Nadine Ramos Mendes

EU – U.S. data transfers, data protection, and foreign surveillance: an irreconcilable reality?

Dissertation to obtain a Master's Degree in Law,
in the specialty of International and European Law

Supervisor:

Doctor Francisco Pereira Coutinho, Professor at NOVA School of Law

September 2022

Declaração antiplágio

Declaro por minha honra que o trabalho que apresento é original e que todas as minhas citações estão corretamente identificadas. Tenho consciência de que a utilização de elementos alheios não identificados constitui uma grave falta ética e disciplinar.

(Nome e assinatura do/a aluno/a)

Lisboa, 15 de setembro de 2022

Nadine Ramos Mendes

Anti-plagiarism statement

I hereby declare that the work I present is my own work and that all my citations are correctly acknowledged. I am aware that the use of unacknowledged extraneous materials and sources constitutes a serious ethical and disciplinary offence.

(Student's name and signature)

Lisbon, 15th September 2022

Nadine Ramos Mendes

Acknowledgements

Thank you to my supervisor, Professor Francisco Pereira Coutinho, for his precious advice and guidance.

To my family, without whom I wouldn't be able to write this thesis, thank you for your silent but steady support and companionship. You gave me the strength to write when I thought I couldn't.

To my partners-in-study, with whom the multiple trips to the library and study sessions online gave me the motivation I sometimes lacked and made me feel less alone in this unique endeavour, I'm grateful beyond words. To my best friend, who never stopped believing in me and who pushed me to go outside when I needed it most, thank you for always cheering me up.

Last, but not least, thank you to all the friends I made, colleagues I worked with, people I met, and professors I looked up to during my academic journey – all of you made academia more special and fascinating.

Quoting and other conventions

This thesis was written following the rules of British English except when directly citing documents written in American English.

Regarding citation, I opted for footnote citations following the Portuguese Norms 405-1 and 405-4 of the Portuguese Quality Institute. To render the thesis more legible, I chose to only add the URL link to footnote citations relating to information obtained from news outlets online, blogposts or official websites. Otherwise, the URL link to other types of sources including academic articles, statutes and case law will be available in the bibliography. More specifically, citation will stick to the following models:

- Academic articles: LAST NAME, First name – Title of the article. Title of the review. Volume, number/issue, page(s) cited. [date of access].
- Webpages and websites: LAST NAME, First name – **Title of the article**. Name of the website. Date of writing. [date of access]. <URL>.
- EU legislation: Name of the law, Official Journal of the EU (OJ) reference, date of publication, page location in the OJ, relevant article or paragraph.
- Foreign legislation: Name of the act, date of publication. Relevant section or article or paragraph.
- Case law: Court, name of the ruling. Number of the case, date. Relevant paragraph.

The bibliography is divided in seven subsections – each is organised by alphabetical order.

(1) Laws, Statutes, and other relevant documents with legal value
(2) Case law
(3) Academic articles
(4) Working papers and reports
(5) Addresses, statements, opinions
(6) Official websites
(7) News articles and other websites

List of abbreviations

CFR – Charter of Fundamental Rights of the European Union

CIA – Central Intelligence Agency

CJEU – Court of Justice of the European Union

CNCTR – Commission nationale de contrôle des techniques de renseignement

CSI – Code de la sécurité intérieure

DGSE – Direction générale de la sécurité extérieure

DGSI – Direction générale de la sécurité intérieure

DNI – Director of National Intelligence

E.O 12333 – Executive Order 12333

ECHR – European Convention on Human Rights

ECtHR – European Court of Human Rights

EDPB – European Data Protection Board

EDPS – European Data Protection Supervisor

EEA – European Economic Area

EU – European Union

FISA – Foreign Intelligence Surveillance Act

FISC – Foreign Intelligence Surveillance Court

FRA – National Defense Radio Establishment

GC – Grand Chamber of the ECtHR

GDPR – General Data Protection Regulation

ISP – Internet service providers

NSA – National Security Agency

PM – Prime Minister

PPD-28 – Presidential Policy Directive-28

SCCs – Standard Data Protection Clauses

TSP – Terrorist Surveillance Program

U.S. – United States

UK – United Kingdom

Number of characters

I hereby declare that the body of this thesis, including spaces and notes, occupies a total of 196 603 characters.

The English version of the abstract occupies 2 344 characters, and the Portuguese version 2 484 characters, including spaces.

Abstract

Ever since the extent of mass foreign surveillance operated by the United States (U.S.) was revealed by Edward Snowden, concerns regarding the bulk collection of personal data have been raised. In the European Union (EU), where the General Data Protection Regulation (GDPR) is in force since 2018, guaranteeing data protection rights and principles applicable to the processing of personal data and extending these outside the continent's borders, the debate has been particularly vigorous. In an increasingly digital and connected world, transnational data flows are important for economic growth, trade, and human connection; however, data transfers between two of the most powerful economies in the world have been challenged in the years following the Snowden leaks with the invalidation by the Court of Justice of the European Union (CJEU) of two adequacy decisions ensuring data transfers between the EU and the U.S. in *Schrems I* (2015) and *Schrems II* (2020). The aim of this thesis is to clarify the EU data transfer legal regime, how American surveillance laws such as Section 702 of FISA and E.O. 12333 are a hinderance to the rights and protections arising from EU law, and whether a reconciliation is possible between data protection and surveillance for foreign intelligence purposes. Besides providing an in-depth look into U.S. laws authorising surveillance programs such as PRISM and Upstream, the difference in treatment between U.S. persons and non-U.S. persons will be emphasised. In addition, an analysis of the consequences of the *Schrems* case law and the shift in legal basis from transfers based on Article 45 of the GDPR pertaining to an adequacy decision, to transfers based on Article 46 regarding the implementation of appropriate safeguards, particularly, Standard Contractual Clauses (SCCs), will bring to light how the matter of data transfers to the U.S. might continue to be an issue due to American surveillance laws themselves. For the sake of perspective, and to gauge the place of data protection in matters of national security in the EU insight into France, Sweden and Germany's surveillance laws and programs will also be provided.

Keywords: data transfers; data protection; adequacy decision; standard contractual clauses; foreign surveillance; Section 702 of FISA; E.O. 12333; PRISM; Upstream; Schrems II.

Resumo

Desde a revelação da vigilância em massa efetuada pelos Estados Unidos (EUA) por Edward Snowden, preocupações relativas à recolha generalizada de dados pessoais têm sido levantadas. Na União Europeia (UE), onde o Regulamento Geral de Proteção de Dados (RGPD) está em vigor desde 2018, garantindo direitos e princípios de proteção de dados aplicáveis ao tratamento de dados pessoais e alargando-os para fora das fronteiras do continente, o debate sobre esta questão tem sido particularmente vigoroso. Num mundo cada vez mais conectado, a transmissão transnacional de dados é importante para o crescimento económico, para o comércio e a conexão humana; contudo, as transferências de dados entre duas das economias mais fortes do mundo têm sido contestadas desde as revelações de Snowden, com a invalidação pelo Tribunal de Justiça da União Europeia (TJUE) de duas decisões de adequação que asseguravam a transferências de dados entre a EU e os EUA em *Schrems I* (2015) e *Schrems II* (2020). O objetivo desta tese é esclarecer o regime jurídico da UE em matéria de transferência de dados, as leis de vigilância americana, designadamente a Secção 702 do FISA e a E.O.12333, e como estas são um obstáculo aos direitos e proteções decorrentes desse regime, assim como avaliar se é possível uma reconciliação entre a proteção de dados e sistemas de informações. Para além de uma análise aprofundada das leis norte-americanas que autorizam programas de vigilância como o PRISM e Upstream, será realçada a diferença de tratamento que existe entre cidadãos norte-americanos e não norte-americanos. Para além disso, uma análise das consequências da jurisprudência *Schrems* e a mudança de base jurídica nas transferências de dados do Artigo 45º do RGPD, relativo a decisões de adequação, para transferências baseadas no Artigo 46º, relativo a transferências sujeitas a garantias adequadas, particularmente as cláusulas-tipo de proteção de dados, permitirá concluir que a questão da transferência de dados para os EUA continuará a ser um tema de debate devido às leis de vigilância americanas. Por uma questão de perspetiva, e para avaliar o lugar da proteção de dados no âmbito da segurança nacional nos Estados-Membros, serão também referidas as leis de vigilância da Franca, Suécia e Alemanha.

Palavras-chave: transferências de dados; proteção de dados; decisão de adequação; cláusulas-tipo de proteção de dados; vigilância estrangeira; Secção 702 do FISA; E.O. 12333; PRISM; Upstream; Schrems II.

Table of contents

Introduction

The revelations of the mass surveillance operated by the United States' government by former National Security Agency (NSA) analyst Edward Snowden in mid-2013 shook the data protection landscape for years to come. Indeed, the realisation that governments and their intelligence services could so easily access their citizens' and non-nationals' personal data raised questions as to the importance of guaranteeing the right to privacy and data protection in a world that is increasingly digitalised and interconnected and threats to national security only grow more dangerous and take multiple forms. In the almost ten years since the Snowden leaks, the European Union (EU) has emerged as the leading superpower in data protection: first, with the adoption of the General Data Protection Regulation (GDPR) in 2016 guaranteeing rights and principles pertaining to the processing of personal data within the EU and the European Economic Area (EEA) as well as when data is transferred abroad, and later on with the Court of Justice of the European Union (CJEU) ruling on data transfer standards regarding transfers to the U.S. – a series of cases that became known as the *Schrems* case law.

