasets." *Security and Privacy, 2008. SP 2008. IEEE Symposium on*, IEEE, 2008.

Newland, Erica and Cynthia Wong. "Data Retention Mandates: A Threat to Privacy, Free Expression, and Business Development." *Center for Democracy & Technology*, Washington, DC, 2011.

Ogura, Toshimaru. "Electronic Government and Surveillance-Oriented Society." *Theorizing surveillance: The Panopticon and Beyond*, Willan Publishing, London, 2006.

Ohm, Paul. "Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization." *UCLA Law Review*, no.197, 2009.

Olarra, Juan Carlos. "Recent Developments in the European Union." *Trusts & Trustees*, 2013.

Papakonstantinou, Vagelis and de Hert, Paul. "The Amended Eu Law on Eprivacy and Electronic Communications after Its 2011 Implementation; New Rules on Data Protection, Spam, Data Breaches and Protection of Intellectual Property Rights." *J. Marshall J. Computer & Info. L.*, vol. 29, 2011.

Raab, Charles D. "Information Privacy: Networks of Regulation at the Subglobal Level." *Global Policy*, vol. 1, no. 3, 2010.

Ramos, Mario H. "Una Vuelta De Tuerca Más a Las Relaciones En Materia De Protección De Datos Entre La Ue Y Los Estados Unidos: La Invalidez De La Decisión Puerto Seguro." *Revista General de Derecho Europeo*, no. 39, 2016.

Rauhofer, Judith. "Just Because You're Paranoid, Doesn't Mean They're Not after You: Legislative Developments in Relation to the Mandatory Retention of Communications Data in the European Union." *SCRIPTed*, vol. 3, 2006.

Rea, Kari. "Glenn Greenwald: Low-Level NSA Analysts Have 'Powerful and Invasive'search Tool." *ABC News*, vol. 28, 2013.

Reding, Viviane. "The Upcoming Data Protection Reform for the European Union." *International Data Privacy Law*, vol. 1, 2011.

Rehder, Jörg and Erika C Collins. "The Legal Transfer of Employment-Related Data to Outside the European Union: Is It Even Still Possible?" *The International Lawyer*, 2005

Richardson, Robert and CSI Director. "Csi Computer Crime and Security Survey." *Computer Security Institute*, vol. 1, 2008.

Rivero, Álvaro F. "Right to Be Forgotten in the European Court of Justice Google Spain Case: The Right Balance of Privacy Rights, Procedure, and Extraterritoriality." *European Union Working Papers*, no.19, Stanford-Vienna Transatlantic Technology Law Forum, 2017.

Roberts, Hal and Palfrey, John. "The EU Data Retention Directive in an Era of Internet Surveillance." *Access controlled: The shaping of power, rights, and rule in cyberspace*, 2010.

Rodotà, Stefano. "Data Protection as a Fundamental Right." *Reinventing Data Protection?*, Springer, 2009.

Schwartz, Paul M. "Preemption and Privacy." *The Yale Law Journal*, 2009.

Shane, Peter M. "Foreword: The NSA and the Legal Regime for Foreign Intelligence Surveillance." 2013.

Shields, Maggie. "Google Reveals Government Data Requests and Censorship" *BBC News*, 20 Apr. 2010.

Simitis, Spiros. "Reviewing Privacy in an Information Society." *University of Pennsylvania Law Review*, vol. 135, no. 3, 1987.

Singer, Natasha. "Data Protection Laws, an Ocean Apart." *New York Times*, 2013.

Smith, Benjamin D. and Daniel A. Grande. "The Current State of Scaffolds for Musculoskeletal Regenerative Applications." *Nat Rev Rheumatol*, vol. 11, no. 4, 2015.

Solove, Daniel J. "A Taxonomy of Privacy." *University of Pennsylvania Law Review*, 2006.

Solove, Daniel J. "Reconstructing Electronic Surveillance Law." *Geo. Wash. L. Rev.*, vol. 72, 2003.

Solum, Lawrence B. "Models of Internet governance." *Internet Governance: Infrastructure and Institutions,* Lee A. Bygrave and Bing, Jon. (eds), Oxford University Press, UK, 2009.

Sookman, Barry B. *Computer, Internet and Electronic Commerce Terms: Judicial, Legislative and Technical Definitions.* Carswell, 2001.

Stepanovich, Amie and Mitnick, Drew and Robinson, Kayla. "United States: the necessary and proportionate principle and US Government." *Global Information Society Watch 2014: Communication Surveillance in Digital Age*, 2014.

Strate, Lance. " The Varieties of Cyberspace: Problems in Definition and Delimitation" , *Western Journal of Communication*, Vol.63, 1999.

Svantesson, Dan J B. "The Times They Are a-Changin'(Every Six Months)--the Challenges of Regulating Developing Technologies." *Forum on public policy: A journal of the Oxford Round Table*, Forum on Public Policy, 2008.

