CROSS BORDER PERSONAL DATA TRANSFERS AND INFORMATION PRIVACY IN THE EUROPEAN UNION

MERWAN VASSEUR

MASTER DIGITAL LAW & MANAGEMENT

LAW FACULTY & ESDES

AUGUST 2022

Abstract

The aim here is to discuss the challenges facing the European Union in its mission to protect fundamental rights and freedoms while also facilitating the exchange of capital on international commercial markets. This mission is even more challenging in the field of personal data protection as they are highly volatile as well as sensitive for the integrity of their data subject.

The author wishes to thank first and foremost his mother and his sister for being incredibly supportive in a complex year. A special thanks goes to Professor Carl Olson of St John's University School of Law for helping and improving my legal writing skills. I wish to thank Professor Katherine Klonick of St John's University School of Law for transmitting her passion of information privacy and helping me realize a part of my professional project.

Of course, I wish to thank UCLY's Law faculty and ESDES for the human and academic experience, as well as my dissertation supervisor for being a passionate and great teacher, Professor Sonal Salwi.

This dissertation is dedicated to Zoe.

Table of contents

Introduction

1. The legend says that the right to privacy, and its child the right to personal data protection, were theorized because of a wedding. In late 19th century in Boston, Massachusetts Samuel D. Warren got married to the daughter of American Senator Thomas Francis Bayard Sr. Both were known in the Bostonian social elite and thus their wedding attracted the "*late nineteenth century sensationalist press*"[1]. During their wedding some uninvited press photographs managed to take some unconsented photos of the bride. It seemed to be the reason that motivated Warren to co-write the article "The Right to Privacy" with his partner and fellow lawyer, Louis D. Brandeis in 1890[2].
2. In their article, Warren and Brandeis set out to demonstrate that the industrial exploitation of the discoveries and inventions of the time such as instantaneous photography as well as new sales methods such as advertising, had favored the development of new types of invasions in the private life. Warren and Brandeis wrote about "*the right to be left alone*", simple yet unequivocal formulation. In their view, new technologies and social evolutions such as tabloid and advertising, had allowed the emergence of invasion of privacy that the common law was unable to remedy adequately because the right affected was not based on either contract or trust, or did not derive from a strictly understood private property.

3. Europe will have to wait until 1948 and the United Nations to see the right to privacy enshrined as a fundamental one in Article 12 of the Universal Declaration of Human Rights: "*No one shall be subjected to arbitrary interference with his **privacy**, family, home or **correspondence**, nor to attacks upon his honor and reputation*". Following this

[1] (Glancy, 1979)
[2] (Warren and Brandeis, 1890)

consecration, the European Convention on Human Rights consecrated the right to privacy in its 8th article (1950).

4. The advent of information technology required that it be supplemented by the right to the protection of personal data. The recognition of a right to the protection of personal data, based on the fundamental rights recognized by the member states and the European Convention for the Protection of Human Rights and Fundamental Freedoms, and in particular the right to privacy, launched the first debates in Europe on the limitations of such rights. The aggregation of the right to privacy and personal data protection was sacralized in Europe in 1995 with the Data Protection Directive 95/46. The Data Protection Directive allowed the European Union to set up the basis of personal data protection framework that will be used later. Notably it defines that some personal data may be processed only in respect of the concerned individual's privacy. The Directive also specifies that the processing of some categories of personal data is in principle prohibited, specifically when it concerns sensitive personal data. Directive 95/46 specifies the circumstances in which it is possible to derogate from the prohibition on the processing of personal data in accordance with the legitimate limits of the right to privacy. The derogations must be provided for by law and must be necessary in a democratic society. Derogations ultimately result from the reconciliation of the right to privacy with other fundamental rights.
5. The Directive was repealed in 2018 because of its lack of coercive power over the member-states, but it managed to implement strong principles still used by the European Court of Justice today.

6. The European Court of Justice's decisions on the articulation of the right to privacy and the right to protection of personal data are common. The Court considers that the fundamental right to the protection of personal data is closely linked to the right to respect for private

life. Moreover, according to the Court, the protection of personal data, resulting from the explicit obligation provided for in Article 8 of the Charter, is of particular importance for the right to respect for private life[3].

7. The Court has often reminded the right to privacy and the right to personal data protection to the rank of fundamental rights to member states and electronic communication service providers. It is imperative for any personal data processing to be interpreted in the light of fundamental rights, which according to the Court, form an integral part of the general principles it protects. The European Court of Justice has also ruled that the right to privacy and the right to protection of personal data are not absolute rights. They may be subject to limitations provided for by law and necessary in a democratic society, in particular for the prevention of serious criminality, for the protection of public order, for the protection of public health or for the protection of the rights and freedoms of others.

8. The Directive 95/46 was replaced by the General Data Protection Regulation (GDPR). The GDPR was adopted by the European Union on the 14th of April 2016. It was officially implemented in each member states' legal systems on the 25th of May 2018. The GDPR was drafted in the European logic of free flow of individuals and capitals, but said free flows aren't solely tangible anymore. Personal data being the new coveted asset, it needed to be thoroughly protected to assure the protection of the fundamental right to privacy. To protect those new forms of exchanges within the EU, the GDPR was adopted as part of the digital single market.

9. The GDPR applies to any data subject, whatever their nationality or place of residence, if their personal data has been processed on EU territory. It does apply to European public or

[3] (*Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others*, [2014])

private entities operating outside the EU but with their social siege registered in the EU and to companies of third-party countries processing the personal data of European citizen.

10. The GDPR defines personal data as any information, of any nature or type, relating to an identified or identifiable natural person (data subject)[4]. An identifiable natural person can be identified, directly or indirectly, by reference to an identifier such as a name, an identification number, location data, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person. The GDPR also extends to digital identifiers such as IP address, cookies, trackers, etc.
11. An additional layer of protection for sensitive data has been set up by the GDPR. It concerns personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs; trade-union membership; genetic data, biometric data processed solely to identify a human being; health-related data; data concerning a person's sex life or sexual orientation.

12. The processing of personal data[5] is characterized by the collection, the usage, and the storage/archiving of data. To carry out the processing of personal data, a precise purpose must always be predetermined by the data controller.
13. The collection of personal data may be written or oral transcripts, photocopies, originals, duplicates, messages, emails, mails, etc. For example: a patient's registration form, making an appointment by e-mail, your job application file.
14. The usage can take all forms: modifications, extractions, analysis, consultations, communications, broadcasts, transfers, searches, etc.
15. The conservation and archiving are carried out according to very precise rules taking in consideration the statute of limitation preexisting in each legal regime.

