AJLS

ASEAN JOURNAL OF LEGAL STUDIES

Journal homepage: https://www.tci-thaijo.org/index.php/AJLS

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

* Tossapon Tassanakunlapan

* Milagros Alvarez Verdugo

ABSTRACT

The goal of this article is studying the provision and implementation of Personal Data Protection in the EU-US Bloc, in order to initiate an International or Universal Regime.

Firstly, it reviews the old regime, which was enacted before the reformation process of EU and US. It shows that the legal consequences of each agreement will be different because their legal nature depends on their launching institution. The different scopes on actors and jurisdiction are critical; IT corporations are multi-national legal persons, under the appliance of the law of specific territory but their activities are trans-border. Moreover, these instruments have been created for decades so there are some out-of date provisions maintained in those legal documents. The implementation of data subjects' rights is increasingly complicated because data is decentralized and under the control of various organizations, private companies and state authorities. Furthermore, the data controller/processor has relationship with state authorities, or the existences of a conflict of interests. Hence, the individual's appeal for remedy is complex as well as the monitoring of duty bearer practice. The hard cases are presented in many court cases of the US Courts and Court of Justice of European Union, and in official reports of competent organizations.

Right to personal data protection often deals with the relationship between exercise of rights and state of emergency or prosecution of criminal and terrorism. As state authorities and courts weight up the reasons for accessing certain data and the potential effect on an individual of such state surveillance, a better necessary precondition and proportionate

solution must be provided. The EU had launched set of regional instruments in 2016. Nonetheless, the problems come from US entities, intelligence authorities and IT corporations, which are subjects under US national security laws. Accordingly, the rights of global netizens are in the realm of US jurisdiction when their personal data is transferred and it may be compromised by US Government. Thus, US was contracted to agree on bilateral instruments with the EU concerning the harmonization of data protection policies, as trade partner in a single e-market, as well as the earlier responses US took for supporting EU data subjects. These reforms of EU and EU-US regime could be extracted or used, as a model, for initiating a universal regime.

Keywords: *Personal Data Protection, Cyberspace, E-Market, Human Rights, Jurisdiction*

CONTENT

The introduction section will outline all of preliminary issues, the prerequisite knowledge and framework of the research, on personal data protection on cyberspace. The studies of this article are based on the EU and EU-US e-market regime.

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.[1] 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.[2] It is usual that attempts to create a safe online society is even harder than in an offline environment because the amount of processed data is far greater than the past.

1. The Result of Study

The objective of this research is to analyze the personal data protection in EU and EU-US regime through the time of reforms. Firstly, the research will differentiate the old regime to protect the right to personal data in the digital age by 3 main issues and the failures the US system generated. Then the controversial cases revealed during 2013 and

[1] 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.

[2] 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.

the benchmarks from EU and US Court decisions for leveling-up the data protection standard will be discussed and, after that, the springing up of reforms of personal data protection regimes that the EU and the US have launched to harmonize single e-market regulation.

1.1. Personal Data Protection under the EU and EU-US E-market legal regime prior to the 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 an international regime, the starting point will show the overlap and insufficiency of the old instruments. The old set of personal data protection laws, which was enacted before the reformation process of EU and US, had been heavily based on implementation at the domestic level.[3]

1.1.1. Predominance of US entities and its effects on global netizens

Most prominently, the discontents the US system brought to the personal data protection recourse came from a direct clash with the state intelligence operation in the national security realm.[4] The intention of US government to conduct mass electronic surveillance on activities relate to terrorism, especially on foreigners who were not under full US constitutional protection, may put further complicated situations for internet users around the world.[5] Since most of the dominant IT corporations are subjected to US or transfer personal data to servers in US territory, the different standard would be the main threat to non-US citizen internet users.

US IT corporation are subject to US domestic laws whereas the rights of global netizens are in the realm of US jurisdiction when such data is transferred to US territory or a US entity and it may be compromised by the exercise of US authorities.

The data controller, ie the US IT corporation, has an obligation to secure their data system and notify data subjects and the state Data Protection Authority (DPA), when data breaches happen. US DPA and the Federal Trade Commission, under Ministry of Commerce, have a duty to provide preparatory and supporting advice[6] especially when there were wide spread of massive electronic data surveillance by US National Security Agency. [7] Before the revelations on June 5th of 2013, both US DPA and IT corporations

---

[3] 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.

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

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

[6] 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.

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

had done nothing. To meet the Adequacy Criterion of EU,[8] the transfer of data across the Atlantic had been under a provision of the EU-US Safe Harbor Agreement, legalizing trans-border data flows.