It is with the view to bring more clarity to data transfer requirements arising from EU law and the subsequent standards they set in third countries such as the U.S., where legal persons are bound by surveillance laws to transmit personal data to intelligence services for foreign intelligence purposes, that this masters' thesis will seek to answer the following research question: "*In a context where the GDPR and the Schrems case law reshaped data transfers standards, is it possible to ensure the protection of personal data when it is transferred to the United States given its surveillance laws authorising large scale surveillance programs?"*

Consequently, in what follows an analysis of EU law regarding data transfers and, more largely, data protection will ensue. In addition, to better understand foreign surveillance operations conducted by the U.S., this thesis will draw from an analysis of legal instruments pertaining to foreign surveillance, as well as reports, studies, news articles, speeches and declassified documents that followed the Snowden leaks. A comparative analysis between surveillance measures applicable to U.S. persons and non-U.S. persons as well as between surveillance operations conducted by the U.S. and EU Member States, and in particular France, is also of interest so as to flesh out similarities

and differences in the treatment of persons and standards applied across both sides of the Atlantic.

As such, Chapter I of this thesis will provide an account of the importance of data transfers in a globalised world, what exactly they entail, and the protections awarded by EU law to personal data in such context. Of particular interest to our research are data transfers based on an adequacy decision and on Standard Contractual Clauses (SCCs) adopted by the European Commission.

Following that, Chapter II will address U.S. foreign surveillance operations impacting EU data subjects, namely PRISM and Upstream, and proceed with an analysis of the laws authorising these programs i.e., the Foreign Intelligence Surveillance Act (FISA) and Executive Order 12333. This will not only contextualise the conclusions made by the CJEU in the *Schrems* case law, in particular *Schrems II*, but it will also clarify the difference in standards present in U.S. law itself concerning surveillance measures applicable within national borders as opposed to programs applicable abroad.

Chapter III will consequently pay close attention to the Court's assessment of U.S. surveillance laws in *Schrems II* and the consequences of the invalidation of *The Privacy Shield* – the most recent adequacy decision upon which data transfers to the U.S. relied upon – with an in-depth analysis of Decision 2021/914 on SCCs, which represents an alternative for data transfers to third countries in the absence of an adequacy decision. Such an analysis will allow us to evaluate whether, notwithstanding an adequacy decision, SCCs are enough to guarantee an equivalent level of protection as that offered within the Union when transferring data to the U.S.

Lastly, Chapter IV will evaluate surveillance activities operated by EU Member States by studying France's surveillance operations and laws, as well as Sweden's and Germany's with the intent of shedding light on the matter that surveillance practices are also widespread within EU borders. A discussion will ensue about whether there exists a double standard regarding expectations demanded of the U.S. and the reality found in Member States. Finally, an analysis of case law from the CJEU and the ECtHR will help in assessing the requirements expected of Member States regarding the collection of personal data for foreign intelligence purposes and the complicated issue of reconciling data protection rules and national security.

Chapter I – Data protection and data transfers in a digital world

In the past years, the amount of data exchanged between the EU and the U.S. has increased exponentially. While in 2005 the transmission of data between the two superpowers was estimated to be around 500 to 1000 gigabits per second (Gbps), by 2014 that flow had grown to more than 20 000 Gbps.[1] This development can be explained by the rising number of businesses choosing to use digital platforms to respond to demand from international customers, but it is also a phenomenon that finds its roots in the increasing number of individuals using social media platforms to form cross-border connections.[2] Indeed, according to Eurostat's latest survey studying the use of social media in the EU at the beginning of 2021, 89% of the surveyed individuals aged 16 to 74 claimed to use the internet "at least once within the three months prior to the survey date" with 80% using the internet daily.[3] Moreover, in 2020, 57% of individuals in the same age category claimed to be users of social media platforms "in the last 3 months prior to the survey" representing an increase of 3% compared to the survey conducted the year prior.[4]

In this new highly digital environment where information travels across the globe in the blink of an eye, how is personal information protected from being misused and mishandled by the corporations, entities or authorities operating these platforms?

Where EU law is concerned, several provisions protect the privacy of citizens and their personal information. According to the Charter of Fundamental Rights of the European Union (CFR) – the main legal instrument laying out the fundamental rights of people in the EU and addressed to EU institutions and Member States when applying EU law,[5] – "everyone has the right to respect for his or her private and family life, home and

[1] MANYIKA, James [et al.] – **Digital Globalization: The New Era of Global Flows** [online]. McKinsey Global Institute. 2016. p. 4.
[2] ibid., pp. 7-8.
[3] EUROSTAT – **Internet usage**. **Digital economy and society statistics – households and individuals** [online article]. 2021. [accessed: 20 April 2022]. Available at: <URL: https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Digital_economy_and_society_statistics_-_households_and_individuals#Privacy_and_protection_of_personal_identity>.
[4] EUROSTAT – **Do you participate in social networks?** [online]. 2021. [accessed: 20 April 2022]. Available at: <URL: https://ec.europa.eu/eurostat/web/products-eurostat-news/-/edn-20210630-1 >.
[5] Charter of Fundamental Rights of the European Union, OJ C 326/391, 26.10.2012, pp. 391–407, Art. 51. [hereinafter: "CFR"].; EUROPEAN COMMISSION – **Why do we need the Charter? The Charter of Fundamental Rights, what it covers and how it related to the European Convention on Human Rights** [online]. [accessed: 14 June 2022]. Available at: <URL: https://ec.europa.eu/info/aid-development-cooperation-fundamental-rights/your-rights-eu/eu-charter-fundamental-rights/why-do-we-need-charter_en>.

communications" and "to the protection of personal data". [6] Contrary to the U.S. where only the right to privacy is guaranteed at the federal level, leaving data protection to rely on sector specific regulation, or otherwise, on individual state initiatives for a more comprehensive and ambitious approach as it is the case for the state of California with California Consumer Privacy Act (CCPA),[7] – data protection is a fundamental right in the EU.[8] As such the exploitation of citizens' personal information is protected by primary law and must obey certain rules: data "must be processed fairly for specified purposes and on the basis of consent of the person concerned or some other legitimate basis laid down by law", rights such as "the right of access" and rectification are guaranteed and independent authorities ensure compliance with these rules.[9]

The General Data Protection Regulation (GDPR), in force since 2016, grants even more security and protection to personal data whenever it is subjected to "processing" activities, i.e. "any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction".[10] Accordingly, the data controller (the natural or legal persons, public authorities, agencies or other bodies, which determine "the purposes and means of processing of personal data"),[11] and the data processor ("which processes personal data on behalf of the controller"),[12] must follow a certain set of principles: data should be processed "lawfully, fairly and in a transparent manner" within the purposes that were outlined or for legitimate purposes

[6] CFR, Art.7, Art. 8.
[7] The right to privacy in the U.S. was recognised by the Supreme Court in the 1965 *Griswold v. Connecticut* ruling as being constitutionally implied in the first, third, fourth, fifth and ninth Amendments (CORNELL LAW SCHOOL – **Privacy** [online]. [accessed: 14 June 2022]. Available at: <URL: https://www.law.cornell.edu/wex/privacy>.; BOYNE, Shawn M. – Data Protection in the United States. The American Journal of Comparative Law [online]. Vol. 66, nº1 (2018), p. 299.; OFFICE OF THE ATTORNEY GENERAL – **California Consumer Privacy Act (CCPA). Factsheet** [online]. [accessed: 06 September 2022]. Available at: <URL: https://www.oag.ca.gov/system/files/attachments/press_releases/CCPA%20Fact%20Sheet%20%28000000002%29.pdf>.
[8] see MCDERMOTT Yvonne – Conceptualising the right to data protection in an era of Big Data. Big Data & Society [online]. 2017. p. 1.
[9] CFR., Art. 8.
[10] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119, 4.5.2016, p. 1–88. Art. 4(2). [hereinafter "GDPR"].
[11] ibid., Art. 4(7).
[12] ibid., Art. 4(8).

("purpose limitation" principle) and limited to the strictest necessary ("data minimisation"), all the while ensuring that the data undergoing processing are accurate ("accuracy" principle), that they are not processed "for longer than is necessary" in relation to its purpose ("storage limitation") and that their protection is guaranteed by implementing "appropriate technical or organisational measures" ("integrity and confidentiality" principle).[13] Furthermore, processing activities are only lawful under specific conditions, such as consent from the data subject, the performance of contractual obligations the data subject signed up to, in matters of conformity with a legal obligation, in order to safeguard the "vital interests of the data subject", for public interest purposes, or "for the purposes of the legitimate interests pursued by the controller or by a third party."[14]

In the ensuing analysis relating to data transfers to the U.S. these principles and protections are relevant as, besides having introduced new rules regarding the handling of data subjects' personal information within the EEA, another one of the GDPR's landmarks was the introduction of Article 3, which extends the Regulation's material scope beyond the Union. Indeed, Article 3 envisions three scenarios for the extraterritorial application of the GDPR. On the one hand, provisions apply to all controllers and processors established in the EEA regardless of whether the processing activities happen elsewhere.[15] On the other hand, controllers and processors who are not established in the EU but whose processing activities concern the personal data of EU data subjects are also bound by the GDPR.[16] In this case, processing must be related to either (1) "the offering of goods and services, irrespective of whether a payment of the data subject is required, to such data subjects", or (2) "the monitoring of their behaviour as far as their behaviour takes place within the Union".[17] Finally, the GDPR's scope of application also concerns controllers and processors who are not in the EEA but "in a place where Member State law applies by virtue of public international law."[18]

As the independent authority responsible for the consistent application of the GDPR, the European Data Protection Board (EDPB) has clarified, Article 3 is addressed to a "particular processing activity, rather than a person (legal or natural)", consequently,

[13] ibid., Art. 5.
[14] ibid., Art. 6.
[15] ibid., Art. 3(1).
[16] ibid., Art. 3(2).
[17] ibid., Art. 3(2)(a)(b).
[18] ibid. Art. 3(3).