[4] Article 4 (1) GDPR
[5] Article 4 (2) GDPR

16. The GDPR also introduces new key actors. First and foremost, the data controller[6] determines the purposes for which and the means by which personal data is processed.
17. The data processor processes personal data only on behalf of the data controller. The data processor is usually a third party external to the company. However, in the case of groups of undertakings, one undertaking may act as processor for another undertaking.
18. Data Protection Officer. It is mandatory to designate one for public authorities, private organizations that must process large amounts of personal and/or sensitive data in the course of their activities.

19. This dissertation will discuss how the European Union, in its quest to protect its data subjects' right to privacy and to personal data protection, had to both harmonize countries and sanction key actors. Effectively, the successive regulations on personal data protection in the EU revealed issues with mass surveillance through irrational data retention periods from certain key actors in the data transfer process.

20. What regulatory balance should the European Union aim for to maintain transnational personal data transfers with third-party countries while protecting its data subjects as well as their fundamental rights and freedoms?
21. The European Union is a major actor of the international data transfer market. It needs to be able to transfer personal data safely and lawfully with third party countries. The European Union has come up with mechanisms to ensure the safety and the lawfulness of international personal data transfers(I). Protection for personal data transfers is also illustrated by the European Court of Justice's work to combat mass surveillance by member-states themselves (II).

[6] Article 4 (7) GDPR

Chapter I: Personal data transfer to third party countries

22. The European Union tends to regulate certain essential aspects of global commercial markets de facto. De facto because its different regulatory frameworks extend to third party legislations outside the Eu's initial scope with no internal legislative implementation. It is particularly the case in anti-trust regulations. The European Union is such a substantial market that almost no corporation would allow itself to not take advantage of it. The EU imposes strict regulations to all companies intending to benefit from the European single market. Thus, international commercial markets tend to adapt to European regulations to a scope wider than the original one intended by the EU. This "*natural*" legal phenomenon was theorized by Professor A. Bradford in an article for the Northwestern Law Review Vol. 107, No. 1 in 2012; as the "*Brussels Effect*". Professor Bradford summarizes it as the ability for the EU to promulgate regulations interfering with transnational markets "*without resorting to international institutions or seeking other nations' cooperation"* resulting in *Europeanization* of global commercial markets[7].

23. This phenomenon has been particularly witnessed in the years following the GDPR's implementation.

[7] Northwestern Law Review Vol. 107, No. 1 in 2012

I) Data transfers to third party countries outside EU

A) Personal data transfers to third party countries

24. International transfers of personal data to countries outside the EU are a major concern for European policy makers. Those transfers are inevitable in a globalized digital market where most data subjects use foreign technology coming from countries outside of the EU. Furthermore, the business incentives cannot be ignored as many European data controllers delegate to third party data processors. European data subjects need to be protected both from commercial profiling and governmental mass surveillance. In this objective, the General Data Protection Regulation was put in place to protect data subjects when their data is being processed in a third-party country.

25. Chapter V of the General Data Protection Regulation sets the framework for personal data transfers to third party countries and international organizations[8].

26. Under **article 45** of the GDPR, the European Commission has the power to determine whether a country outside the EU, through its domestic legislation, offers a level of protection of personal data equivalent to that guaranteed within the European Union. Such a decision authorizes data flows from the European Union to the appropriate third country, without the need for a transfer mechanism under **Article 46 of the GDPR** or a specific authorization for the transfer.

[8] www.cnil.fr (CHAPITRE V - Transferts de données à caractère personnel vers des pays tiers ou à des organisations internationales, 2022)

27. Countries recognized as adequate according to the European Commission:

- Andorra
- Argentina
- Canada
- Faroe Islands
- Guernsey
- Israel
- Isle of Man
- Japan
- Jersey
- New Zealand
- Republic of Korea
- Switzerland
- UK
- Uruguay under certain conditions

28. An adequacy decision is based on the standard of substantial equivalence. A global assessment of the country's data protection framework is done, with respect to both the data protection measures and the oversight or redress mechanisms available. When assessing the adequacy of the level of protection, the Commission shall consider the elements described in **Article 45.2** such as the rule of law, respect for human rights and fundamental freedoms, the existence and effective functioning of one or more independent supervisory authorities in the third country, etc. The Commission may also consider the existence of international commitments by the third country in the field of data protection, such as the Council of

Europe Convention 108 and the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.

29. The third-party countries that obtained an adequacy decision are constantly monitored and evaluated every 4 years by the European Commission.

30. Not all countries in the world are awarded an adequacy decision. The GDPR therefore provided for "fallback mechanisms" that allow the transfer of data to third party countries under certain precise conditions and appropriate safeguards. The absence of an adequacy decision does not make international data transfers impossible.

31. These appropriate safeguards are listed under **article 46** of the GDPR.

32. Personal data may be transferred outside the EU if the transfer is made between public authorities or bodies. The transfer needs to be contractually set up through a legally binding and enforceable contract (**Art. 46 §2-a GDPR**). The parties to the contract must be public bodies, if a private individual or entity enters the contractual relationship, it isn't an appropriate safeguard according to **article 46 of the GDPR**. As for any personal data transfer contract for any data processor and/or controller, this contract must protect the data subjects whose personal information is processed by the public authorities. **Article 46 §3, b of the GDPR** provides the possibility to consider administrative arrangements for public authorities and/or bodies that do not possess the authority to enter in those contractual relationships.

33. **Article 46 §2-c of the GDPR** provides the possibility for countries not eligible to an adequacy decision to adopt standard data protection clauses known as "Standard

Contractual Clauses" drafted by the European Commission. These Standard Contractual Clauses must be added to data transfer contracts in third party countries to protect European data subjects. The standard contractual clauses are meant to protect data subjects but also to be safeguards for transfers to third party countries that do not provide the level of protection demanded by the EU. There are two sets of standard contractual clauses, one for controllers and one for processors. The clauses for controllers are meant to protect the rights of data subjects, while the clauses for processors are meant to protect the controller's interests. The clauses for controllers require the controller to take measures to ensure the security of the data, to ensure the confidentiality of the data, and to ensure that the data is only used for the purposes for which it was collected. The clauses for processors require the processor to take measures to ensure the security of the data, to ensure the confidentiality of the data, and to ensure that the data is only used for the purposes for which it was collected.