Tene, Omer. "What Google Knows: Privacy and Internet Search Engines." *Utah Law Review, Forthcoming,* 2007.

Teubner, Gunther. "Societal Constitutionalism: Alternatives to State-Centred Constitutional Theory?", in Christian Joerges, Inger-Johanne Sand and Gunther Teubner (eds), *International Studies in the Theory of Private Law Transnational Governance and Constitutionalism*, Oxford: Hart Publishing, UK, 2004.

Thompson, Marcelo. "In Search of Alterity: On Google, Neutrality and Otherness." *Google and the Law*, Springer, 2012.

Van Alsenoy, Brendan et al. "Search Engines After'google Spain': Internet@ Liberty or Privacy@ Peril?" 2013.

Voss, W Gregory. "Preparing for the Proposed Eu General Data Protection Regulation: With or without Amendments." *Bus. L. Today*, 2012.

Walker, Clive. "Cyber-Constitutionalism and Digital Democracy." *The Internet, Law and Society,* Longman, London, 2000.

Weber, Rolf H. "Regulatory Autonomy and Privacy Standards under the Gats." *Asian Journal of WTO & International Health Law and Policy*, vol. 7, 2012.

Weiss, Martin A and Archick, Kristin. "US-EU Data Privacy: From Safe Harbor to Privacy Shield." *Congressional Research Service*, 2016.

Winston, Joel. "Letter from Joel Winston, Acting Assoc. Dir., Div. of Fin. Practices, FTC, to Christine Varney, Esq." *Hogan & Hartson*, 2001.

Wright, David et al. "Are the OECD Guidelines at 30 Showing Their Age?" *Communications of the ACM*, vol. 54, no. 2, 2011, pp. 119-127.

Yarow, Jay. "This Chart Shows Google's Incredible Domination of the World's Computing Platforms." *Retrieved April*, vol. 23, 2014.

3. Electronic Sources

"A Race to the Bottom: Privacy Ranking of Internet Service Companies." *The Citizen Lab*, 13 Jun. 2007, https://citizenlab.org/2007/06/a-race-to-the-bottom-privacy-ranking-of-internet-service-companies/. Accessed 29 Jun. 2015.

"Ashley Cole Risks England Career with Twitter Rant at FA." *The Sun*, 2012, www.thesun.co.uk/archives/football/968697/cole-twitter-shock/. Accessed 2 May 2014.

"DHS Press Secretary Arrested on Child Seduction Charges." *Associated Press*, 2006, www.foxnews.com/story/2006/04/05/dhs-press-secretary-arrested-on-child-seduction-charges.html. 2 May 2014.

"E- market- Definition of E-market in English | Oxford Dictionaries." *Oxford Dictionaries | English*, https://en.oxforddictionaries.com/definition/e-market. Accessed 1 May 2014.

"E-Marketplace Meaning in the Cambridge English Dictionary." http://dictionary.cambridge.org/dictionary/english/e-marketplace. Accessed 1 May 2014.

"Frequently Asked Questions." *Google Transparency Report,* www.google.com/transparencyreport/userdatarequests/faq/#are_the_observations_comprehensive. Accessed 31 Oct. 2012.

"Government Requests." *Google Transparency Report*, www.google.com/transparencyreport/removals/ government/. Accessed 6 Nov. 2015.

"How Online Gambling Works." *HowStuffWorks*, 2005, http://entertainment.howstuffworks.com/online-gambling.htm. Accessed 2 May 2014.

"Internet - Definition of Internet in English | Oxford Dictionaries." *Oxford Dictionaries | English*, https://en.oxforddictionaries.com/definition/internet. Accessed 2 May 2014.

"Internet Power Is the New Force for Social Impact." *Social Enterprise,* 7 Dec 2011, www.socialenterpriselive.com/section/comment/community/20111207/internet-power-the-new-force-social-impact. Accessed 20 Nov 2012.

"Internet: Need to Cite Wikipedia since It Is the Biggest Open "internet" Access Website for Common Definition." *Wikipedia*, https://en.wikipedia.org/wiki/Internet:_Need_to_cite_Wikipedia_since_it_is_the_biggest_open_%E2%80%98internet%E2%80%99_access_website_for_common_definition. Accessed 2 May 2014.

"Privacy Policy – Privacy & Terms – Google." *Google*, www.google.com/policies/privacy/. Accessed 7 Nov. 2015.

"Q1 2014 Smartphone OS Results: Android Dominates High Growth Developing Markets." *ABIresearch*, 6 May 2014, www.abiresearch.com/press/q1-2014-smartphone-os-results-android-dominates-hi/. Accessed 2 Apr. 2015.

"Surveillance | Define Surveillance at Dictionary.com." www.dictionary.com/browse/surveillance. Accessed 2 May 2014.