"where the processing of personal data falls within the territorial scope of the GDPR, all provisions of the Regulation apply to such processing".[19] Thus, the guarantees that legal persons outside the EU are expected to comply with, are as important as the protections legal persons within the EU must conform with under the penalty of an administrative fine.[20]

In a world where data flows are as important for economic growth as "traditional flows of traded goods" and where digital platforms offer not only a new entryway into the economy, but also ensure social interactions and the sharing of innovative ideas,[21] the stakes are therefore high. Indeed, the GDPR itself emphasises the importance of transnational data flows "for the expansion of international trade and international cooperation" but also underlines the subsequent "challenges and concerns" arising from the increase in transfers,[22] – particularly the "increased risk" associated with data transfers to third countries where "the ability of natural persons to exercise data protection rights in particular to protect themselves from the lawful use or disclosure of that information" may be undermined.[23]

As such, in Chapter V, the GDPR sets out three different ways to transfer data to third countries or international organisations outside the EU: data transfers may be based either on an adequacy decision, the implementation of appropriate safeguards or by derogation of these pathways, but only on very specific conditions.[24] In particular, Article 44 underlines that data being processed in a third country or that is transferred with the intent of being processed as well as any "onward transfers of personal data", must meet Chapter V requirements so "the level of protection of natural persons guaranteed by this Regulation is not undermined."[25] For the purposes of this master thesis, focus will mainly narrow on Article 45 addressing "transfers on the basis of an adequacy decision" and Article 46 pertaining to "transfers subject to appropriate safeguards".[26]

One the one hand, data transfers based on an adequacy decision pursuant to Article 45 are the most straightforward way of transferring data to a third country as, in its

[19] ibid., Art. 70.; EDPB – Guidelines 3/2018 on the territorial scope of the GDPR (Article 3) [online]. Version 2.1. 12 November 2019. p. 4.
[20] GDPR, Art. 83.
[21] MANYIKA, James [et al.] – op cit., p. 2.
[22] GDPR, recital 101.
[23] ibid., recital 116.
[24] ibid., Art.44-49.
[25] ibid., Art. 44.
[26] ibid., Art. 44-46.

assessment procedure, the Commission has already found the country as providing a level of protection "essentially equivalent to that ensured within the Union" and consequently adopted a legal framework – an adequacy decision – upon which data transfers can rely upon without any further conditions.[27] In its evaluation, the Commission must consider multiple factors such as the rule of law, human rights, criminal law and legislation applicable to national security, as well as investigate whether public authorities have access to personal data or if there is an independent supervisory authority overseeing the implementation of data protection rules and capable of enforcing them.[28]

On the other hand, supposing the Commission has failed to reach an agreement with a third country or international organisation on such a legal framework, data transfers still remain a viable option; however, this is only relevant in cases where the controller and processor are able to implement "appropriate safeguards" and "on condition that enforceable data subject rights and effective legal remedies for data subjects are available".[29] Pursuant to paragraph two of Article 46 "appropriate safeguards" include either a "legally binding and enforceable instrument between public authorities or bodies", "binding corporate rules", SCCs adopted by the Commission or the supervisory authority and approved by the Commission, "an approved code of conduct pursuant to Article 40" or "an approved certification mechanism pursuant to Article 42".[30] Of particular interest are the SCCs adopted by the Commission as per Article 46(2)(c), which will be discussed in depth in Chapter III of this master's thesis. In the same manner that an adequacy decision entails that the third country offers an equivalent level of protection for data subjects, SCCs must follow the same requirement and, if needed, be supplemented with "additional measures to compensate for lacunae in protection of third-country legal systems".[31]

Having established a link between provisions of EU law pertaining to data protection and the rights and obligations arising from them, as well as the fact that data transfers from the EU are only possible if the third country or international organisation

[27] ibid., Art. 45; recital 104.
[28] ibid., Art. 45(2).
[29] ibid., Art. 46.
[30] ibid.
[31] MILDEBRATH, Hendrik – **The CJEU judgment in the *Schrems II* case** [online]. European Parliamentary Research Service. 2020. p. 1.

offers an equivalent level of protection to the one found in the EU, another aspect that requires clarification is what exactly a *data transfer* to a third country or to an international organisation consists of – something which the GDPR is silent about.[32]

Where case-law is concerned, in *Bodil Lindqvist*, the CJEU clarified what *cannot* be considered a data transfer.[33] Whilst responding to the reference for preliminary ruling by the Swedish Court of Appeal (Göta hovrätt) on the interpretation of Directive 95/46/EC, the ancestor of the GDPR,[34] the Court emphasised that it is not because information is uploaded to an internet page and becomes available to persons in a third country that the action necessarily constitutes a data transfer.[35] Indeed, "it is necessary to take account both of the *technical nature of the operations* thus carried out and of *the purpose and structure of Chapter IV of that directive* where Article 25 appears."[36]

In this instance, the Court found that while Mrs. Lindqvist uploaded the personal data of her colleagues to her personal page, her website did not have the "technical means to send that information automatically to people who did not intentionally seek access to those pages".[37] Hence, the personal data uploaded to the internet by Mrs. Lindqvist and accessible to persons in a third country "[was] not directly transferred between those two people but *through the computer infrastructure* of the hosting provider where the page is stored".[38] Furthermore, the Court found that the Commission's intent with Article 25 of Directive 95/46/EC was not to regard the mere uploading of information to the internet and its subsequent accessibility in a third country as a data transfer, as that would make "the special regime provided for by Chapter IV", a "regime of general application, as regards operations on the internet".[39] Accordingly, this would mean that whenever data uploaded to a hosting provider in the EU became available in a third country judged as

[32] EDPB – Guidelines 05/2021 on the Interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR [online]. 18 November 2021. p. 4. [hereinafter: "Guidelines 05/2021"].
[33] Judgement of the Court of November 2003. Criminal Proceedings against *Bodil Lindqvist*. Reference for a preliminary ruling: Göta hovrätt-Sweden., EU:C:2003:596, Case C-101/01. [hereinafter: "*Bodil Lindqvist*"].; this case follows proceedings instituted against Mrs. Lindqvist, who uploaded her colleagues' personal information on her website without their consent, being subsequently found guilty in Sweden of violating data protection laws (§2 of the ruling).
[34] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281, 23.11.1995, pp. 31–50.
[35] *Bodil Lindqvist*, §57.
[36] ibid.
[37] ibid., § 60.
[38] ibid., § 61.
[39] ibid., § 69.

not providing an adequate level of protection, all uploading of data to the internet would have to be suspended as per Article 25(4) of the Directive.[40]

The Court's ruling can therefore be summarized as such:

> "The reply to the fifth question must therefore be that there is no 'transfer [of data] to a third country' within the meaning of Article 25 of Directive 95/46 where an individual in a Member State loads personal data onto an internet page which is stored with his hosting provider which is established in that State or in another Member State, thereby making those data accessible to anyone who connects to the internet, including people in a third country."[41]

More recently, the EDPB added to the Court's findings and brought more precision by outlining three cumulative criteria for a data transfer to occur. First, the data controller and processor must be "subject to the GDPR for the given processing" meaning that one of the two scenarios laid out in Article 3 regarding controllers and processors not established in the Union must be applicable to the processing activity in question.[42] Secondly, the controller or processor acting as an "exporter", "discloses by transmission or otherwise makes personal data, subject to this processing, available to another controller, joint controller or processor ("importer").[43] And thirdly, the controller or processor acting as "importer", "is in a third country or is an international organisation, irrespective of whether or not this importer is subject to the GDPR in respect of the given processing in accordance with Article 3."[44] In this case, the transfer "needs to comply with the conditions of Chapter V and frame the transfer by using the instruments which aim at protecting personal data after they have been transferred to a third country or international organisation", that is to say, either on an adequacy decision as per Article 45 or on the basis of safeguards envisioned by Article 46, except when the transfer falls within the derogations pursuant to Article 49.[45]

The matter of what constitutes a data transfer and the territorial scope of the GDPR are crucial to understand the current stalemate and situation regarding data transfers to the U.S and the impact of surveillance laws on data protection rules. Indeed, propelled by the 2013 Snowden revelations of U.S. mass surveillance, the privacy activist

[40] ibid.
[41] ibid., § 71.
[42] Guidelines 05/21, p. 4 *supra* note 33.
[43] ibid.
[44] ibid.
[45] ibid., p. 8.