The effectiveness of the enforcement regimes in various countries depends on the extent of judicial interpretation and on other comparative aspects of data protection laws.[9] There are processing dispute resolution procedures in the EU but not in the Safe Harbor Agreement.[10] 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.[11]

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.[12] In 2012 the EPIC appealed to the United States District Court for the District of Columbia seeking disclosure of any communications between the National Security Agency (NSA) and Google Inc. regarding encryption and cyber security.[13] Many cases lead to the revelation of cooperation between NSA and IT corporations which impacted personal data protection.

The NSA‘s PRISM project collects data from the most powerful IT corporations of the world such as Google,[14] Yahoo, Facebook etc. The identification of the place, time and activity of people could be tracked and traced orderly from big data collection[15] that gathers from cyberspace globally, including data for non-US citizens outside US territory.

Since the US Courts have made decisions which set the precedent on data collecting and sharing by IT corporations and state authorities because they are the subjects under US jurisdiction.[16] 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).[17] This

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

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

[10] 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.

[11] 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.

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

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

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

[15] 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.

[16] 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.

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

case celebrated the full constitutional rights enjoyed by the US citizen but the protection for the non-US citizen still remains.[18]

On other side of the Atlantic, Court of Justice of the European Union CJEU had launched a series of decisions relating to personal data protection by IT corporations and states, especially US national entities. Since then, 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[19] and operates by the coordination with UK, an EU Member State at that time, and has made direct breaches on personal data of data subjects around the world.

A Facebook user, who claims his data was breached by US Agencies, filed the case called the *Schrems Case* after his name.[20] 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.[21] 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."[22]

The CJEU concluded that Safe Harbor and US legislation do not provide 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, and this compromises the essence of this fundamental right, which is an important component of the rule of law.[23] Thus, the Safe Harbor decision did not contain sufficient remedies for individuals in case of violations by IT corporations or a state national authority.

Therefore, CJEU invalidated Safe Harbor on 6 October 2015. The EU and the US needed to renegotiate a new agreement to regulate data flows between both sides of Atlantic.

In conclusion, the difficulties came from the failure of the US legal system to protect the personal data of data subjects. The inadequacy of the US system brought deterioration to the personal data protection. The program of the US government to conduct mass electronic surveillance on activities related to terrorism, especially on foreigners who are out of the full US constitutional protection, may present further obscure scenarios for internet users globally.

---

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

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

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

[21] 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.

[22] 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.

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

1.1.2. Different standards and the difficulties from fragmented jurisdiction

Personal data protection has been recognized in diverse instruments from international organizations to the EU regional bloc and the 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.[24] 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.[25]

The common points and differences of definition and scope written in various sources, brings complications to the implementation of personal data protection. Many activities in the public or the private sector are under the scope of personal data protection instruments which cover large amounts of information.[26] But it has brought difficulties to individuals for exercising their right in other countries.[27] However, the different scopes are on actors and jurisdictions, as the most powerful actors who control and process personal data are IT corporations, which are multi-national legal persons and under the appliance of the law of specific territories but their activities are trans-border.[28]

The instruments recognizing the right to personal data have been created for decades so there are some out-of date provisions maintained in those legal documents. The more advances in technology, the more complexity it brought into the legal atmosphere.[29] 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.[30]

The '*fairly and lawfully*' principle provides a 'lens' through which the other provisions in the Data Protection Directive should be interpreted.[31] Since the data processor has no direct obligations to data subjects, it will impact how data protection issues are addressed

[24] Kuner, Christopher. "An International Legal Framework for Data Protection: Issues and Prospects." *Computer law & security review*, vol. 25, no. 4, 2009, p. 307.
[25] 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.
[26] Cate, Fred H. "The Failure of Fair Information Practice Principles." *Consumer Protection in the Age of the Information Economy,* 2006.
[27] 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.
[28] Kuner, Christopher. "European Data Protection Law." *Corporate Compliance and Regulation,* Oxford University Press, UK, 2007, ch.2.37.
[29] 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.
[30] 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.
[31] 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.

in the data processing business and data sharing on preventing and suppressing crime and terrorism[32] especially when the third party is subject to a different jurisdiction.[33]

The jurisdiction of EU laws and extraterritorial application of EU data protection law was re-affirmed more strongly in the *Google Spain Case.*[34] 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'.[35] The CJEU also held that the right to delete data under the EU Data Protection Directive applies to the results of Internet search engines[36] ('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 although 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,[37] and often do so in practice.[38] Court decisions from one EU Member State can also be enforced in another Member State with relative ease.[39] 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.[40] The difficulty of asserting legal rights abroad is not unique to protection of personal data, but results from the fact that there is no global legal regime for the implementation of consumer rights in cyberspace, or for the recognition and enforcement of court decisions in other countries.