"Thailand's Social Media Battleground." *New Mandala*, 26 Mar 2015, www.newmandala.org/thailands-social-media-battleground/. Accessed 2 May 2015.

"Welcome to The Privacy Shield" *Privacy Shield.* www.privacyshield.gov/welcome. Accessed 11 May 2016.

"What Is a Data Subject? // A Definition from the Opt-4 Data Protection Dictionary." www.opt-4.co.uk/dictionary/DataSubject.asp. Accessed 2 May 2014.

"Complaint and Request for Injunction, Request for Investigation and for Other Relief." Federal Trade Commission, 20 Apr. 2007, www.epic.org/privacy/ftc/google/epic_ complaint.pdf. Accessed 29 Jun. 2015.

"Cyberspace - Definition of Cyberspace in English | Oxford Dictionaries." *Oxford Dictionaries | English*, https://en.oxforddictionaries.com/definition/us/cyberspace. Accessed 2 May 2014.

"Google PPC Online Advertising." *Google AdWords – Google,* https://adwords.google .com/home/. Accessed 7 Nov. 2015.

"Google Privacy Chief Talks." www.out-law.com/page-8285. Accessed 7 Nov. 2015.

"Make Money Online through Website Monetization." *Google AdSense,* www.google.com/ad sense/start/#/? modal_active=none. Accessed 7 Nov. 2015.

"Resolutions since 2004 are listed on the European Data Protection Supervisor website." *European Conference*, www.edps.europa.eu/EDPSWEB/edps/Cooperation/ Eurconference. Accessed 12 May 2015.

"Summaries of EU Legislation: The Reference for a Preliminary Ruling." *Europa*, http://europa.eu/legislation_ summaries/institutional_affairs/decisionmaking_process/l14552_en.htm. Accessed 20 Feb. 2013.

"Surveillance - Definition of Surveillance in English | Oxford Dictionaries." *Oxford Dictionaries | English*, https://en.oxforddictionaries.com/definition/surveillanc. Accessed 2 May 2014.

"Surveillance Meaning in the Cambridge English Dictionary." http://dictionary.cambridge. org/dictionary/english/surveillance. Accessed 2 May 2014.

"Timeline of the new EU Data Protection Regulation – latest developments and implementation." Allen&Overy, www.allenovery.com/publications/en-gb/data-protecti on/Pages/Timetable.aspx. Accessed 21 Jan. 2017.

"What Is an Electronic Marketplace?: Learn How Your Company Can Use E-Markets to Expand Your Business." *eMarket Services*, www.emarketservices.com:80/start/ Knowledge /index.html. Accessed 1 May 2014.

"Whitepaper: Understanding Web Filtering Technologies." *BLOXX*, www.bloxx.com/ downloads/US/bloxx_whitepaper_webfilter_us.pdf. Accessed 16 Nov. 2016.

"Why Google Pays 10 Billion USD to Its Competitor Mozilla?." *Pubarticles*, http://articles.pubarticles.com/why-google-pays-10-billion-usd-to-its-competitor-mozilla-1324916942,640235.html. Accessed 31/10/2012.

"Yahoo Privacy Center." *Yahoo,* https://policies.yahoo.com/us/en/yahoo/privacy/index.htm. Accessed 7 Nov. 2015.

Ashayagachat, Achara. "Inmates blame UDD for Ah Kong's death." *bangkokpost*, 2012, www.bangkokpost.com/lite/topstories/292704/inmates-blame-udd-for-ah-kong-death. Accessed 21 Nov. 2012.

Barwick, Hamish. "Social Networking Websites May Face Government Regulation." *Computerworld*, 16 Mar. 2012, www.computerworld.com.au/article/418730/social_ networking_websites_may_face_government_regulation/. Accessed 4 Nov. 2013.

Busby, Scott. "State Department on Internet Freedom at RightsCon." 4 Mar. 2014, www.humanrights.gov/2014/03/04/state-department-on-internet-freedom-at-rightscon/. Accessed 14 Nov. 2015.

Cushing, Tim. "Declassified FISA Court opinion shows NSA lied repeatedly to the Court as well." *Techdirt,* 21 Aug. 2013, www.techdirt.com/articles/20130821/16331524274 /declassifiedfisa-court-opinion-shows-nsa-lied-repeatedly-to-court-as-well.shtml. Accessed 14 Nov. 2015.

DLA Piper. "EU General Data Protection Regulation - Key Changes | DLA Piper Global Law Firm."www.dlapiper.com/en/uk/focus/eu-data-protection-regulation/key-changes/. Accessed 14 Jan. 2017.

Edwards, Elaine. "Independence of Data Protection Commissioner Questioned." *The Irish Times*, 28 Jan. 2016, www.irishtimes.com/business/technology/independence-of-data-protection-commissioner-questioned-1.2513682. Accessed 10 Nov. 2016.