Maximilian Schrems filed a complaint to the Irish Data Protection Commissioner (DPC) arguing that the Facebook Ireland could not transfer users' data to its parent company in U.S. (Facebook Inc.) due to surveillance laws requiring the social media company to reveal users' personal information to U.S. intelligence, something which, according to Mr. Schrems, undermined protections guaranteed by EU Law.[46] With this complaint, Mr. Schrems was questioning the very foundation upon which all data transfers from the EU to the U.S. relied upon at the time: the Commission's Adequacy Decision 2000/520/EC or *The Safe Harbour Privacy Principles*.[47] As it turned out, the *Safe Harbour Principles* proved indeed insufficient to protect data subjects' personal data from the prying eyes of U.S. intelligence as the CJEU emphasised in the landmark *Schrems I* ruling whereby it invalidated Decision 2000/520/EC on the grounds that surveillance operated by the U.S. infringed the principle of proportionality in two ways: first, by allowing the collection of data in an unrestricted and generalised manner, and secondly, by not providing legal remedies to EU data subjects so they could vindicate rights guaranteed by EU law.[48] Moreover, as the Court underlined, the Commission never stated in its adequacy decision "that the United States in fact 'ensures' an adequate level of protection by reason of its domestic law or international commitments".[49]

Less than a year after *Schrems I*, the *Safe Harbour Principles* were hastily replaced by Decision 2016/1250 or *The Privacy Shield Decision*,[50] in what appeared to be a "temporary solution".[51] As a matter of fact, both the European Data Protection Supervisor (EDPS)[52] and Article 29 Working Party raised concerns in their opinions prior to the adoption of *The Privacy Shield Decision* arguing that "the scale of signals

[46] SCHREMS, Max – Comentário ao Acórdão in **Em Foco: O Encarregado de Proteção de Dados**. Fórum de Proteção de Dados [online]. Lisbon: Comissão Nacional de Proteção de Dados, n°7 (2020), p. 109.
[47] Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles, OJ L 215, 25.8.2000, pp. 7–47.
[48] Judgement of the Court (Grand Chamber) of 6 October 2015, *Maximilian Schrems v. Data Protection Commissioner*. Reference for preliminary ruling from the High Court (Ireland), EU:C:2015:650, Case C-362/14. §91-98, §106. [hereinafter: "*Schrems I*"].
[49] ibid.
[50] Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield, OJ L 207, 1.8.2016, pp. 1–112. [hereinafter: "Privacy Shield Decision"].
[51] CANTO MONIZ, Graça – A Extraterritorialidade do Regime Geral de Proteção de Dados Pessoais da União Europeia: Manifestações e Limites. Lisboa: Faculdade de Direito Universidade Nova de Lisboa, 2018, p. 265. PhD Dissertation.
[52] The EDPS is the supervisory authority monitoring the application of data protection rules by EU institutions, see: EUROPEAN DATA PROTECTION SUPERVISOR (EDPS) – **About** [online]. [accessed: 15 June 2022]. Available at: <URL: https://edps.europa.eu/about-edps_en>.

intelligence and the volume of data transferred from the EU subject to potential collection once transferred and notably when in transit is likely to be still high",[53] and that there existed "a number of important unresolved issues" such as a lack of oversight and supervision regarding compliance with the principles.[54] At the time, Mr. Schrems cautioned that "Privacy Shield is an updated version of the illegal 'Safe Harbor'. Nothing in US surveillance law was changed or fixed",[55] implying that U.S. laws themselves were the main point of contention.

As it is known today, these concerns turned out to be correct as in the *Schrems II*, the CJEU invalidated Decision 2016/1250 invoking, yet again, an infringement of the principle of proportionality by American surveillance laws concerning limitations to fundamental rights such as the right to privacy and data protection, as well as the lack of legal remedies available to EU data subjects.[56] These points will be further discussed in detail in Chapter III of this thesis but, first, an understanding of the mass surveillance operated by U.S. authorities as well as the laws enabling it is necessary.

[53] EDPS – **Opinion 4/2016 on the EU-U.S. Privacy Shield draft adequacy decision** [online]. 30 May 2016. pp. 6-7. cited by CANTO MONIZ – op cit., p. 266.
[54] ARTICLE 29 WORKING PARTY (Art. 29 WP) – EU – U.S. Privacy Shield – First annual Joint Review [online]. 20 November 2017. p.2.; cited by CANTO MONIZ – op cit., p. 266.
[55] SCHREMS, Max – op cit., pp. 109-110.
[56] Judgment of the Court (Grand Chamber) of 16 July 2020. *Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems*. Request for a preliminary ruling from the High Court (Ireland). §184-202, EU:C:2020:559, Case C-311/18. [hereinafter: "*Schrems II*"].

Chapter II – U.S. surveillance programs and their legal background

1. U.S. surveillance programs: PRISM and Upstream

The extent of U.S. surveillance was brought to light by Edward Snowden via *The Guardian*[57] and *The Washington Post*[58] on 6 June 2013 when both news outlets published a court order issued by the Foreign Intelligence Surveillance Court (FISC) requiring Verizon, one of the main telecommunications companies in the country, to provide U.S. citizens' daily communications to the NSA. Indeed, the order demanded the transmission "on an ongoing daily basis" of "all call detail records or "telephony metadata" created by Verizon for communications (i) between the United States and abroad; or (ii) wholly within the United States, including local telephone calls."[59] The secrecy and underground nature of this operation was emphasised in the court order itself which prohibited the disclosure "to any other person that the FBI or NSA has sought or obtained tangible things under this Order" – except for the employees tasked with transmitting the data to the NSA, an attorney for legal advice or a FBI pre-approved individual.[60]

Inside EU borders, the leak that caused most concern was the disclosure of the PRISM program.[61] Indeed, among the information obtained by Snowden, a Power Point presentation dating from April 2013 revealed that a surveillance program codenamed PRISM enabled the NSA to collect information "directly from the servers of these Internet Service Providers (ISP): Microsoft, Yahoo, Google, Facebook, PalTalk, AOL, Skype, YouTube and Apple", therefore allowing the agency to easily collect data pertaining to

---

[57] GREENWALD, Glenn – **NSA collecting phone records of millions of Verizon customers daily** [online]. The Guardian. 6 June 2013. [accessed: 29 April 2022]. Available at: <URL: https://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order>. cited by LYON, David – Surveillance, Snowden, and Big Data: Capacities, consequences, critique. Big Data & Society [online]. SAGE journals. 2014. p. 2.

[58] LEE, Timothy B. – **Report: NSA asked Verizon for records of all calls in the U.S.** [online]. The Washington Post. 5 June 2013. [accessed: 29 April 2022]. Available at: <URL: https://www.washingtonpost.com/news/wonk/wp/2013/06/05/nsa-asked-verizon-for-records-of-all-calls-in-the-u-s/ >.

[59] THE GUARDIAN – **Verizon forced to hand over telephone data – full court ruling** [online]. 6 June 2013. [accessed: 29 April 2022]. Available at: <URL: https://www.theguardian.com/world/interactive/2013/jun/06/verizon-telephone-data-court-order >.

[60] ibid.

[61] GELLMAN, Barton, POITRAS Laura – **U.S., British intelligence mining data from nine U.S. Internet companies in broad secret program** [online]. The Washington Post. 7 June 2013. [accessed: 29 April 2022]. Available at: <URL: https://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html>. cited by LYON, David, op cit. *supra* note 57.; GREENWALD, Glenn, MACASKILL, Ewen – **NSA Prism program taps in to user data of Apple, Google and others** [online]. The Guardian. 7 June 2013. [accessed: 29 April 2022]. Available at: <URL: https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data>.

"E-mail, Chat – video, voice, Videos, Photos, Stored data, VoIP, File transfers, Video Conferencing, Notifications of target activity – logins, etc., Online Social Networking details, Special Requests".[62] Concretely, the NSA only has to provide a "selector" to these ISP – that is to say, an identifier of the person they seek to obtain information about, *e.g.*, an email address, and the company is required to make available "the communications sent to or from that selector to the government".[63] Besides the NSA, which "receives all data collected through PRISM", the FBI and CIA are also able to obtain data collected through PRISM.[64]

According to one of the leaked slides, the beginning of PRISM collection dates back to 2007 for Microsoft, 2008 for Yahoo, 2009 for Google and Facebook and 2010 for YouTube.[65] As a result of this previously secret cooperation and the data collected by the NSA, the agency was able to complete a large number of intelligence reports – the biggest contributors being Yahoo, followed by Microsoft and Google.[66] By 2011, it is estimated that 91% of the intelligence gathered by the NSA was obtained through the PRISM program.[67]

Besides PRISM, another program that was revealed as impacting EU data subjects was the Upstream collection program, which according to the slides leaked by Snowden, enables the "collection of communications on fiber cables and infrastructure as data flows past".[68] As the High Court of Ireland stated in its reference for preliminary ruling in *Schrems II*, Upstream collection enables the NSA to gather communications flowing through the "backbone of the Internet" i.e., the "network of cables, switches and routers" via the private companies operating the infrastructure.[69] Not only does this allow direct access to metadata, but also to the content of communications themselves, including those

---

[62] MACASKILL, Ewen, DANCE, Gabriel – **NSA Files: Decoded. What the revelations mean for you** [online]. The Guardian. 1 November 2013. [accessed: 26 April 2022]. Available at: <URL: https://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded#doc/3>.

[63] MEDINE, David [et al.] – **Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act** [online]. Privacy and Civil Liberties Oversight Board. 2014. p. 7.

[64] ibid.

[65] ibid.

[66] MACASKILL, Ewen, DANCE Gabriel – op cit. *supra* note 62 at <URL: https://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded#doc/4 >.

[67] MEDINE, David [et al.] – op cit. p. 33.

[68] MACASKILL, Ewen, DANCE Gabriel – op cit.