34. However, as it will be discussed later, the Court of Justice of the European Union declared in its case *Data Protection Commissioner v Facebook Ireland Ltd and Maximilian Schrems II*, that the standard contractual clauses may not be enough when the third-party country is evidently not providing adequate personal data protection. In those cases, it is the responsibility of the data processors and controllers to establish additional measures to remedy the issue. Among these additional measures the GDPR lists Binding Corporate Rules, Approved Code of Conducts, Approved certification mechanisms and binding contractual clauses between data processors and controllers with their subcontractors.

35. Binding Corporate Rules are governed by **Article 47 of the GDPR**. They are defined as internal rules relating to the protection of personal data in private entities within the same group of companies, or a group of companies engaged in a joint economic activity, active

both in and out of the European Union, for transfers or for a set of transfers of personal data. The rules may relate to the collection of personal data and their processing, the security of personal data, the exercise of the rights of the data subject concerned and the data protection authority. The BCRs' of the private entity must consider the specificities of its own activities, to protect efficiently the rights and freedoms of the data subjects.

36. Those binding company rules mainly concerns multinational private organizations, established in several countries of the European Union and outside the European Union. The binding company rules for each organization must be recognized by the European Commission or by a competent supervisory authority.

37. **Article 40 of the GDPR** governs the use of codes of conduct. These codes are drafted on a voluntary basis by organizations and private entities. They define specific data protection rules for data controllers and their processors. They are a useful and effective accountability mechanisms. Codes of conduct provide a detailed description of what constitutes the most responsible, accountable, and ethical behavior within an industry. When it comes to data protection, the codes of conduct function as regulations for data controllers and processors to protect the integrity of data subjects.

38. In other areas of compliance law, private entities tend to benchmark their compliance to a certain regulation with approved certifications mechanisms. The General Data Protection Regulation authorizes approved certifications in its **46th article**. Thomson Reuter's glossary defines those certification mechanisms in the field of data protection as "*a voluntary mean for controllers or processors to enhance transparency and demonstrate compliance with the GDPR for their processing activities, in line with the accountability principle, and to*

enable individuals to quickly ascertain the level of data protection of relevant goods and services data"[9].

39. All data processors and data controllers must bear in mind that approved certification mechanisms, like code of conducts, are not sufficient by themselves to guarantee personal data protection and security during international transfers. To secure efficiently these transfers, data processors and controllers must guarantee that security through binding enforceable contracts to protect the rights of data subjects.

40. These appropriate safeguards provided by article 46 of the GDPR may be bypassed in certain specific situations. **Article 49 of the GDPR** provides for these specific situations. First and foremost, personal data may be transferred to a third-party country when the data subject has explicitly consented to the proposed transfer, after being informed of the specific purpose of the transfer as well as its risks in the absence of appropriate safeguards.
41. An exception may also be made to article 46 of the GDPR when, at the data subject's initiative and request, the transfer is necessary for the performance of a contract with the data processor or controller.
42. As for most regulatory measures, an exception is made when the transfer of personal data is made in the scope of public interest such as the European organization Europol.
43. An exception is also allowed according to article 49 of the GPDR when the personal data transfer is necessary for the establishment, exercise, or defense of legal claims in a judicial procedure.
44. Transfer may also be qualified as necessary under article 49 when it is done in the vital interest of the data subject or when the data subject isn't legally capable of giving consent.

[9] (Certification mechanism | Practical Law, 2022)

45. Some countries fall out of all exceptions and regulations predicted by the GDPR. These particular cases need specific international agreements with the European Union. The United States of America have benefited from a specific international agreement between 2016 and 2020.

B) The curious case of the United States

46. In October 2015, while the GDPR was still being drafted, the European Court of Justice invalidated the International Safe Harbor Principles which regulated international data transfers, notably with the US. **The U.S.-EU Privacy Shield** was officially launched on the 12th of July 2016 as a successor to the Safe Harbor Privacy Principles. The purpose of this agreement was to protect the personal data of European citizens that are stored and processed by companies and authorities based in the United States after being transferred there. It exclusively regulated the processing of personal data. The US-EU Privacy Shield was supposed to completely remedy the incompatibility of the American legal system with European regulations on the protection of personal data, and thus allow the free transfer of personal data to entities adhering to the framework. The Privacy Shield added additional guarantees for data subjects compared to the Safe Harbor system.

47. The prerequisite for the validity of the Privacy Shield was the adequacy decision by the European Commission[10], which certified that the United States had adequate data protection standards for the storage and processing of personal data from EU data subjects. The 2016 adequacy decision was reviewed annually and renewed if the required level of data

[10] www.cnil.fr (CHAPITRE V - Transferts de données à caractère personnel vers des pays tiers ou à des organisations internationales, 2022)

protection was met. The European Commission and the United States Department of Commerce conducted this review jointly with the participation of experts.

48. The EU-US Privacy Shield guaranteed European citizens comprehensive rights when personal data was transferred to certified companies in the United States. A certification mechanism was used to distinguish compliant companies from the rest. The companies that were recognized compliant to the GDPR's standards by the United States Department of Commerce were listed for every data subject's information. EU citizens could contact the companies directly to assert these rights. These companies were required to respond to citizens' concerns within 45 days. EU data subjects were guaranteed the same rights they were entitled to under Chapter 3 of the GDPR. Data subjects may address their national data protection authorities who will in their turn address the US Federal Trade Commission to enforce those rights. If no other form of agreement could be reached, an arbitration procedure with a binding arbitration decision would serve as the final decision.

49. Despite these theoretically thorough data protection measures, mass surveillance had not been completely ruled out nor regulated. Certain areas of data collection were left for broad interpretation such as counterterrorism, cybersecurity, protection of U.S. and its allied forces and other areas of concern under the Executive Order 12333 and the Foreign Intelligence Surveillance Act.

II) Case law analysis of Schrems II by the ECJ: Dismantlement of the privacy shield

A) Facts and background

50. The case originated from activist Maximilian Schrems' call for the Irish Data Protection Commissioner to invalidate the Standard Contractual Clauses used by Facebook in its transfers of personal data to its headquarters in the U.S. The personal data, both in transit to and when stored in the US, it was argued, could be accessed by US intelligence agencies. This, according to Schrems, would be in violation of the GDPR and, more broadly, EU-law.