EPIC. “Freedom of Information Act Request and Request for Expedited Processing.” 4 Feb. 2010, https://epic.org/privacy/nsa/foia/NSA-Google_FOIA_Request.pdf. Accessed 16 Nov. 2015.

Gallagher, Sean. "How the NSA’s Muscular tapped Google’s and Yahoo’s private networks." *Ars Technica*, 31 Oct. 2013, http://arstechnica.com/information-technology/ 2013/10/how-the-nsas-muscular-tapped-googles-and-yahoos-private-networks/. Accessed 6 Mar. 2015.

Gellman, Barton and DeLong, Matt. "How the NSA's Muscular program collects too much data from Yahoo and Google." *The Washington Post*. http://apps.washingtonpost.com/g/page/world/how-the-nsas-muscular-program-collects-too-much-data-from-yahoo-and-google/543/#document/p3/a129339. Accessed 28 Feb. 2015.

Gellman, Barton and Soltani, Ashkan and Peterson, Andrea. "How we know the NSA had access to internal Google and Yahoo cloud data." *The Washington Post*, 4 Nov. 2013. http://www.washingtonpost.com/blogs/the-switch/wp/2013/11/04/how-we-know-the-nsa-had-access-to-internal-google-and-yahoo-cloud-data/. Accessed 6 Mar. 2015.

Google, Facebook, Dropbox, Yahoo Abate, Tom. “Net censorship, propaganda on the rise.” *GlobalPost*, 30 May 2010, http://www.globalpost.com/dispatch/technology/090407/net-censorship-propaganda-the-rise. Accessed on 21 Nov 2012.

Google. “Google Transparency Report.” http://www.google.com/transparencyreport/userdatarequests/faq/. Accessed 31 Oct. 2014.

Hansell, Saul. "Google Wants to Dominate Madison Avenue, Too." *The New York Times*, 30 Oct. 2005, www.nytimes.com/2005/10/30/business/yourmoney/google-wants-to-dominate-madison-avenue-too.html. Accessed 7 Nov. 2015.

Ingram, Mick."Google Publishes Figures on Government Requests for Data." *World Socialist Web Site*, 26 Apr. 2010, www.wsws.org/en/articles/2010/04/goog-a26.html. Accessed 31 Oct. 2013.

Institute, Forsa. “Opinions of citizens on data retention.” 2 Jun. 2008, www.vorratsdatenspeicherung.de/content/view/228/79/. Accessed 21 Apr. 2014.

Kassim, Saleem. "Twitter Revolution: How the Arab Spring Was Helped By Social Media." 4 July 2012, https://mic.com/articles/10642/twitter-revolution-how-the-arab-spring-was-helped-by-social-media. Accessed 2 May 2014.

Kelion, Leo. “Future of the Internet Debated at NetMundial in Brazil.” *BBC*, 23/4/2014, www.bbc.com/news /technology-27108869. Accessed 16/11/2016.

Kerry, John. “Remarks to the Freedom Online Coalition Conference.” *US Secretary of State*, 28 Apr. 2014, www.state.gov/secretary/remarks/2014/04/225290.htm. Accessed 14 Nov. 2015.

Korff , Douwe. "EU-US Umbrella Data Protection Agreement : Detailed Analysis by Douwe Korff." *European Area of Freedom Security & Justice*, 14 Oct. 2015, https://free-group.eu/2015/10/14/eu-us-umbrella-data-protection-agreement-detailed-analysis-by-douwe-korff/. Accessed 12 Apr.2017.

Lardinois, Frederic. "Google, Facebook, Dropbox, Yahoo, Microsoft and Apple Deny Participation in NSA PRISM Surveillance Program." *TechCrunch*, 6 Jun. 2013. http://techcrunch.com/2013/06/06/google-facebook-apple-deny-participation-in-nsa-prism-program/. Accessed 6 Mar. 2015.

Lederman, Marty. “The Kris Paper, and the Problematic FISC Opinion on the Section 215 “Metadata” Collection Program.” *Just Security*, 1 Oct. 2013, http://justsecurity.org/2013/10/01/kris-paper-legality-section-215-metadata-collection/. Accessed 14 Feb. 2017.

Lee, Timothy B. "Here's Everything We Know About PRISM to Date." *Wonkblog*, 12 Jun. 2013. http://www.washingtonpost.com/blogs/wonkblog/wp/2013/06/12/heres-everything-we-know-about-prism-to-date/. Accessed 6 Mar. 2015.

Mahabadi, Ladan. “Price of Monopoly and Democracy, Internet and Democracy Blog.” *Price of Monopoly and Democracy*, 19 Aug. 2008, https://blogs.law.harvard.edu/idblog/2008/ 08/19/price-of-monopoly-and-democracy/. Accessed on 20 Nov. 2012.