[69] *Schrems II*, § 62.

of non-US citizens "associated with a 'selector'".[70] Contrary to PRISM, which only targets electronic or Internet communications, data collection pursuant to the Upstream program also targets phone calls.[71] However, access to the information collected is not the same for all U.S. intelligence agencies. While the NSA has access to all data collected through PRISM and Upstream, the CIA and FBI's access is dependent on which information the NSA chooses to share with and send to these agencies.[72]

Although U.S. surveillance practices were no secret prior to the Snowden's leaks – it was widely known that, after the September 11th terrorist attacks, the NSA was engaging in the mass collection of domestic calls,[73] – what shook the data protection landscape in the EU was the fact that the same surveillance techniques were being applied outside of the U.S.'s borders. In the same way the American government was "mining" domestic data,[74] – that is to say, "creating profiles by collecting and combining personal data, and analysing it for particular patterns of behaviour deemed to be suspicious",[75] it was using similar mining projects such as XKeyscore abroad. In the slides leaked by Snowden, XKeyscore is described as the "widest reaching" system enabling the NSA to collect and analyse data from "150 sites" and "over 700 servers" around the world.[76] The system facilitates the indexation of "e-mail addresses, file names, IP addresses and port numbers, cookies, webmail and chat usernames and buddylists, phone numbers, and metadata from web browsing sessions (including words typed into search engines and

[70] ibid.
[71] MEDINE David [et al.] – op cit., p. 7 *supra* note 63.
[72] ibid., p. 34-35.
[73] BIGNAMI, Francesca – European Versus American Liberty: Comparative Privacy Analysis of Antiterrorism Data Mining. Boston College Law Review [online]. Vol. 48, nº 3 (2007), p. 614.; KRIS, David S. – On the Bulk Collection of Tangible Things. Journal of National Security Law & Policy [online]. Vol. 7, nº 2 (2014), pp. 210-211.
[74] see for instance the Total Information Awareness project later renamed "Terrorism Information Awareness" (TIA) data mining project aimed at collecting and mining a wide range of information about U.S. citizens discussed by BIGNAMI, F. – op cit., p. 616 *supra* note 73.
[75] SOLOVE, Daniel J. – Data Mining and the Security-Liberty Debate. The University of Chicago Law Review [online]. Vol 75, nº 1, p. 343.
[76] see GREENWALD Glenn – **Xkeyscore: NSA tool collects 'nearly everything a user does on the internet'** [online]. The Guardian. 31 July 2013. [accessed: 19 May 2022]. Available at: <URL: https://www.theguardian.com/world/2013/jul/31/nsa-top-secret-program-online-data>.;THE GUARDIAN – **XKeyscore presentation from 2008 – read in full** [online]. 31 July 2013. [accessed: 19 May 2022]. Available at: <URL: https://www.theguardian.com/world/interactive/2013/jul/31/nsa-xkeyscore-program-full-presentation>.

locations visited on Google Maps)" and, consequently, makes the extraction of information of a targeted individual or selector easier.[77]

All in all, the PRISM and Upstream program leaks reveal just how much "the NSA thus depends on codes, the algorithms, plus the witting or unwitting cooperation of both telephone and internet corporations in order to do surveillance".[78] Nevertheless, the heads of U.S. Intelligence at the time – the Director of National Intelligence (DNI) James R. Clapper, the Director of the NSA General Alexander Keith, and the U.S. Deputy Attorney General, James M. Cole, – deemed as "inaccurate" the information exposed by Snowden while speaking in a joint statement for the House Permanent Committee on Intelligence in October 2013.[79]

Additionally, when broaching the subject of foreign surveillance and Section 702 of the Foreign Intelligence Surveillance Act (FISA) – the main legal basis for surveillance operations abroad which will be discussed in depth in the next section of this thesis, – the heads of American Intelligence underlined that data collection pertaining to these programs "targets only non-U.S. persons overseas, and that targeting and minimization procedures and acquisition guidelines are required to ensure that the statutory restrictions are followed and to govern the handling of any U.S. person information that may be incidentally acquired".[80] They went on to criticise, the "inaccurate reporting about the program" and reassured that "the Government does not have access to communications carried by U.S. electronic communications service providers without appropriate legal authority" – implicitly referring to the orders issued by the FISC authorising surveillance programs prior to their implementation, – and that "the Government cannot collect information under Section 702 unless there is an appropriate and documented foreign intelligence purpose, such as preventing terrorism or weapons of mass destruction proliferation". [81]

---

[77] BOWDEN, Caspar – **The US surveillance programmes and their impact on EU citizens' fundamental rights**. Directorate General for Internal Policies Police Department C: Citizens Rights and Constitutional Affairs. Brussels: European Parliament, 2013. pp. 13-14.
[78] LYON, David – op cit., p.3 *supra* note 57.
[79] CLAPPER, R. James [et al.] – **Joint Statement of DNI James Clapper, DIRNSA Gen. Keith Alexander, and DAG James Cole Before the House Permanent Select Committee on Intelligence** [online]. Washington D.C. 29 October 2013. p. 3.
[80] ibid., p. 5.
[81] ibid.

However, the sheer extent of the collection authorised by both PRISM and Upstream, as well as the mining of foreign data thanks to systems such as XKeyscore, raises fears as to whether the data being collected is strictly related to foreign intelligence purposes. There is no question that U.S. intelligence operations are worrying considering data protection rules guaranteed by EU law, but what statutes of U.S. law authorise this kind of surveillance and why does this matter in the context of data transfers from the EU to the U.S.? These are questions that will be answered in the next section of this master's thesis.

2. American laws authorising foreign surveillance

As briefly mentioned, the main piece of legislation governing foreign intelligence gathering is Section 702 of FISA, however, Executive Order 12333 (E.O 12333) and Presidential Policy Directive 28 (PPD-28) are also important legal instruments that regulate the collection, dissemination and retention of information pertaining to non-U.S. persons.[82] The next subsections will explore each of these legal texts so as to provide an understanding of how the PRISM and Upstream program came to be and how U.S. surveillance laws enabling these programs come into conflict with EU law, in particular Article 45 of the GDPR, as the CJEU ruled in *Schrems II* – one of the subject matters of Chapter III.

2.1 – Section 702 of the Foreign Intelligence Surveillance Act (FISA)

2.1.1 – Historical background

Historically speaking, Section 702 is the product of the progressive pressure put on the U.S government to clarify surveillance practices that were secretly put in place after the September 11th attacks and progressively revealed to the public by the media, starting with a report published by *The New York Times*, in December 2005, claiming that a "presidential order signed in 2002" authorised the warrantless surveillance of "internal telephone calls and international e-mail messages of hundreds, perhaps thousands, of people inside the United States".[83] These allegations were confirmed the following day

[82] BIGNAMI, Francesca – **The US legal system on data protection in the field of law enforcement. Safeguards, rights and remedies for EU citizens** [online]. Directorate General for Internal Policies, Policy Department C: Citizens Rights and Constitutional Affairs. Brussels: European Parliament, 2015. p. 6, 21.; MEDINE, David [et al.] – op cit., pp. 100-101 *supra* note 63.

[83] MEDINE, David [et al.] – op cit., p. 5, pp. 16-17.; RISEN, James, LICHTBLAU, Eric – **Bush Lets U.S. Spy on Callers Without Courts** [online]. The New York Times. 16 December 2005. [accessed: 01 June

by president George W. Bush who insisted that the surveillance had solely a counterterrorist purpose and was focused on the targeting of "international communications of people with known links to al Qaeda and related terrorist organizations" with the goal of intercepting communication chains between terrorists abroad and their allies on American territory.[84] Although this monitorisation which later came to be known as the Terrorist Surveillance Program (TSP) evaded Court orders, the President emphasised that it was approved by the Attorney General and the Counsel to the President, and reviewed by the Justice Department and "NSA's top legal officials".[85]

The TSP not only enabled the NSA to "(1) collect the contents of certain international communications", but also to "(2) collect in bulk non-content information, or "metadata", about telephone and Internet communications".[86] From October 2001 to January 2007, President George W. Bush freely renewed this authorisation until the government was pushed to seek the approval of the FISC, thereby transferring the program "to the authority of the FISA".[87] Consequently, the Bush administration obtained a FISC court order known as the "Foreign Telephone and Email Order" authorising the electronic surveillance practices that were already in place under the TSP.[88]

In addition to the Foreign Telephone and Email Order, the Bush administration also relied on "the then-existing FISA statute to obtain individual court orders to compel private companies to assist the government in acquiring the communications of individuals located overseas who were suspected of engaging in terrorism and who used United States-based communication service providers",[89] which is very reminiscent of the PRISM program but on a smaller, individual scale.

2022]. Available at: <URL: https://www.nytimes.com/2005/12/16/politics/bush-lets-us-spy-on-callers-without-courts.html>.

[84] THE WHITE HOUSE PRESIDENT GEORGE W. BUSH – **President's Radio Address** [online]. White House Radio. 17 December 2005. [accessed: 01 June 2022]. Available at: <URL: https://georgewbush-whitehouse.archives.gov/news/releases/2005/12/20051217.html>.

[85] MEDINE, David [et al.] – op cit., p.17.

[86] ibid. p. 16. citing OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE - **DNI Announces the Declassification of the Existence of Collection Activities Authorized by President George W. Bush Shortly After the Attacks of September 11, 2001** [online]. 21 December 2013. [accessed: 01 June 2022]. Available at: <URL: https://icontherecord.tumblr.com/post/70683717031/today-the-director-of-national-intelligence>.

[87] OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE – op cit.

[88] MEDINE, David [et al.] – op cit., p. 17.

[89] ibid., p. 18. citing WAINSTEIN, Kenneth L. – **Statement of Kenneth L. Wainstein Assistant Attorney General** [online]. United States Senate: Select Committee on Intelligence, 1 May 2007, pp. 6-7.