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.[41] Most restrictions deal with the relationship between a state of emergency and personal data protection.[42] The state

[32] 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.
[33] Raab, Charles D. "Information Privacy: Networks of Regulation at the Subglobal Level." *Global Policy*, vol. 1, no. 3, 2010, pp. 291-302.
[34] CJEU. *Case C-131/12 Google Inc. v Agencia Española de Protección de Datos.* 13 May 2014.
[35] 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.
[36] CJEU. *Case C-131/12 Google Inc. v Agencia Española de Protección de Datos.* 13 May 2014. paras. 89-99.
[37] EU. *Directive 95/46/EC*. 1995, Article 28(6).
[38] 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.
[39] under 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.
[40] 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.
[41] Galetta, Antonella and De Hert, Paul. *A European perspective on data protection and access rights*. Vrije Universiteit, Brussel, 2013, p. 4.
[42] Nowak, Manfred. *United Nations Covenant on Civil and Political Rights: Ccpr Commentary.* Engel, Lancaster, 1993, p. 462.

authorities and courts must weigh up the reasons for accessing certain data and the potential effect on an individual of such state surveillance.[43] 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.[44] Nonetheless, most US-influenced IT corporations are a subject under US national security laws, the Patriot Act, Homeland Security Act and Foreign Intelligence Surveillance Act, which may compromise the full enjoyment of personal data protection.

Most data protection instrument impose a similar obligation on public authorities and private parties.[45] 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.[46] 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 a service provider, or other 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 the existence of any responsive records.[47] This case affirmed the exemption power of national Security to exercise secrecy mission above the protection of civil rights.

Problems emerging 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.[48] 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.

[43] 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.

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

[45] 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.

[46] 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.

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

[48] 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.

In the *Digital Rights Ireland Case*, attention focused particularly on the principle of purpose limitation,[49] on the right to access of individuals to their personal data and on the control by independent data protection authorities.[50] However, data retention needs a shred of evidence to suggest that the subject's 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.[51] In the aftermath, the Data Retention Directive was invalidated by the CJEU on 8th April 2014 since it did not meet the EU principle of proportionate and necessary exemptions.

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 the benchmarks the US and EU Courts had set in past cases, the US Government and EU Legislation Unit have launched a set of laws in the interest of reformation.

The US and EU appointed a committee to create changes for a better solution to handle the problems. Accordingly, the EU approved General Data Protection Regulation (GDPR) and Directive on Judicial and Criminal Matters was then brought to the US to sign an 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 in 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 the US Government, especially from the EU, the main e-market trading counterparts.

1.2.1. Responses of US relating to personal data protection for non-US citizen data subjects

There are initiatives from the US and EU to address the problem of personal data protection in the 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 was declared by President Obama Presidential Policy

[49] 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.

[50] 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.

[51] 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.

Directive 28 (PPD-28), to better protect personal data of all persons including non-U.S citizens worldwide. [52]

The critical improvement is the Judicial Redress Act, which 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 citizens access to U.S. courts to enforce privacy rights in relation to personal data transferred to the U.S. for law enforcement purposes.[53]

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.[54] It also introduces some new tools for international transfers, As regards adequacy decisions, the GDPR provides more precise and detailed elements that must be taken into account when assessing the level of data protection provided in the legal order of a third country.[55]

Under this privacy shield, the redress mechanism will inform a complainant 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.[56] EU citizens are capable of lodging complaints directly to their local DPAs. Remedy mechanisms determine a period for responses by a subject organization. The privacy shield also creates a new arbitration right for unresolved complaints.[57]

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.[58]

1.2.2. Harmonize legal standard Trans-Atlantic

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.[59] It provides for an effective sanctions regime by harmonizing the powers of national data protection

[52] 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.

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

[54] 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.

[55] 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.

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

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

[58] 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.