51. In 2013, Maximilian Schrems, a young Austrian activist, took up the issue of the validity of the Safe Harbor and challenged its validity in a dispute with Facebook Ireland. Maximilian Schrems requested that the Irish Data Protection Commission (DPC) should prohibit Facebook from transferring his personal data to the United States, arguing that the law and practices in force in that country did not guarantee sufficient protection against the surveillance activities carried out by public authorities. The complaint was dismissed. The DPC rejected Mr. Schrems' request on the grounds that the European Commission had already recognized the existence of an adequate level of protection in its decision 2000/520 endorsing the Safe Harbor mechanism. The DPC considered that it could neither rule on its validity nor oppose its application by ordering the suspension of the transfer.

52. Maximilian Schrems consequently referred the matter to the Irish Supreme Court, which referred two questions to the European Court of Justice for a preliminary ruling. This led the Court to a first decision (*ECJ 6th of October 2015 Maximillian Schrems v. Data*

Protection Commissioner C-362/14)[11] invalidating the International Safe Harbor Principles. Despite this invalidation, US data controllers could still rely on the European Commission's standard contractual clauses for their data transfers, as Facebook did, for example, following the "*Schrems I*" decision. However, Maximilian Schrems also criticized the standard contractual clauses for failing to comply with European law regarding important eavesdropping and surveillance by the American authorities.

53. Following this reasoning, the DPC then referred to the Irish Supreme Court the question of whether the standard contractual clauses should also be invalidated. The Irish Supreme Court in turn referred a series of problematics to the European Court of Justice for a preliminary ruling. The cited issues concerned both the standard contractual clauses and the Privacy Shield.

54. The European Court of Justice addressed the issue of knowing whether European data subjects' personal data were sufficiently protected when processed on American soil. Following this reasoning, the European Court of Justice sought to know if the US-EU Privacy Shield could ensure a sufficient level of protection for personal data. And if the data process on American soil was done out of bounds from the Privacy Shield, the European Court of Justice questioned the efficiency of standard contractual clauses in personal data transfers from European data subject.

[11] (Judgment of the Court (Grand Chamber) of 16 July 2020 Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems, 2022)

B) On the invalidity of the Privacy Shield

55. Article 44 of the General Data Protection Regulation (GDPR) states that in the event of a transfer of data to a third country, the level of protection of individuals guaranteed by the GDPR must not be compromised. However, the European Court of Justice considers in the *Case C-311/18 – Data Protection Commissioner v Facebook Ireland Ltd and Maximilian Schrems*, known as "*Schrems II*", "*that the law of that third country* (the U.S.*) does not provide for the necessary limitations and safeguards with regard to the interferences authorized by its national legislation and does not ensure effective judicial protection against such interferences. As far as concerns effective judicial protection, it adds that the introduction of a Privacy Shield Ombudsperson cannot, in its view, remedy those deficiencies since an ombudsperson cannot be regarded as a tribunal within the meaning of Article 47 of the Charter"* (§168).

56. An Ombudsperson (under the Privacy Shield) acts as an accountable representant for US Intelligence authorities. Used mainly to facilitate access to personal data for national security purposes. The Ombudspersons was intended to provide a framework for interference with the rights of European data subjects and to provide them with a right of appeal.

57. Regarding the Ombudspersons, the Court notes in §160 of the C-311/18 case that the existence of the Ombudsman mechanism cannot mask the lack of effective guarantees against generalized access to data. The Court also notes in §195 of the same case that they do not represent a sufficient guarantee of personal data protection because of their lack of independence towards the American government, going as far as to report their activity "*directly to the Secretary of State*". Furthermore, it appears the Ombudspersons are unable to enforce any binding rulings to any intelligence authority, rendering any appeal from data

subjects ineffective. The Court considers this mechanism insufficient. Some surveillance programs fall outside the jurisdiction of the Ombudsman, so that the individuals concerned have no means of redress. Other surveillance programs do not confer enforceable rights against the U.S. authorities, including the right to an effective judicial remedy. Moreover, where the Ombudsman may intervene, the Court notes that he or she does not have functional independence, particularly with respect to the conditions for his or her dismissal, nor the power to adopt binding decisions with respect to the surveillance services.

58. The U.S. has committed itself to ensuring that organizations participating in the Privacy Shield provide an adequate level of data protection, the agreement provides for a limitation to this protection. The Court reminds us that these exceptions are allowed in the name of "*national security, public interest, and law enforcement requirements*" (§164). Recital 136 of the Privacy Shield adds that this interference by U.S. Intelligence authorities in data subjects' personal data is limited *"to what is strictly necessary to achieve the legitimate objective pursued and that there is effective judicial protection against interference of this nature"* (§167).

59. Referring to its first Schrems judgment, the European Court of Justice considers that the interference of the American Intelligence authorities necessarily infringes Articles 7 and 8 of the EU's Charter of Fundamental Rights (§ 169 to 171) regarding the right to privacy and to personal data protection. However, the Court does not qualify those articles as "absolute prerogatives" (§172). The limitation of these rights is tolerated only if it is proportionate, necessary, and provided by law, considering the effective and enforceable rights of the concerned data subjects.

60. The Court argues that among all data protection deficiencies in American legislature, the interferences from U.S. surveillance and intelligence programs and authorities are of a great concern.