When a switch in the wording of the Foreign Telephone and Email Order was made by the FISC during the May 2007 renewal process, giving the Court more leeway in determining surveillance targets instead of the government,[90] the Bush administration sought to curb the new hurdle by proposing an amendment to FISA, and consequently, bringing back to the government the authority to determine foreign surveillance targeting.[91] Thus, a temporary solution was found in the Protect America Act, signed into law in August 2007 and amending FISA to authorise the collection of foreign intelligence "concerning persons reasonably believed to be outside the United States" with "the assistance of a communications service provider, custodian, or other person (…) who has access to communications".[92] The Protect America Act was the precursor to Section 702 of FISA, and was officially repealed by Section 702 when its 180-day sunset clause came into effect.[93]

2.1.2 – Legal analysis

In July 2008, the FISA Amendments Act (FAA), also known as the Foreign Intelligence Surveillance Act of 1978 Amendments Act, was enacted and signed into law, adding Title VII "Additional procedures regarding certain persons outside the United States" which Section 702 is part of to the 1978 Act and, consequently, granting U.S. intelligence the power to target "certain persons outside the United States other than United States persons".[94] Contrary to the "traditional" FISA, which only regulates electronic surveillance "exclusively between or among foreign powers" within the United States borders,[95] the introduction of Section 702 granted the Attorney General and the DNI the power to "authorize jointly, for a period of up to 1 year from the effective date of the

[90] While in the January 2007 Order the authorisation of communication and metadata collection was conditioned to the government showing "probable cause determination regarding one of the communicants, and the email addresses and telephone numbers to be tasked were reasonably believed to be used by persons located outside the United States", the May 2007 order renewal replaced the word "government" by "court.; see MEDINE, David [et al.] – op cit., p.18. citing MUKASEY, Michael B. – **Classified certification of the Attorney General of the United States** [online]. 19 Sept 2008 (declassified 5 May 2014). MDL Dkt. No. 06-1791-VRW. §37-38.

[91] MEDINE, David [et al.] – op cit., pp. 18-19.

[92] Protect America Act of 2007, Public Law. No. 110-55, 121 Stat. 552, 5 August 2007. 50 USC 1805b.(a)(3). [accessed: 01 June 2022]. [hereinafter: "Protect America Act of 2007"].

[93] MEDINE, David [et al.] – op cit., p.19.; Protect America Act of 2007, 50 USC 1803(c).

[94] CONGRESS.GOV. – **H.R. 6304 – 110th Congress (2007-2008)** [online]. Library of Congress, 2008. [accessed: 29 May 2022]. Available at: <URL: https://www.congress.gov/bill/110th-congress/house-bill/630>.

[95] Foreign Intelligence Surveillance Act of 1978 (FISA), 25 October 1978. Sec. 102, 50 USC § 1802(A)(i). [hereinafter: "50 USC § 1802"]; Sec. 101(f)(1) defines electronic surveillance as "the acquisition by an electronic mechanical, or other surveillance device of the contents of any wire or radio communication sent by or intended to be received by a particular, known United States person who is in the United States".

authorization, the targeting of persons reasonably believed to be located outside the United States to acquire foreign intelligence information". [96]

However, such an authorisation must follow a certain procedure. Apart from the fact that Section 702 doesn't allow U.S. intelligence to "intentionally" target any American citizen, whether they are in U.S. territory or outside its borders, or whether the person at the beginning or end of the communication is in the United States,[97] this collection of information is only lawful if "notwithstanding any other provision of law", it follows a court order issued by the FISC approving the Attorney General or DNI's surveillance request, formally known as "certification" or, in the case of an emergency, the "determination" issued by the Attorney General and the DNI.[98] In addition to this, "targeting" and "minimization" procedures must be complied with.[99]

A. Certifications

The first step in the approval of surveillance targeting non-U.S. persons is the submission of "a written certification and any supporting affidavit, under oath and under seal" by the Attorney General and the DNI to the FISC, whose job is to review the document according to FISA standards.[100] These certifications must fulfil a number of conditions laid out in subsection (g) of Section 702 in order to be approved: they must contain provisions addressing the minimisation and targeting procedures employed in the collection (see *infra*), guidelines ensuring respect for the limitations laid out in subsection (b), which essentially guarantee that U.S. persons will not be intentionally targeted and, finally, they must attest that "the acquisition involves obtaining foreign intelligence information from or with the assistance of an electronic communication service provider".[101] Therefore, the requirement that service providers assist U.S. intelligence in foreign intelligence gathering is explicitly written into law.

Here it is relevant to clarify what FISA means by "foreign intelligence information". According to Section 101 of the Act, this is an expression encompassing any information that might assist the U.S. "to protect against" a variety of potential events

[96] Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2008 (FAA), 10 July 2008. Sec. 702, 50 USC § 1881a.(a)(c)(2). [hereinafter Section 702 of FISA: "50 USC §1881a."].
[97] 50 USC §1881a.(b).
[98] 50 USC §1881a. (a)-(e).
[99] ibid.
[100] 50 USC §1881a. (g)(1).
[101] 50 USC §1881a.(g)(2)(A).

initiated by a "foreign power" or "agents of a foreign power" and compromising national security, namely, the "actual or potential attack or other grave hostile acts", "sabotage or international terrorism", "clandestine intelligence activities by an intelligence service or network", as well as any information concerning a "a foreign power or foreign territory that relates to, and if concerning a United States person is necessary to the national defense or the security of the United States" or "the conduct of the foreign affairs of the United States".[102]

Although certifications must meet some requirements prior to their authorisation by the FISC as mentioned above, the constraints set seem to serve more to protect the targeting of U.S. citizens' communications. This is especially true where the "limitations" to targeting are concerned, which relate more to the protection of U.S. persons from intentional targeting,[103] rather than laying out viable safeguards for the objects of the surveillance authorisation *i.e.,* non-U.S. persons.

Additionally, when compared to Title I of FISA pertaining to the "traditional" surveillance of foreign elements within U.S. borders, Section 702 is slacker in terms of requirements prior to the authorisation of surveillance. As the Privacy and Civil Liberties Oversight Board stated in their report, "Section 702 differs from the traditional FISA electronic surveillance framework both in the standards applied and in the lack of individualised determinations by the FISC".[104] The more lenient Section 702 allows for more general certifications wherein "categories of foreign intelligence information" are described as per the definition of "foreign intelligence information", but does not ask the Attorney General and DNI to elaborate on the identity of the targeted individuals.[105] By contrast, Title I constrains the Attorney General or Federal Officer in their submission of an "application for an order approving electronic surveillance" to the FISC (the equivalent to a certification under Section 702), to identify the target of the electronic surveillance, as well as show proof that the target is indeed "a foreign power or an agent of a foreign power" and that "each of the facilities or places at which the electronic surveillance is directed is being used, or is about to be used by a foreign power or an agent of a foreign power".[106] On the contrary, a certification submitted to the FISC under Section 702 "is

[102] 50 USC §1801(e).
[103] 50 USC §1881a.(g)(2)(iv).
[104] MEDINE, David [et al.] – op cit., pp. 24-25.
[105] ibid.
[106] USC §1804(a)(3)(4).

not required to identify the specific facilities, places, premises, or property at which an acquisition authorised under subsection (a) will be directed or conducted".[107]

B. Determination

Apart from submitting a certification for approval to the FISC, surveillance operations may also be authorised under what Section 702 calls a "determination" – an exceptional procedure only to be used in "exigent circumstances" wherein the Attorney General and the DNI demonstrate that "intelligence important to the national security of the United States may be lost or not timely acquired" if a FISC court order is to be awaited.[108] A determination may be issued prior to the submission of a certification or while a certification is under the judicial review of the FISC.[109]

C. Targeting procedures

As stated above, among the requirements set for the approval of foreign surveillance we find the requisite description of the targeting procedures that will be used to obtain signals intelligence. These should "ensure that any acquisition authorised under subsection (a) is limited to targeting persons reasonably believed to be located outside the United States", and safeguard against the "intentional acquisition" of communications where the sender or recipient are in U.S. territory.[110]

As previously discussed in the first section of the present chapter, in the case of PRISM, targeting is achieved by choosing a "selector" identifying the targeted non-U.S. person, such as an email address or phone number, which is then sent to the electronic communications service provider in question so as to obtain information "sent to or from" that selector.[111]

As for the targeting procedures concerning Upstream collection – occurring with the cooperation of service providers operating the very infrastructure making the exchange of communications possible (e.g., network of cables) – they are outlined in subsection (h) of Section 702 pertaining to "directive" and according to which the DNI and the Attorney General "may direct in writing, an electronic communication service provider to – (A) immediately provide the Government with all information, facilities, or

[107] 50 USC §1881a.(g)(4).
[108] 50 USC §1881a.(c)(2).
[109] 50 USC §1881a.(c)(3).
[110] 50 USC §1881a.(d).
[111] MEDINE, David [et al.] – op cit., p. 33.; 50 USC §1881a.(g)(2)(A).

assistance necessary to accomplish the acquisition in a manner that will protect the secrecy of the acquisition (…) (B) maintain under security procedures approved by the Attorney General and the Director of National Intelligence any records concerning the acquisition or the aid furnished that such electronic communication service provider wishes to maintain".[112]

Specifically, the collection of telephone communications through the Upstream program happens in a similar manner to PRISM: a selector, in this case a phone number, is sent to the service provider so as to acquire communications "either to or from" the chosen telephone number acting as the target.[113] However, the acquisition of Internet communications occurs differently particularly because it is achieved through the acquisition of Internet *transactions*, that is to say, "any set of data that travels across the Internet together such that it may be understood by a device on the Internet",[114] with the characteristic of being "to", "from" or "about" a selector.[115] The added complexity of Internet transactions is that they go beyond the simple one-way communications between target and server (called "single discrete communication") and contain multiple chains of communication wherein if one single communication is about, to or from the selector, the NSA will collect the whole chain (called "multiple discrete communications" (MCTs)).[116] The danger is therefore acquiring "communications that are not about a tasked selector and may have no relationship, or no more than an incidental relationship to the targeted selector".[117] Consequently, the acquisition of MCTs carries the inherent risk of obtaining data that are unrelated to the target, or even collecting U.S. communications when they are caught in the loop – which is why tougher minimisation rules regulating the "retention, and use of such upstream data" are necessary.[118]

It was perhaps for this reason that in 2017 the NSA formally announced that "its Section 702 foreign intelligence surveillance activities will no longer include any upstream internet communications that are solely "'about' a foreign intelligence target", that is to say the collection of communications including a targeted selector such as an