Mahabadi, Ladan. “Price of Monopoly and Democracy, Internet and Democracy Blog.” *Price of Monopoly and Democracy*, 19 Aug. 2008, https://blogs.law.harvard.edu/idblog/2008/08/19/price-of-monopoly-and-democracy/. Accessed on 20 Nov. 2012.

Pensador, Ray. “The Surveillance State As Foucault’s Panopticon.” *Daily Kos*, 11 Sep 2013, www.dailykos.com/story/2013/9/11/1238013/-The-Surveillance-State-As-Foucault-s-Panopticon. Accessed 11 Nov 2013.

Powles, Julia. “Big Business Was the Winner at Netmundial.” *Wired UK*, April 2014. http://www.wired.co.uk/news/archive/2014-04/28/internet-diplomacy-netmundial. Accessed 14 Mar. 2016.

Reisinger, Don. "Finland Makes 1Mb Broadband Access a Legal Right." *CNET,* 14 Oct. 2009,www.cnet.com/uk/news/finland-makes-1mb-broadband-access-a-legal-right/. Accessed 20 Nov. 2012.

Robson, Paul L. "Who’s Afraid of Google?." *The Economist*, 30 Aug 2007, http://www.economist.com/node/9725272. Accessed 14 Nov. 2015.

Rosencrance, Linda. "Survey Finds Solid Opposition to Release of Google Data to Feds." *Computerworld*, 24 Jan. 2006, www.computerworld.com/article/2561275/data-privacy/survey-finds-solid-opposition-to-release-of-google-data-to-feds.html. Accessed 7 Nov. 2015.

Ruddick, Graham. "Online Shopping to Grow by £320bn in Three Years." *The Telegraph,* 7 Jun. 2015, www.telegraph.co.uk/finance/newsbysector/retailandconsumer/11657830/Online-shopping-to-grow-by-320bn-in-three-years.html. Accessed 2 May 2016.

Saturday, Aidan M and others. "Europe Revives Claims of Microsoft Web Browser Monopoly." *AppleInsider*, //appleinsider.com/articles/09/01/17/europe_revives_claims_of_microsoft_web_browser_monopoly. Accessed 21 Nov. 2012.

Schmitt, Desirée. "Taking a Look at Two Cases in the Margin of the CJEU’s “Privacy Spring.” before and after the General Data Protection Regulation: Weltimmo and Bara." *Jean-Monnet-Saar*, 2016, http://jean-monnet-saar.eu/?p=1453. Accessed 10 Jan. 2017.

Simpson, Gemma. "Google Scores Lowest in Privacy Rankings." *ZDNet*, www.zdnet.com/article/google-scores-lowest-in-privacy-rankings/. Accessed 29 Jun. 2015.

Vangie, Beal. "What Is Pay per Click (PPC)?." *Webopedia Definition* www.webopedia.com/TERM/P/PPC.html. Accessed 7 Nov. 2015.

Wearden, Graeme and Treanor, Jill. “UN Needs Agency for Data Protection, European Commissioner Tells Davos.” *The Guardian*, 22 Jan. 2015, section Technology, www.theguardian.com/technology/2015/jan/ 22/un-agency-data-protection-davos-edward-snowden. Accessed 12 Nov. 2016.

YouTube. “How Content ID Works.” https://support.google.com/youtube/answer/ 2797370?hl=en. Accessed 16 Nov. 2016.

Documents

1. International treaties

A. Under UN system

UN. *International Convention of the Protection of the Child*. 1989.

UN. *International Convention on the Protection of the Rights of All Migrant Workers and Members of Their Families*. 1990.

UN. *International Convention on the Protection of the Rights of All Migrant Workers and Members of Their Families*. 1990.

UN. *International Covenant on Civil and Political Right.* 1966.

UN. *Optional Protocol to the International Covenant on Civil and Political Rights*. 1966

UN. *Universal Declaration on Human Rights*. 1948.

B. Under Council of Europe

Council of Europe. *Convention for the Protection of Human Rights and Fundamental Freedoms*. 1950.

Council of Europe. *Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (Convention108).* 1981.

Council of Europe. *Convention on Cybercrime.* 2004.

C. EU-US Bilateral Agreements

EU-US. *Privacy Shield*. 2016

EU-US. *Safe Harbor Agreement*. 1998.

EU-US. *Umbrella Agreement*. 2016.

D. Others

WTO. *General Agreement on Trade in Services (GATS).* 1995.

EU. *Treaty on European Union (TEU)*. 2007.

EU. *Treaty on the Functioning of the European Union (TFEU)*. 2012.

League of Arab States. *Arab Charter on Human Rights*. 2004.

Organization of African Unity. *African Charter on the Rights and Welfare of the Child*. 1990.

Organization of American States. *American Convention on Human Rights*. 1969.

Organization of American States. *American Declaration of the Rights and Duties of Man*. 1948.

2. United Nations

International Law Commission. "Report on the Work of its Fifty-Eighth Session (1 May to 9 June and 3 July to 11 August 2006)." *UN Doc A/61/10,* New York, 2006.