61. Section 702 of the Foreign Intelligence Surveillance Act (FISA) of 1978 named "PROCEDURES FOR TARGETING CERTAIN PERSONS OUTSIDE THE UNITED STATES OTHER THAN UNITED STATES PERSONS"[12] and the Executive Order (E.O.) 12333 of 1981 titled "United States Intelligence Activities" are the two main statutes at issue. The European Court of Justice rules that they allow intelligence and surveillance agencies to collect and process important amount of personal data, including data on European data subjects. The collection and processing of personal data by those agencies interfere with the rights guaranteed under the GDPR. It is stated that Section 702 of FISA does not precise any limitation or scope of action for their surveillance program, which goes into contradiction with the GDPR's principle of predefined and limited data collection (§180)[13]. The Court held that Section 702 of the Foreign Intelligence Surveillance Act (FISA) does not provide a level of protection substantially equivalent to that of the Union in that the authorization provided for its foreign intelligence surveillance program does not include any limitations or safeguards for the non-American persons concerned, whose rights are not enforceable against the U.S. authorities before the courts (§178 to 181). Moreover, the Court argues that some U.S. Intelligence authorities are not concerned by any type of redress mechanism from a data subject who would have been victim of an unlawful electronic surveillance and/or personal data collection. And "*such a lacuna in judicial protection in respect of interferences with intelligence programmes based on that*

[12] Govinfo.gov. 2008. *To amend the Foreign Intelligence Surveillance Act of 1978 to establish a procedure for authorizing certain acquisitions of foreign intelligence, and for other purposes.* [online] Available at: https://www.govinfo.gov/content/pkg/BILLS-110hr6304pcs/html/BILLS-110hr6304pcs.htm.
[13] *Data Protection Commissioner v Facebook Ireland Ltd and Maximilian Schrems* [2020] C-311/18 (European Court of Justice).

presidential decree makes it impossible to […] *that United States law ensures a level of protection essentially equivalent to that guaranteed by Article 47 of the Charter*" (§191). The Court found that it is the case for EO 12333 which does not provide the required data protection, nor does it render U.S. authorities accountable. This unaccountability is due to the fact that the rights created by EO 12333 are not binding nor enforceable against U.S. Intelligence authorities.

62. These statues are even more detrimental to the European fundamental rights and freedoms, as they allow the U.S. intelligence authorities to collect data on a massive scale without necessarily associating it with a specific target, nor framing it by judicial surveillance (§ 183 and 184). Thus, these texts contravene Article 52 of the Charter of Fundamental Rights' principle according to which limitations to fundamental rights may be authorized only if they are proportional, necessary, and done in the scope of general interest (§ 185).

63. Moreover, the Court recalls that the absence of a right to an effective judicial remedy disregards the essential content of the fundamental right to effective judicial protection. This factor must be considered when assessing the adequacy of the level of protection, as data subjects may have to bring their complaints against data processing operations carried out by U.S. authorities before American courts (§189). In this regard, the Court notes that European Data subjects do not enjoy the protection offered to American citizens regarding the protection of their privacy. It concludes that the data protection shield does not provide guarantees equivalent to those provided for in the Charter. In doing so, the Court held that the data protection shield is incompatible with Union law and declared it invalid (§201).

C) The Standard Contractual Clauses' personal data protection insufficiency

64. Amongst the issues treated by the European Court of Justice in "Schrems II" was the invalidity of the U.S.-EU Privacy Shield on the basis that American legislature did not offer sufficient guarantees to comply with GDPR standards and protect European data subject. By rendering the Privacy Shield void, the Court invalidated the European Commission's adequacy decision for the United States. As introduced before in this dissertation, in the absence of adequacy decision, **Article 46** and following of the GDPR dictates that a transfer of personal data to a third-party country may happen only if appropriate safeguards were provided and if the data subjects have enforceable rights and effective remedies.

65. The European Court of Justice dedicates an important part of its syllogism to the issue of standard contractual clauses usage on American soil. Standard contractual clauses (SCC) are not binding to third countries, a technicality that raised the issue of its capability of ensuring data protection for European data subjects. The Court reminds us that no adequacy decisions are required to adopt SCCs in third party countries as they do not aim to harmonize an entire legislation but rather a contractual relationship. The purpose of the standard clauses is to provide a model that facilitates the provision of appropriate safeguards by data exporters and the uniformity of those safeguards. While the decision adopting the standard clauses has no normative value of its own, it is the incorporation of these clauses into an international data transfer contract that gives them a contractual nature and binding force. The Court also reminds us that the application of standard clauses does not in itself guarantee the lawfulness of the processing operation consisting in transferring the data; it depends on the legal basis and the purpose of the processing.

66. Moreover, as detailed above, for the European Court of Justice, the American legal system does not provide European data subjects with a level of protection that is considered adequate, and the standard contractual clauses do not fully remedy the problems raised.
67. Indeed, the standard contractual clauses are only binding on the parties to their conclusion. They do not entail any obligation for the authorities of the third country. Therefore, depending on the state of the law and practices in the third country, they may not fully remedy the shortcomings in the protection of the data subject.

68. Unlike adequacy decisions, it is up to data controllers and processors to ensure that the use of standard clauses ensures this level of protection.
69. In the event of access to data by the public authorities of the third country, the exporter of the data must consider the relevant elements of the legal system of the third country and ensure that the protection of data resulting from the use of standard clauses will not be jeopardized. Unless the data exporter can ensure additional safety mechanisms such as data encryption, SCCs would be useless in a third-party legislation where no sufficient data protection regulation is in place. It is not limited to standard contractual clauses, but extends to all mechanisms for providing appropriate safeguards, such as binding corporate rules, certification mechanism or appropriate safeguards subject to authorization by the competent supervisory authority.
70. The European Court of Justice has held, in order to invalidate the Privacy Shield, that the level of data protection in the U.S. is not substantially equivalent. The disregard of the proportionality requirement and the lack of an effective judicial remedy cannot be compensated for by the standard data protection clauses. Thus, a transfer of data to the United States cannot take place on this basis or on other appropriate guarantees. The Court also considers that the supervisory authorities are required to suspend or prohibit the transfer

of personal data when the standard contractual clauses cannot be complied with in the third country and a level of protection equivalent to that resulting from Union law cannot be ensured. In this sense, the Irish Data Protection Commissioner ordered the temporary suspension of transfers by Facebook Ireland to the United States, but the Irish Supreme Court suspended this decision.

71. The European Court of Justice specifies the conditions for the validity of the decision to adopt standard contractual clauses.

72. The SCCs must include effective mechanisms to ensure a level of data protection equivalent to the European standards. If no such standard of protection is reachable, the data exporter must suspend, at least temporarily, the data transfers. These mechanisms result in a set of obligations on the exporter and importer of the data and in the recognition of rights for the data subjects. To ensure an equivalent level of protection, SCCs require the parties to the contract to process data in accordance with the GDPR. In the presence of a data importer acting as a processor, the obligations of a processor under the GDPR are declined, namely the prohibition to process data outside the instructions of the controller, the obligation to put in place technical and organizational measures to ensure compliance of the processing, the obligation to ensure the confidentiality and security of the data, the obligation to cooperate with the exporting controller in exercising the rights of the data subjects or the obligation to notify personal data breaches. Moreover, with respect to compliance with these clauses, the parties must first ensure that the legislation of the country of destination allows the importer of the data to comply with them.