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

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.[60]

The EU-US Privacy Shield core principles are the same as Safe Harbor by harmonizing data protection within EU-US single e-Market. The Privacy Shield includes statements regarding the enforcement body, a new arbitration right, disclosures to public authorities, and the company's liability for onward transfers.[61]

The EU Directive on Criminal and Judicial Matters includes harmonized rules for international transfers of personal data in the context of criminal law enforcement cooperation.[62] 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.[63] It urges states to provide independent national data protection authorities that can afford individuals effective judicial remedies.[64]

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 at every level. The provision covers all the substantive EU data protection principles: processing standards, safeguards and individual rights.[65] The agreement provides to the data subject judicial redress rights concerning US domestic law reforms to support EU citizens. Nevertheless, it contains some inferior aspects and threats to the data protection standard of the EU: different definition, oversight and rights of the data subject to claim remedy, especially for non-EU citizens even they live in EU territory.[66]

1.2.3. Balancing the interests between the 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

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

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

[62] 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.

[63] 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.

[64] 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.

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

[66] 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.

intelligence practices with international human rights law. These include more specific definitions of the purposes for which surveillance can be undertaken.[67]

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, 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.[68] 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.[69] However, there are still some overlaps between the US framework and the new principles where US practice may fail to comply since the old court precedent, Glomar Response, remains.

Furthermore, the US reviews the USA Freedom Act which would prevent bulk collection by requiring a nexus to an investigation, bringing clarity to Section 215 of the 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.[70]

The critical improvement is the Judicial Redress Act, which extends to EU citizens the protection of 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 of 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.[71] Additionally, the Judicial Redress Act gives 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.[72] Still non-EU citizen are not entitled to enjoy these rights.

The GDPR provides comprehensive, detailed and transparent derogations to transfer personal data outside the EU, and the reform clarifies those rules in many ways.[73] The provisions on the independence, functions and powers of EU DPAs are expressed in

[67] Obama, Barack. *US Presidential Policy Directive 28 – Signals Intelligence Activities*. The White House Office of the Press Secretary, 17 Jan. 2014.
[68] European Commission. *EU-U.S. Privacy Shield: Frequently Asked Questions*. Brussels, 29 Feb. 2016.
[69] Obama, Barack. *US Presidential Policy Directive 28 – Signals Intelligence Activities*. The White House Office of the Press Secretary, 17 Jan. 2014.
[70] 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.
[71] European Data protection Supervisor. *Opinion 1/2016*. 12 Feb. 2016, p. 43.
[72] European Commission. *EU-U.S. Privacy Shield: Frequently Asked Questions*. Brussels, 29 Feb. 2016.
[73] European Commission. *Questions and Answers - Data protection reform*, Brussels. 21 Dec. 2015, p. 3.

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.[74]

The privacy shield sets 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 a more responsive and proactive system, where certification and an annual recertification process remain, but the Department of Commerce will monitor compliance via detailed questionnaires.[75] Moreover, the Federal Trade Commission will maintain a "flag list" for organizations that are subject to FTC or court orders in privacy shield cases.

The 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 which does not meet the adequacy standard.[76] 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.[77]

The 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.[78] It also expands to the whole law enforcement sector the principle of independent oversight including effective powers to investigate and resolve individual complaints.[79] 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 the EU and EU-US regime set a new harmonized standard for a liberal market economy country to follow. It could be transformed into an international treaty open for other states to ratify. The international community may use this set of standards as a foundation to draft an international instrument on personal data protection for

[74] European Commission. *Agreement on Commission's EU Data Protection Reform Will Boost Digital Single Market*. Brussels, 15 Dec. 2015, p. 3.
[75] 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.
[76] 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.
[77] 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.
[78] 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.
[79] 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.

signing and accession. The more inclusive approach would solve the problem on jurisdiction, and make the compliance of personal data protection to different jurisdictions possible.

2. Proposal for drafting an 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, through the user putting their data in a social network, or indirectly, through people using an search engine or tab bar that allows 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 self-verification by 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.[80] Notwithstanding this, laws could, in fact, prove hard to apply efficiently due to deadlocks relating to jurisdiction.

2.1. Single set of common rules

While data protection legislation has a cross-border dimension, its subsequent development has 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,[81] 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 an EU-US bilateral basis. It includes a privacy shield for fundamental personal data exchanges and an 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 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

[80] 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.
[81] 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.

processes.[82] Consequently, these set of EU-US instruments have the potential to set a standard for international data protection initiatives and for other regional organizations since it covers a vast majority of states in the regime of liberal market economy countries.

To provide 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,[83] including the provisions covering the situation at issue on the conflict of applicable law in different jurisdictions.