La Rue, *Frank. Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression*. 2011.

Scheinin, Martin. *Report of the Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms While Countering Terrorism, Martin Scheinin: Addendum: Mission to the United States of America.* UN, 2007

UN General Assembly, *Forty-third Session*, *Supplement No. 40* (A/43/40). 1989.

UN Human Rights Committee (HRC). *CCPR General Comment No. 16: Article 17 (Right to Privacy), The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation*. 8 Apr. 1988.

UN Human Rights Committee. *Communication No.488/1992 Toonan v Australia*. 1992.

UN Human Rights Committee. *Communications No.1482/2006*. 2006.

UN Human Rights Committee. *Communications No.903/1999*. 1999.

UN Internet Governance Forum (IGF). *The Internet Rights and Principles Dynamic Coalition*. 2014.

UN Special Rapporteur on the et al. *Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression.* 2013.

UN. *A/HRC/17/27*. 2011.

UN. *A/HRC/23/40*. 2013.

UN. *A/HRC/27/37*, 2014.

UN. *A/HRC/28/L.27*. 2015.

UN. *A/HRC/29/32. 2015.*

UN. *A/HRC/RES/17/4*. 2011.

UN. *A/HRC/RES/5/1*. 2007.

UN. *A/RES/45/95*. 1990.

UN. *A/RES/57/239*. 2003.

UN. *CCPR General Comment No. 34*. 2011.

3. OECD

OECD, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*. 1980.

OECD Organisation for Economic and Development. *Annex to the Recommendation of the Council of Guidelines Governing The Protection of Privacy and Transborder Flows of Personal Data.* 23 Sep. 1980.

OECD Organisation for Economic and Development. *Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security*. OECD Publishing, 2002.

OECD. *Report on the Cross-Border Enforcement of Privacy Laws*. 2006.

4. Council of Europe

A. European Court of Human Rights

European Court of Human Rights. *Application 22009/93 Z v Finland,* 1997.

European Court of Human Rights. *Case 47143/60 Roman Zakharov v. Russia. 2015.*

B. Others

Council of Europe Committee of Ministers. *Resolution (73) 22 on the protection of the privacy of individuals vis-a-vis electronic data banks in the private sector.* 1973.

Council of Europe Committee of Ministers. *Resolution (74) 29 on the protection of the privacy of individuals vis-a-vis electronic data banks in the public sector*. 1974.

Council of Europe. *Explanatory Report to Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*. Strasbourg, 1973.

5. European Union

A. EU Law

EU. *Charter of Fundamental Rights of the European Union*. 2000.

EU. *Council Framework Decision 2008/977/JHA on the Protection of Personal Data Processed in the Framework of Police and Judicial Cooperation in Criminal Matters*. 2008.

EU. *Directive 95/46/EC*. 1995. (Directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data)

EU. *Directive 2000/520/EC.* 2000.

EU. *Directive 2002/58/EC*. 2002

EU. *Directive 2006/24/EC.* 2006.

EU. *Directive 2009/136/EC*. 2009.

EU. *Directive 2016/680*. 2016. (Directive on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the

prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA)

EU. *Regulation (EC) 44/2001*. 2001.

EU. *Regulation (EU) 2016/679*. 2016. (General Data Protection Regulation)

B. European Commission

European Commission, *First report on the implementation of the Data Protection Directive (95/46/EC): COM (2003) 265 final.* Brussels, 15 May 2003.

European Commission. " ." *Final Report*, 2010.

European Commission. *Agreement on Commission's EU Data Protection Reform Will Boost Digital Single Market*. Brussels, 15 Dec. 2015.

European Commission. *COM (90) 314 final - SYN 287 and 288*. Brussels, 13 Sep. 1990.

European Commission. *COM(2012)0011*. 2012.

European Commission. *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions.* Bryssel, 2014.

European Commission. *Communication From The Commission to The European Parliament and The Council Transatlantic Data Flows: Restoring Trust through Strong Safeguards, COM(2016) 117 final*. Brussels, 29 Feb. 2016.

European Commission. *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: The European Agenda on Security,* COM(2015) 185 final. Strasbourg, 28 Apr. 2015.

European Commission. *Data Protection in the European Union Citizens' perceptions: Analytical Report*. 2008

European Commission. *Draft Commission Decision pursuant to Directive 95/46/EC of the European parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield.* 2016.

European Commission. *EU Commission and United States agree on new framework for transatlantic data flows: EU-US Privacy Shield*. Strasbourg, 2 Feb. 2016.

European Commission. *EU Data protection reform on track: Commission proposal on new data protection rules in law enforcement area backed by Justice Ministers*. Luxembourg, 9 Oct. 2015.