73. In the event of a breach of the clauses or inability to comply with them, the standard contractual clauses provide for an obligation to inform the data importer of its inability to

comply with its obligations under the contract. For example, if the state of the law or a change in the law negatively affects the guarantees and obligations offered in the contract, then it is provided that the exporter of the data may suspend or terminate the contract and the importer must return or destroy the data. If, despite notification of the change in legislation by the country of destination, the exporter wishes to continue transferring the data, he must inform the supervisory authority so that the latter can assess the compliance of the data processing. The supervisory authority may decide to suspend or prohibit the transfer as a corrective measure.

74. Although the standard contractual clauses remain valid, it is now extremely complicated for a European entity to use them to control a transfer to the U.S., even if the European Court of Justice does not explicitly rule on this point.
75. The data controller must either ensure that its American co-contractor does not fall under the scope of the contentious surveillance laws, which is rare in practice, or implement measures to satisfactorily regulate these laws, which is a priori impossible for a private actor.

76. Thus, the content of the standard contractual clauses must guarantee an adequate level of data protection and, when this can no longer be guaranteed, the transfer must be stopped.

D) Specific derogations

77. The only alternatives presenting themselves to data exporter and importer in the U.S. are the specific derogations **under Article 49 of the GDPR**. These specific derogations place

a significant legal risk on the parties to the contract. The level of legal insecurity and unpredictability is significant when a contract is not protected by either an adequacy decision or by SCCs. The entire risk is borne by the parties, who must consent to this "unregulated" transfer to make it valid. To compensate the risk, those unregulated transfers need to be occasional and relatively small in scope.

78. This presents an issue for the European Court of Justice. Now that the U.S.-EU Privacy Shield has been invalidated, that the SCCs have been judged as inefficient as protection mechanisms by themselves in data transfers to the U.S., remains the question of data transfers under the Article 49 of the GDPR. The Court has established numerous times the incompatibility of the American legislature with GDPR-standards of data protection, if it would completely ban any data transfer to the U.S. it would render the derogations introduced by Article 49 useless. It would mean that for any third-party country, the absence of an adequacy decision or of numerous safeguards added to the SCCs is synonym of impossibility to export or import personal data from the EU, even under Article 49's exceptions.

79. Thus, even though the Court in its case "Schrems II" only specifically invalidated the Privacy Shield and pointed out the insufficiency of SCCs, the fact is that all personal data transfers to the U.S. are forbidden. They are forbidden either by the Court's decision or by the data protection authorities who will consider any personal data transfer to the U.S. as a situation in which a violation of fundamental rights could occur.

80. The European Court of Justice's Case C-311/18 *Data Protection Commissioner v Facebook Ireland Ltd and Maximilian Schrems* (2020) was symptomatic of the European "war" on unregulated mass surveillance to protect European data subjects and their fundamental rights. This war goes further than the transfer of personal data to third party countries (II).

Chapter II: The turbulent balance between personal data protection and mass surveillance

81. The regulation of mass surveillance is illustrated in the European Court of Justice's decisions condemning the generalized and unjustified retention of personal electronic communications while still taking in consideration important exceptions(A). These decisions allow us to open the discussion on possible future evolutions of European legislation on the matter (B).

I) The EU's condemnation of generalized and undifferentiated retention of personal data

82. The European judge has constantly reiterated his condemnation of any mass storage of data in a generalized and undifferentiated manner[14]. This jurisprudence was repeated in the Schrems judgment of October 6, 2015[15], but also and above all in the European Court of Justice decision *Tele2 Sverige AB v Post-och telestyrelsen and Secretary of State for the Home Department v Tom Watson and Others C-203/15* from the 21st of December 2016. It drew the consequences at the Irish national level of the invalidation of Directive 2006/24/EC, enjoining providers of electronic communication services, to retain communications metadata for the purpose of fighting important criminality or terrorism.

83. The French Conseil D'Etat in its preliminary question in the Case C-511/18 to the European Court of Justice argued that the serious and permanent threats to national security, and in

[14] (*Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others*, [2014])
[15] (*Maximillian Schrems v. Data Protection Commissioner*, [2015])

particularity terrorism justified the obligation of generalized and undifferentiated retention by electronic communications providers[16].

84. In the case C-511/18 *La Quadrature du Net e.a. contre Premier ministre e.a.* from the 6th of October 2020, the European Court of Justice first had to dispel doubts about the applicability of Directive 2002/58, "Privacy and Electronic Communications".
85. Several Member States contested the applicability of the directive on the grounds that it could not apply to national regulations aimed at safeguarding national security, an area for which they alone are responsible and sovereign. The Court interpreted Article 15(1) of Directive 2002/58[17], as a legislative measure mandating electronic communications service providers to retain traffic and location data, but also as a legislative measure mandating them to grant access to those data to the competent authority (§96).
86. The Court interpreted the Directive according to its finality and objectives. Reminding us that the purpose of the Directive is to protect data subjects from the increased risks of mass automated data storage, collection, and processing (§106). This objective lies in the same legal ideology that gave birth to the GDPR and its regulations around personal data transfers towards third-party countries.
87. The Court will therefore consider that the storage of traffic and location data constitutes not only a derogation from Article 5(1) of Directive 2002/58, but also an interference with the fundamental rights to respect for private life and to the protection of personal data,

[16] (*Demande de décision préjudicielle présentée par le Conseil d'État (France) le 3 août 2018 – La Quadrature du Net, French Data Network, Fédération des fournisseurs d'accès à Internet associatifs, Igwan.net / Premier ministre, Garde des Sceaux, ministre de la Justice, Ministre de l'Intérieur, Ministre des Armées*, [2018])
[17] "*Member States may adopt legislative measures to restrict the scope of the rights and obligations (…) when such restriction constitutes a necessary, appropriate, and proportionate measure within a democratic society to safeguard national security (i.e., State security), defense, public security, and the prevention, investigation, detection, and prosecution of criminal offences or of unauthorized use of the electronic communication system (…). To this end, Member States may, inter alia, adopt legislative measures providing for the retention of data for a limited period justified on the grounds laid down in this paragraph (…)*" – Article 15(1) of Directive 2002/58

enshrined in Articles 7 and 8 of the Charter of Fundamental Rights of the European Union. The Court recalls the extent to which these data are likely to reveal information on many aspects of the private life of the persons concerned, including sensitive information[18]. Taken as a whole, such data may make it possible to draw very precise conclusions about the private life of the persons whose data have been stored, such as their daily habits, permanent or temporary places of residence, daily or other movements, activities, social relations, and social circles frequented by these persons. "*These personal data provide the means to establish the profile of the persons concerned, information which is just as sensitive, regarding the right to privacy, as the content of the communications themselves*" § 117).