2.2. Regulating the high capacity trans-border entity

Since the court decision in many cases used the principle of territoriality and the "adequacy principle" to effectively address the jurisdiction, so the issue that some IT corporations might tend to artificially select which national law to comply with and which national data protection authority to deal with. The additional "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.

2.2.1. Regulating trans-national IT corporations

For employing an adequacy principle, data protection related trust-marks, particularly web seals, flags, constitute the practical extension of self-regulatory attempts by trade-counterparts in the 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 as the notification of the processing to data protection authorities confirms its lawfulness in the e-market. Look at the model of the US: the web seal program TRUSTe (originally E-Trust) was 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[84] and then the privacy shield that is open for company to register. The Privacy Shield is controlled and guaranteed by US Federal Trade Commission.[85]

By adapting the Accountability Principle of the 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.[86] They range

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

[83] 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.

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

[85] 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.

[86] 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

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.[87]

2.2.2. Regulating state intelligence agencies

In an international treaty, the part for data protection for police and criminal justice authorities, especially national and international intelligence units to counter organized crime and terrorism, will take account of the specific needs of legal enforcement.[88] 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.[89] 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.[90] However, it must respect the different legal traditions in state parties and be fully in line with the international treaties on Human Rights.[91]

2.3. Establishing the 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.[92] Moreover, all national data protection authorities should have to present activity reports annually, which will be made public.[93] All of this aims at ensuring consistency in the application of the regulation by the national authorities. The 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,[94] such as Trustmark Emblems.

---

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

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

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

[90] 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

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

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

[93] Ibid, Article 59.

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

The universal regime should settle the one-stop-shop, and businesses and individuals will only have to deal with one single supervisory authority. The one-stop-shop for individual complainants would be an important path for an effective remedy and provide greater opportunity for an internet user to contact the oversight mechanism. The accessible and affordable dispute resolution mechanisms is ideal, and 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 has exhausted domestic remedies, and as a last resort there will be an arbitration mechanism.[95] Furthermore, the redress possibility in the area of national security for state party citizen must be handled by an Ombudsperson independent from the national intelligence services involved.

Data protection for police and criminal justice authorities needs supervision by independent national data protection authorities or impartial courts, and effective judicial remedies for suffering data subjects must be provided.[96]

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[97] thereafter.

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

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

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

REFERENCES

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 Right*, European Parliament, Brussels, 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.

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

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

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

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.

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.

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.

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.

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

EU. *Directive 95/46/EC*. 1995.

EU. *General Data Protection Regulation*. 2016.

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

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. *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. *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. *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.
European Data protection Supervisor. *Opinion 1/2016*. 12 Feb. 2016, p. 43.
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, p. 278.
Galetta, Antonella and De Hert, Paul. *A European perspective on data protection and access rights*. Vrije Universiteit, Brussel, 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.
Global Privacy Counsel. *Article 29 Working Party Letter to Mr. Peter Fleischer on Google*. 16 May 2007.
Greenleaf, Graham. "Sheherezade and the 101 Data Privacy Laws: Origins, Significance and Global Trajectories." *Journal of Law, Information & Science*, 2013.
Grimm, Dieter. "Der Datenschutz vor einer Neuorientierung" *Juristenzeitung*, 2013.
Human Rights Committee. *Communication No.488/1992 Toonan v Australia.* 1992
Human Rights Committee. *Communication No.903/1999*. 1999.
Human Rights Committee. *Communication No.1482/2006*. 2006.
Hunton&Williams. *Overview of the EU General Data Protection Regulation*. 2016.
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.
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.
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.
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.

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.

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

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

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.

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

Masing, Johannes. "Herausforderungen Des Datenschutzes." *Neue Juristische Wochenschrift*, vol. 65, no. 33, 2012.

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.

Milanovic, Marko. "Human Rights Treaties and Foreign Surveillance: Privacy in the Digital Age." *Harv. Int'l LJ*, vol. 56, 2015.

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.

Nowak, Manfred. *United Nations Covenant on Civil and Political Rights: Ccpr Commentary*. Engel, Lancaster, 1993.

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

Omtzigt, Pieter. Mass Surveillance DOC.13734. *Committee on Legal Affairs and Human Rights Session*, Brussels, 2015.

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.

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

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.

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.

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.

UN. *A/HRC/RES/17/4*. 2011.

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.

United States Court of Appeal Second Circuit. *Case 678 F.3d Electronic Privacy Information Center v. National Security Agency*. 2012.

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.

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

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

Working Party Article29. *Statement of the Working Party 29 on the EU – U.S. Umbrella Agreement*. Brussels, Oct. 2016.