[112] 50 USC §1881a.(h)(1).; MEDINE, David [et al.] – op cit., p. 35.
[113] MEDINE, David [et al.] – op cit., p. 36.
[114] ibid., p. 39.
[115] ibid., p. 37.
[116] ibid., p. 39.
[117] MONACO, Lisa O., INGLIS, John Chris, LITT, Robert S. – **Joint Statement at a hearing concerning "FISA Amendments Act Reauthorization"** [online]. 8 Dec. 2011, p. 7. cited by MEDINE, David [et al.] – op cit., p. 40.
[118] MEDINE, David [et al.] – op cit., p. 41.

email address but wherein the persons at both ends of the communication might not be the intended targeted individual.[119] The agency implied that technical limitations and the importance of safeguarding against the unintentional acquisition of domestic communications as well as information unrelated to foreign intelligence purposes were behind this decision.[120] As part of this measure, the agency also included the suppression of "the vast majority of previously acquired upstream internet communications".[121]

Targeting measures implemented by the NSA based on selectors linked to targeted individuals was what led the Privacy and Civil Liberties Oversight Board to conclude that Section 702 is not, per se, a bulk collection program and can be best described as "programmatic surveillance".[122] According to the Board, in the year 2013, 89 138 persons were targeted as part of the surveillance authorised by Section 702.[123]

D. Minimisation procedures

According to subsection (e), "minimization procedures that meet the definition of minimization procedures under section 101(h) or 301(a)" shall be put in place by the Attorney General and the DNI and undergo judicial review by the FISC.[124] Their purpose is "to minimize the acquisition and retention, and prohibit the dissemination, of nonpublicly available information concerning unconsenting United States persons consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information". [125] This includes the protection of the identity of U.S. persons by ensuring that consent is given prior to the use of any personal information going beyond the aim of FISA i.e. obtain foreign intelligence information within the meaning of section 101(e), the adoption of a plan of action guiding the retention and dissemination of information for law enforcement purposes, and the implementation of procedures ensuring that the content of communications of U.S. persons will not be divulged or disseminated beyond a 24 hour time frame, except where the Attorney General can obtain

[119] NSA, CSS – **NSA Stops Certain Section 702 "Upstream" Activities** [online]. Press Release. 28 April 2017. [accessed: 17 June 2022]. Available at: <URL: https://www.nsa.gov/Press-Room/Press-Releases-Statements/Press-Release-View/Article/1618699/nsa-stops-certain-section-702-upstream-activities/>.
[120] ibid.
[121] ibid.
[122] MEDINE, David [et al.] – op cit., p. 113.
[123] ibid.
[124] 50 USC §1881a.(e).
[125] 50 USC §1801(h)(1).

a court order extending this period, or where the Attorney General "indicates a threat or death or serious bodily harm to any person".[126]

As the Privacy and Civil Liberties Oversight Board described, minimisation procedures function as a "set of controls on data to balance privacy and national security interests" and are applied differently in each agency depending on how intelligence is used and acquired.[127] However, as may be concluded if a closer look is taken, the limits imposed by minimisation procedures are mainly directed at the protection of U.S. persons' and domestic communications that may potentially be caught in the midst of targeting of non-U.S. persons.

As a matter of fact, in the declassified minimisation procedures implemented in 2020 by the NSA it is firmly stated that "a person known to be currently outside the United States, or whose location is unknown, will not be treated as a United States person".[128] Consequently, rules applying to U.S. persons such as the destruction of personal information unrelated to foreign intelligence, and the five-year limit for retention of data, at first glance, do not apply to non U.S. persons.[129] For instance, the data retention limit only applies to foreign communications concerning a United States person, as section 7(a)(1) of the procedures reads: "retention of foreign communications of or concerning United States persons is permitted for a period of five years from the expiration date of the certification authorizing the collection".[130] In contrast, section 8 of the document dealing with "other foreign communication" *i.e.* 'full' foreign communication unrelated to U.S. persons, reads only that "foreign communications of or concerning a non-United States person may be retained, used, and disseminated in any form in accordance with other applicable law, regulation, and policy"[131] – in this regard, applicable law setting retention and dissemination limits of non-U.S. persons' data were introduced by Presidential Police Directive – 28, which will be discussed *infra.* Moreover, the fact that U.S. persons' identity is anonymised prior to the transmission of foreign

[126] 50 USC §1801(h)(2)(3)(4).
[127] MEDINE, David [et al.] – op cit., pp. 50-51.
[128] BARR, William P. – Minimization procedures used by the National Security Agency in connection with the acquisition of foreign intelligence information pursuant to Section 702 of the Foreign Intelligence Surveillance Act of 1978, as amended [online]. Office of the Director of National Intelligence (ODNI): 16 Sept. 2019 (declassified 26 April 2021), p. 4, Sec. 3(j)(2).
[129] ibid., p. 5, Sec. 4(b)(1).
[130] ibid. p. 12, Sec.7(a)(1).
[131] ibid., p. 14, Sec. 8.

communications, or only after consent is obtained,[132] but the same possibility is not considered for foreign communication unrelated to U.S. persons reveals that there is a disregard for the protection of non-U.S. persons' data. The mere fact that section 8 dealing with foreign communications is so curt and short compared to the rest of the document shows just how much the protection of personal data of non-U.S. persons is relegated to a second-class status.

E. Judicial review

The authority responsible for the judicial review of the requirements arising from Section 702 is the Foreign Intelligence Surveillance Court or FISC. The Court, which was established at the time of the enactment of FISA in 1978, sits "eleven federal district court judges who are designated by the Chief Justice of the United States" and whose term is limited to a maximum of 7 years.[133] Regarding foreign intelligence of non-U.S. persons its functions include reviewing certifications submitted by the Attorney General and the DNI, as well as the targeting and minimisation procedures and, where applicable, amendments to these procedures and to certifications.[134] In its assessment, the Court must also ensure compliance with the Fourth Amendment to the Constitution of the United States.[135]

However, as already has been pointed out, limitations to the authorisation pursuant to Section 702 and subjected to FISC review are more aimed at the protection of U.S. citizens than non-U.S. persons, consequently, it may be concluded that the judicial review operated by the FISC follows the same direction and ensures the protection of U.S. persons' privacy more than the individuals whose surveillance is authorised by Section 702.

In the same way that a discrepancy is found between Section 702 certification requirements and the standards expected of traditional FISA certifications (or "applications for an order") pursuant to Title I of FISA, differences in the process of judicial review can also be observed. While under Section 105 pertaining to "issuance of an order", the FISC must find probable cause that the target is indeed a foreign power or

[132] ibid., p. 12, Sec.7(b).
[133] UNITED STATES FOREIGN INTELLIGENCE COURT – **About the Foreign Intelligence Surveillance Court** [online]. [accessed: 08 July 2022]. Available at: <URL: https://www.fisc.uscourts.gov/about-foreign-intelligence-surveillance-court>.
[134] 50 USC §1881a.(i)(1)(A).
[135] 50 USC §1881a.(i)(3)(A).

an agent thereof and that the facilities targeted by electronic surveillance are being or will be used by the targeted individual prior to the approval of the application submitted by the Attorney General or Federal officer,[136] under Section 702 the FISC "does not see or approve the specific persons targeted or the specific communications facilities that are actually tasked for acquisition",[137] as certifications are not required to specify the location of targets (see *supra*).[138]

2.2 – Executive Order 12333

Besides FISA, another legal instrument that regulates foreign intelligence gathering and surveillance is Executive Order 12333 (E.O. 12333).[139] E.O. 12333 was first issued in 1981 by President Ronald Reagan and subsequently amended in 2003, 2004 and 2008, with the purpose "to enhance human and technical collection techniques, especially those undertaken abroad, and the acquisition of significant foreign intelligence, as well as the detection and countering of international terrorist activities, the spread of weapons of mass destruction, and espionage conducted by foreign powers."[140]

The Executive Order does not only identify the various intelligence agencies and entities of the executive branch making up the "Intelligence Community" (a total of ten elements such as the Central Intelligence Agency, the Defense Intelligence Agency, the NSA and the National Geospatial Intelligence Agency, as well as the Department of State, the Department of Treasury and the Department of Defense) and, consequently, the participants in the collection, analysis and dissemination of foreign information, but it also lays out the "duties and responsibilities" arising from these activities,[141] therefore setting legal standards, albeit much more "permissive" than the ones imposed by FISA, for foreign surveillance.[142]

Indeed, the only limits constraining surveillance activities operated by American the Intelligence Community are restrictions meant to protect U.S. persons. Therefore, according to section 2.3 of the document, the collection, retainment and dissemination of

[136] 50 USC §1805(a)(3).
[137] MEDINE, David [et al.] – op cit., p. 27.
[138] 50 USC § 1881a.(g)(4).
[139] BIGNAMI, Francesca (2015) – op cit., p. 27 *supra* note 82.; JAYCOX, Mark. M – No Oversight, No Limits, No Worries: A Primer on Presidential Spying and Executive Order 12,333. Harvard National Security Journal [online]. Vol 12 (2021), p.75.
[140] Executive Order 12333 "United States Intelligence Activities", as amended by Executive Orders 13284 (2003), 13355 (2004) and 13470 (2008). §2.2. [hereinafter: "E.O. 12333"].
[141] E.O. 12333, §1.7 – § 1.10.
[142] BIGNAMI, Francesca – op cit., p. 27 *supra* note 82.

information related to Americans must respect "procedures established by the head of the Intelligence Community element concerned or by the head of a department containing such element and approved by the Attorney General".[143] Concerning "collection techniques", they must be "the least intrusive techniques feasible within the United States or directed against United States persons abroad".[144] Nothing in E.O. 12332 explicitly mentions the protection of the personal data of non-U.S. persons' against abuses, reflecting again, to an even greater extent, the second-class status that non-U.S. persons are relegated to, but which the adoption of PPD-28 attempted to curb.