European Commission. *European Commission launches EU-U.S. Privacy Shield: stronger protection for transatlantic data flows*. Brussels, 12 July 2016**.**

European Commission. *EU-U.S. Privacy Shield: Frequently Asked Questions*. Brussels. 29 Feb. 2016.

European Commission. *Guide to EU-US Privacy Shield.* 2016.

European Commission. *Opinion 6/2015*. 2015.

European Commission. *Proposal for a Council Decision on the signing, on behalf of the European Union, of an Agreement between the United States of America and the European Union on the protection of personal information relating to the prevention, investigation, detection, and prosecution of criminal offenses*. 2016.

European Commission. *Q&A: Guidance on transatlantic data transfers following the Schrems ruling*. Fact Sheet, Brussels, 6 Nov. 2015.

European Commission. *Questions and Answers - Data protection reform*, Brussels. 21 Dec. 2015.

European Commission. *Questions and Answers on the EU-US data protection "Umbrella agreement"*. Brussels, 1 Dec. 2016.

European Commission. *Restoring Trust in EU-US data flows - Frequently Asked Questions*. Brussels, 27 Nov. 2013.

C. Council of the European Union

Council of the European Union. *5418/16 ADD 1*. 2016.

Council of the European Union. *Internet governance principles.* 2011.

Council of the European Union. *Report on the findings by the EU Co-chairs of the ad hoc EU-US Working Group on Data Protection 16987/13*, Brussels, 27 Nov. 2013

Council of the European Union. *Statement of the Council's reasons: Position (EU) No 5/2016 C158/46*. 2016.

D. Court of Justice of the EU

Court of Justice of European Union. *C-594/12 Seitlinger and Others*. 2014.

Court of Justice of European Union. *Case 4-73 J. Nold, Kohlen- und Baustoffgroßhandlung v Commission of the European Communities***.** 14 May 1974.

Court of Justice of European Union. *Case C- 518/07 Commission v Germany.* 2010.

Court of Justice of European Union. *Case C-101/01 Criminal proceedings against Bodil Lindqvist*. 2003.

Court of Justice of European Union. *Case C-131/12 Google Inc. v Agencia Española de Protección de Datos.* 13 May 2014.

Court of Justice of European Union. *Case C-201/14 Smaranda Bara and Others v Președintele Casei Națională de Asigurări de. Sănătate and Others*. 2015.

Court of Justice of European Union. *Case C-230/14 Weltimmo s.r.o. v. Nemzeti Adatvédelmi és Információszabadság Hatóság*. 2015.

Court of Justice of European Union. *Case C-288/12 European Commission v Hungary.* 2014.

Court of Justice of European Union. *Case C-362/14 Maximillian Schrems v Data Protection Commissioner*. 6 Oct. 2015.

Court of Justice of European Union. CJEU. *Case C-293/12 Digital Rights Ireland Ltd. v. Minister for Communications, Marine and Natural Resources*. 2014.

Court of Justice of European Union. *ECLI:EU:C:2014:238 Joined cases.* 2014.

Court of Justice of European Union. *The Court of Justice Declares that the Commission's US Safe Harbour Decision Is Invalid*. 6 Oct. 2015.

E. Others

Article 29 Data Protection Working Party. *letter to Vice-President Reding WP29*. Brussels, 10 Apr. 2014.

Article 29 Data Protection Working Party. *Opinion 01/2016 on the EU – U.S. Privacy Shield draft adequacy decision*. 13 Apr. 2016.

Article 29 Data Protection Working Party. *Opinion 3/2010 on the principle of accountability*. WP 173, 13 Jul. 2010

Article 29 Data Protection Working Party. *Press Release*. Brussels, 21 Jun. 2007.

Article 29 Data Protection Working Party. *Statement of the Working Party 29 on the EU – U.S. Umbrella Agreement*. Brussels, Oct. 2016.

Article 29 Data Protection Working Party. *The Future of Privacy WP168.* 1 Dec. 2009.

Europa. *Proposal for a Directive of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data by Competent Authorities for the Purposes of Prevention, Investigation, Detection or Prosecution of Criminal Offences or the Execution of Criminal Penalties, and the Free Movement of Such Data*, *COM/2012/010final*. 25 Jan 2012.

European Data protection Supervisor. *Opinion 1/2016*. 12 Feb. 2016.

European Union Agency for Fundamental Rights. *Data Protection in the European Union: the Role of National Data Protection Authorities*. 2010

LIBE Committee Inquiry. *Electronic Mass Surveillance of EU citizens*. 2014.

Omtzigt, Pieter. *Mass Surveillance DOC.13734*. Committee on Legal Affairs and Human Rights Session, Brussels, 2015.

6. EU-US

EU-US HLCG. *Annex to Final Report by EU-US High Level Contact Group on information sharing and privacy and personal data protection.* 2009.

EU-US HLCG. *Opinion of the European Data Protection Supervisor on the Final Report by the EU-US High Level Contact Group on information sharing and privacy and personal data protection.* 2011.