88. As for all fundamental rights, a limitation to that right is appropriate if it constitutes a necessary, appropriate, and proportionate measure within a democratic society to safeguard national security, defense, and public safety, or to ensure the prevention, investigation, detection, and prosecution of criminal offences. However, the Court reminds its readers that derogations and limitations to those rights cannot, under any circumstances, become the rule (§106). The exception must never become the principle. Recalling the principles of its classic proportionality review, the Court noted that derogations from the principle of confidentiality of communications can only be accepted insofar as they appear to be necessary, appropriate, and proportionate in a democratic society in the light of the objectives pursued.

89. The Court re-emphasizes the superior nature of the objective of safeguarding national security, it justifies limitations to fundamental rights and thus to generalized and undifferentiated personal data retention (§136). Data collected and processed for this

[18] (*Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others*, [2014])

national security purpose are authorized by the Court to be massively stored in a generalized and undifferentiated manner, on the double condition that it is for a limited period, and that the existence of a serious threat to national security that is real and present or foreseeable is recognized.

90. However, the Court precises that for “lower” risks to public safety such as “serious” criminality, generalized and undifferentiated personal data retention remains impossible (§141). Under the justification of combating serious criminality and ensuring public safety, the Court does allow targeted retention of traffic and location data (§146).

91. Exceptions to the principle of prohibiting mass storage in a generalized and indiscriminate manner also include legislative measures providing for the preventive retention of IP addresses and civil identity data for the purpose of fighting crime and safeguarding public security. According to the Court, such data are "less sensitive than other traffic data" (§152), even though it may allow digital profiling (§153). For the Court, a legislative measure providing for the generalized and undifferentiated retention of IP addresses alone does not appear, in principle, to be contrary to Article 15(1) of Directive 2002/58, read in the light of Articles 7, 8 and 11, provided that this possibility is subject to strict compliance with the substantive and procedural conditions governing the use of such data. The Court emphasizes, however, that only the fight against serious crime and the prevention of serious threats to public security are of such a nature as to justify this interference, as is the safeguarding of national security.

92. The last exception made by the Court consists of data relating to the civil identity of data subjects, data which, by their very nature, do not provide any sensitive information on their private life. For this reason, the Court considers that the interference entailed by the storage of such data cannot, in principle, be qualified as serious (§ 157). It therefore concludes that

the processing of such data, in particular their storage and access for the sole purpose of identifying the user concerned, and without such data being linked to information relating to the communications made, are likely to be justified by the objective of "*prevention, investigation, detection and prosecution of criminal offences in general*" (§ 158). Here, the Court clearly follows the GDPR's logic on the lawfulness of personal data processing, allowing for public interest without causing any prejudice to the concerned data subjects.

II) Possible legislative evolutions

93. If the European Court of Justice seems to call into question numerous State practices in intelligence or judicial procedures, a careful reading of these judgments shows that it nevertheless leaves room for national legislators to draw up new ways of reconciling the two a priori irreconcilable requirements of security and freedom.

94. These decisions opened the debate in the European Union. While the EU, as an international organization, firmly banned generalized and undifferentiated personal data retention for Intelligence agencies, the member states declare that surveillance in the objective of public safety falls under their sovereignty. However, the precedent created by case law *Tele2 Sverige AB v Post-och telestyrelsen and Secretary of State for the Home Department v Tom Watson and Others C-203/15* should lead to more scrutiny in the way intelligence authorities collect, process and stock personal data. In theory, following this precedent, no personal data retention by a governmental agency should be authorized on the sole basis of reasonable efficiency. Such retention should only be allowed when the importance of the situation justifies that this retention is the best mechanism to ensure public safety. Therefore

generalized, and undifferentiated personal data retention was only allowed by the Court in cases of serious threat to national security, as explained before.

95. However, the tensed geopolitical context of the past half-decade (terrorism, espionage, wars in Europe, etc.) made the debate fiercer; as a data retention regime, not as an exception but as the rule, was considered by some member-states. The case C-203/15 ensured that it won't happen as the Court emphasized on the need for limitations to fundamental rights to be exceptional and temporary.

96. The European Commission proposed a directive, the Digital Services Act, on the protection of personal data processed by law enforcement authorities (through electronic communication services providers) a few months after the Court's decisions. The directive was drafted to comply with the above-mentioned precedent. The directive, which was then under discussion by the European Parliament, had the objective of providing strict safeguards for the collection, storage, retention, and exchange of personal data processed by law enforcement authorities, to balance the interest of public safety with the need to protect the fundamental rights of individuals. In particular, the directive would have established a clear legal basis that would restrict the collection, retention, and use of personal data to cases where it is necessary and proportionate to prevent, investigate, detect, or prosecute criminal offenses or threats to public security. The directive would also have created a specific obligation for data retention, which would be subject to conditions that would ensure that personal data is collected and used only for purposes that are strictly necessary in a democratic society. The directive was first rejected by the European Parliament before coming to a pre-agreement in April 2020[19].

[19] (DSA : le règlement sur les services numériques vise une responsabilisation des plateformes, 2022)

97. Another first step in the right direction was taken by the European Commission with the proposal of the e-Privacy Regulation. The e-Privacy Regulation would extend the scope of the GDPR to any service that offers electronic communications, such as WhatsApp, Gmail, and Facebook. The regulation would ensure that the same rules apply to all electronic communication service providers, regardless of their business model. The regulation would also establish rules to protect the confidentiality of electronic communications, including the prohibition of electronic communications service providers from processing electronic communications data without the consent of the users. The regulation is currently under discussion by the European Parliament. The regulation would establish a European regime for the protection of electronic communications data, including data retention, data disclosure, and data protection. It would also establish rules to ensure that electronic communications data is only processed in a way that is necessary and proportionate to the legitimate interests of the state.
98. The European Union is currently facing a major challenge in the field of data protection. The European Court of Justice has repeatedly ruled that the European Union must ensure that its member states comply with the European Convention on Human Rights and the Charter of Fundamental Rights of the European Union. However, the European Union has not yet adopted a comprehensive framework for the protection of personal data.