7. United States of America

A. Domestic Law

Obama, Barack. *US Presidential Policy Directive 28 – Signals Intelligence Activities*. The White House Office of the Press Secretary, 17 Jan. 2014.

United States of America. Foreign Intelligence Surveillance Act. 2008.

United States of America. *Freedom Act*. 2015.

United States of America. Freedom Act. 2015.

United States of America. Freedom of Information Act. 1966.

United States of America. Homeland Security Act. 2002.

United States of America. Judicial Redress Act. 2016.

United States of America. Patriot Act. 2001.

United States of America. Privacy Act. 1974.

Reagan, Ronald. *Executive Order 12333—United States Intelligence Activities*. 1981.

B. Domestic Courts cases

United States Court of Appeal Second Circuit. *Case 678 F.3d Electronic Privacy Information Center v. National Security Agency*. 2012.

United States Court of Appeals for the District of Columbia. *Case 257 F.3d Students against Genocide v. Dep't of State*. 2001.

United States Court of Appeals for the District of Columbia. *Case 565 F.3d Larson v. Dep't of State*. 2009, paras. 857, 868; US Second Circuit, *Case 592 F.3d 60 Wilner v. Nat'l Sec. Agency*. 2009.

United States Court of Appeals for the District of Columbia. *Case 642 F.3d 1161 Roth v. Dep't of Justice*. 2011.

United States Court of Appeals for the District of Columbia. *Case 777 F.3d Martin v. Hearst Corp*. 2015.

United States Court of Appeals for the District of Columbia. *Opinion*. 20 Mar. 2012.

United States Court of Appeals Second Circuit. *Opinion ACLU v. Clapper*. 7 May 2015.

United States District Court for the District of Columbia, *Case 11-5233 EPIC vs. NSA*. Document #1373260. 05 Nov. 2012.

United States District Court for the District of Columbia, *Case 957 F. Supp. 2d 1 Klayman v. Obama.* 16 Dec. 2013.

United States District Court Memorandum Opinion. *798 F.Supp.2d 26 (D.D.C. 2011)*. 8 Jul. 2011.

United States Second Circuit Court. *Case 306 F.3d 17 Specht v. Netscape Communications Corp.* 2002.

United States Trial Court of New York state. *Case 151769/2013 Anonymous v. Does*. 3 Dec. 2014.

C. Others

Houses of the Oireachtas Tithe an Oireachtas. *European Union Data Protection Law & Policy*. 2016

U.S. Department of Commerce. *FAQ - Investment banking and audits*. 29 Jan. 2009.

US Department of Commerce, *Welcome to the U.S.-EU & U.S.-Swiss Safe Harbor Frameworks*, 9 Oct. 2015.

US Federal Trade Commission. *Safe Harbor Principles Annex*. 2000.

US Federal Trade Commission. *Safe Harbor Principles*. 2000.

White House. *The National Strategy to Secure Cyberspace*. 2003.

8. Non-Governmental Organizations

Electronic Privacy Information Center. *EPIC's Complaint against NSA*. 13 Sep. 2010.

Electronic Privacy Information Center. *EPIC's Notice of Appeal*. 9 Sep. 2011.

European Digital Rights. *The Slide from "Self-Regulation" to Corporate Censorship.* January, 2011.

Global Privacy Counsel. *Article 29 Working Party Letter to Mr. Peter Fleischer on Google*. 16 May 2007.

International Coalition of Civil Organizations on Internet Freedom. *International Principles on the Application of Human Rights to Communications Surveillance*. 2014.

International Conference of Data Protection and Privacy Commissioners. "International Standards on the Protection of Personal Data and Privacy." *Madrid Resolution*, Vol. 5, 2009.

ISO. *ISO/IEC 27001*. 2005.

ITI. *The U.S. Privacy and Data Protection Framework: Basic Characteristics and Recent Reforms*. 18 Jan. 2016.

Raab, Charles D. and Jones, Richard. *A report presenting a review of the key features raised by the political perspectives of surveillance and democracy*. 2013.

RAND Europe. *Review of the European Data Protection Directive*. 2009.

Digital Rights Ireland. *DRI challenges independence of Ireland's Data Protection Authority*. DRI challenges independence of Ireland's Data Protection Authority, 28 Jan. 2016.

Electronic Privacy Information Center. *NSA's March 10, 2010 letter acknowledging of receipt of EPIC's FOIA request and invoking the Glomar Response*. 10 Mar. 2010.

Electronic Privacy Information Center. *EPIC's May 7, 2010 Administrative Appeal to the NSA*. 7 May 2010.

9. Others

African Union. *African Union Principles on Freedom of Expression*. 2002.

APEC. *Privacy Framework.* 2005.

Republic of South Africa, *General Intelligence Laws Amendment Bill*. 2013.

United Kingdom. *Data Protection Act*. 1998.