99. Member states who haven't already complied with the new standards introduced in the discussed case-laws should encounter a coercive pressure from the European Union, as it was the case for the basic standards of the GDPR between 2018 and 2020. Or they will see their internal regime on personal data retention evolve as case-laws accumulate on the precedent of the cited cases. Data subjects will probably action constitutional reviews

against electronic communication providers storing personal data for governmental authorities.

100. As mentioned before, the European Court of Justice through its many impactful cases and the GDPR aim for the same objective, the protection of European data subjects and their fundamental rights. While the GDPR focuses on technical, legal, and contractual mechanisms to protect personal data, the European Court of Justice aims to force electronic communication service providers, and the governmental authorities they work with, to comply and respect European fundamental rights in all judicial and legal procedures. Simply put, while the GDPR acts *a priori*[20], the European Court of Justice acts *a posteriori*.

101. A serious challenge awaits the European Union for future regulations. The cases cited in this dissertation have brought into light the necessity to define data subjects and their personal data according to certain identifiers and markers. For electronic communication service providers and governmental authorities not to store personal data generally and indifferently, legislators may have to rely on social profiling. By refusing massive data retention under most circumstances, the Court may have to accept data retention based on ethnic, social, religious, political groups. However, such division of citizens is prohibited in most member-states of the EU, such as France[21], and is a flagrant disrespect to the fundamental rights the European Convention on Human Rights[22] and the Charter of Fundamental Rights of the European Union[23]

[20] Even though national data protection authorities have the power to fine GDPR violators.
[21] Article 226-19 of the French Penal Code
[22] (European Charter of Human Rights, 2006)
[23] (Charter of Fundamental Rights of the European Union, 2000)

Conclusion

102. Personal data transfers are inevitable. The European Union, in its grand enterprise of expanding its single market in a digital single market, had to compromise and find a regulatory balance between facilitating personal data transfers and protection the fundamental rights and freedoms of its data subjects. The General Data Protection Regulation allowed the EU to implement a safe regulatory framework for personal data transfers to third party countries. The issue was to safely guarantee those transfers with countries possessing a data protection regime below the European standards. It was the case for the United States, compelling the European Court of Justice to invalidate the U.S.-EU Privacy Shield for issues of mass surveillance and shortcomings in the protection of data subjects' rights.

103. The European Court of Justice has served as a legislative and judicial safeguard against limitations on fundamental rights and freedoms in the context of mass surveillance. In this optic, through different complex cases, the Court has reminded every key actor in the data processing industry, whether they be electronic communication service providers or governmental authorities, of the relative prohibiting of generalized and undifferentiated personal data retention. Relative prohibition because the Court's decision was symptomatic of legislative and judicial safeguards permissibility towards limitations of fundamental rights in the name of national safety.

Bibliography

Bradford, A., 2012. The Brussels Effect. *Northwestern Law Journal*, 107(1).

Practical Law. 2022. *Certification mechanism | Practical Law*. [online] Available at: <https://uk.practicallaw.thomsonreuters.com/w-014-8170?transitionType=Default&contextData=(sc.Default)&firstPage=true> [Accessed 25 August 2022].

2022. *CHAPITRE V - Transferts de données à caractère personnel vers des pays tiers ou à des organisations internationales*. [online] Available at: <https://www.cnil.fr/fr/reglement-europeen-protection-donnees/chapitre5#:~:text=Un%20transfert%20de%20données%20à,internationale%20en%20question%20assure%20un> [Accessed 24 August 2022].

Europarl.europa.eu. 2022. *Charter of Fundamental Rights of the European Union*. [online] Available at: < https://www.europarl.europa.eu/charter/pdf/text_en.pdf > [Accessed 26 August 2022].

Data Protection Commissioner v Facebook Ireland Ltd and Maximilian Schrems [2020] C-311/18 (European Court of Justice).

Demande de décision préjudicielle présentée par le Conseil d'État (France) le 3 août 2018 – La Quadrature du Net, French Data Network, Fédération des fournisseurs d'accès à Internet associatifs, Igwan.net / Premier ministre, Garde des Sceaux, ministre de la Justice, Ministre de l'Intérieur, Ministre des Armées [2018] C-511/18 (European Court of Justice).

Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others [2014] C-293/12 (European Court of Justice).

Douville, T., 2020. *Invalidation du Privacy Shield et insuffisance des clauses-types : fin (temporaire ?) des transferts de données à caractère personnel vers les États-Unis*. Aj Contrat. Dalloz, p.436.

vie-publique.fr. 2022. *DSA : le règlement sur les services numériques vise une responsabilisation des plateformes*. [online] Available at: < https://www.vie-publique.fr/eclairage/285115-dsa-le-reglement-sur-les-services-numeriques-ou-digital-services-act > [Accessed 26 August 2022].

Echr.coe.int. 2006. *European Charter of Human Rights*. [online] Available at: <https://www.echr.coe.int/documents/convention_eng.pdf> [Accessed 26 August 2022].

Glancy, D., 1979. The Invention of the Right to Privacy. *Arizona Law Review*, 21(1), p.6.

Curia.europa.eu. 2022. *Judgment of the Court (Grand Chamber) of 16 July 2020 Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems*. [online] Available at:<https://curia.europa.eu/juris/document/document.jsf?text=&docid=228677&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=4594815 > [Accessed 25 August 2022].

Maximillian Schrems v. Data Protection Commissioner [2015] C-362/14 (European Court of Justice).

Govinfo.gov. 2008. *To amend the Foreign Intelligence Surveillance Act of 1978 to establish a procedure for authorizing certain acquisitions of foreign intelligence, and for other purposes.* [online] Available at: < https://www.govinfo.gov/content/pkg/BILLS-110hr6304pcs/html/BILLS-110hr6304pcs.htm > [Accessed 24 August 2022].

Warren, S. and Brandeis, L., 1890. The Right to Privacy. *Harvard Law Review*, IV(5).