More concretely, E.O. 12333 authorises surveillance programs "travelling through or 'transitioning' the American telecommunications backbone that is not to or from a U.S. person", as well as the gathering of data "at foreign access points through which foreign communications transit within and/or between foreign countries", – which are programs similar to the upstream collection authorised by Section 702.[145] These techniques have as their background what was dubbed as "transit authority" surveillance: a secretive practice established during the Reagan administration meant to circumvent FISA's warrant-related standards by using E.O 12333 to allow the NSA, "on domestic soil and without a warrant, to collect foreign-to-foreign communications that are passing over the American network" and, subsequently, enabling the bulk collection of communications' content as well as metadata.[146] It is estimated that the amount of signals intelligence collected through "transit authority" surveillance is second to the volume of data obtained through the programs authorised by Section 702.[147] XKeyscore, as described above, is one of the programs falling under "transit authority" and falling under E.O. 12333.[148]

3. Presidential Policy Directive – 28 (PPD-28)

PPD-28 was the response of the Obama Administration to the Snowden leaks. Through the legal framework, the Administration sought to appease tensions with its allies and

[143] E.O. 12333, § 2.3.
[144] ibid., § 2.4.
[145] JAYCOX, Mark. M – op cit., p. 91 *supra* note 139.
[146] SAVAGE, Charlie – **Power Wars document: Transit Authority and the 1990 Lawton surveillance memo** [online]. 18 November 2015. [accessed: 11 June 2022]. Available at: <URL: https://charliesavage.com/2015/11/power-wars-document-transit-authority-and-the-1990-lawton-surveillance-memo/>.
[147] JAYCOX, Mark. M – op cit., pp. 95-96.
[148] ibid.

curb the "international trust deficit" caused by the revelations, thereby providing policy solutions and principles aimed at protecting "global privacy rights".[149]

Besides emphasizing that data collected by surveillance programs have a strictly "foreign intelligence or counterintelligence purpose",[150] of note is the acknowledgement, in section 2 of the PPD-28, that bulk collection may result in the gathering of personal information that is unrelated to foreign intelligence purposes and that this risk should be countered with "new limits (….) to protect the privacy and civil liberties of all persons, whatever their nationality and regardless of where they might reside."[151] The Directive also emphasises that data resulting from bulk collection, shall be used solely for the purpose of:

> "(1) espionage and other threats and activities directed by foreign powers or their intelligence services against the United States and its interests; (2) threats to the United States and its interests from terrorism; (3) threats to the United States and its interests from the development, possession, proliferation, or use of weapons of mass destruction; (4) cybersecurity threats; (5) threats to U.S. or allied Armed Forces or other U.S or allied personnel; and (6) transnational criminal threats (…)".[152]

Most importantly, PPD-28 sets out limitations on the processing of non -U.S. persons' personal data by the Intelligence Community.[153] Safeguards include the implementation of the same minimization procedures pursuant to section 2.3 of E.O. 12333 and applicable to the dissemination and retention of personal information of U.S. persons with a maximum retention limit set to 5 years, unless the DNI decides otherwise for national security purposes.[154] Therefore, like under E.O. 12333, the dissemination and retainment of non-U.S. persons' data should obey the procedures set out by the designated head of the Intelligence agency or element of the Intelligence Community in question or,

[149] MARGULIES, Peter – Global Cybersecurity, Surveillance, and Privacy: The Obama Administration's Conflicted Legacy. Indiana Journal of Global Legal Studies [online]. Vol. 24, nº. 2 (2017), p. 471.
[150] Presidential Policy Directive – Signals Intelligence Activities [online]. The White House Office of the Press Secretary. 17 January 2014. Sec. 1. [hereinafter: "PPD-28"].
[151] ibid., Sec. 2.
[152] ibid.
[153] ibid., Sec. 4.
[154] ibid., Sec. 4(a)i.

alternatively, follow the measures set by head of department in charge of surveillance activities and approved by the Attorney General.[155]

Nonetheless, if read carefully, the limitations pursuant to section 2.3 of E.O. 12333 don't amount to much given that the Intelligence Community has free reign to collect, retain and disseminate various "types of information" such as "information constituting foreign intelligence or counterintelligence, including such information concerning corporations or other commercial organizations"[156] – and which, given the broad definition of "foreign intelligence" as per E.O. 12333 (i.e., "information relating to the capabilities, intentions, or activities of foreign governments or elements thereof, foreign organizations, foreign persons, or international terrorists"),[157] still allows for great manoeuvre on the part of U.S. intelligence. Other types of information allowed to be processed include "information obtained in the course of a lawful foreign intelligence, counterintelligence, international drug or international terrorism investigation", data about individuals "who are reasonably believed to be potential sources or contacts for the purpose of determining their suitability or credibility" and "incidentally obtained information that may indicate involvement in activities that may violate Federal, state, local or foreign laws".[158]

PPD-28 also takes steps to reassure that access to retained personal information is exclusive to trained and authorised personnel, and that only information that is consistent with "applicable IC [Intelligence Community] standards for accuracy and objectivity" will be stored and disseminated.[159] Furthermore, it introduced oversight and audit examinations of the multiple elements of the Intelligence Community, as well as their policies and procedures, with the DNI responsible for resolving compliance issues and in charge of notifying, if necessary, non-compliance issues impacting non-U.S. persons to their respective government.[160]

Even though PPD-28 is, as former Assistant Attorney General David S. Kris put it, "an unprecedented change in U.S. intelligence policy,[161] and an attempt at

[155] E.O. 12333, §2.3.
[156] ibid., §2.3(b).
[157] ibid., § 3.5(e).
[158] ibid., §2.3(b), (c), (f), (i).
[159] PPD-28, Sec. 4(a)(ii.), (iii.).
[160] ibid., Sec. 4(a)(iv.).
[161] KRIS, David S. – op cit., p. 289 *supra* note 73.

"unprecedented transparency",[162] it is also true that the protections introduced by the Policy Directive are unlikely to result in an important change in the predicament of data subjects and in the collection and use of their personal information by U.S. intelligence. Indeed, as previously discussed, protections guaranteed to non-U.S. persons are the same available to U.S. persons pursuant to E.O. 12333, which has been described as a "permissive" due to "the breath of permitted dissemination under Section 2.3."[163] Only the data retention standards introduced by PPD- 28 are likely to be of consequence for non-U.S. persons.[164]

4. Conclusion

Having come to the end of an analysis of the U.S. statutes and legislative frameworks governing foreign surveillance, it is evident that there is a distinction between surveillance conducted within U.S. borders and surveillance targeting non-U.S. persons abroad. In fact, this divergence was underlined as early as 1972 by the Supreme Court of the United States in the *Keith* ruling. [165]

This case, which follows three individuals accused of planning an attempt on government property and whose communications were wiretapped with the approval of the Attorney general only bypassing a court warrant on the grounds of protecting "the national security",[166] was the start of the distinction between the "domestic aspects of national security" and the surveillance of "activities of foreign powers or their agents".[167] While the Court ruled that surveillance without a warrant was unconstitutional and counter to the Fourth Amendment as it interferes with rights guaranteed by the United States constitution,[168] it stated that the same criteria and protections don't always apply in matters of surveillance of "foreign powers".[169]

[162] MARGULIES, Peter – op cit., p. 486 see *supra* note 149.
[163] KRIS, David S. – op cit., p. 294 *supra* note 73.; BIGNAMI, Francesca – op cit., p. 29 *supra* note 82.
[164] KRIS, David S. – op cit., p. 293-294.
[165] BIGNAMI Francesca – op cit., p. 20.; *United States v. United States Dist. Ct*. (Keith), 407 U.S. 297 (1972). [hereinafter: "407 U.S. 297"].
[166] 407 U.S. 297 (1972) at § U.S. 299-301.
[167] BIGNAMI Francesca – op cit., p. 20.; 407 U.S. 297 (1972), §321.
[168] The Fourth Amendment reads: "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." (U.S. Constitution. amend. IV. Available at: <URL: https://www.senate.gov/civics/resources/pdf/US_Constitution-Senate_Publication_103-21.pdf >).
[169] 407 U.S. 297 (1972), §321-322, in particular, footnote 20.

As Francesca Bignami pointed out in her study "The US legal system on data protection in the field of law enforcement", the *Keith* ruling shaped the "two-part scheme" characteristic of U.S. surveillance laws: indeed, "the law is largely designed to exclude domestic security threats from the special framework set out for surveillance (considered foreign because it either involves foreign entities or is conducted abroad) and to protect the speech and privacy rights of US citizens."[170] This conclusion is stark in our analysis. As was pointed out, there are significant differences between Title I of FISA pertaining to foreign intelligence surveillance inside U.S. borders and Title VII of FISA as amended by the FAA in 2008 and its Section 702 authorising surveillance of non-U.S. persons.

This discrepancy is also present in E.O. 12333, which is as silent as Section 702 on the matter of limitations pertaining to the collection, retention and dissemination of the personal data of non-U.S. persons but enables even more the collection of data in bulk. In fact, the only protections envisioned in both legal frameworks are meant to protect U.S.-persons. Although PPD-28 granted more protection to non-U.S. persons, it is still far from EU law requirements concerning data protection in the context of data transfers to the U.S. as per Chapter V of the GDPR.

As mentioned in Chapter I of this thesis, the appropriateness of U.S. surveillance laws was assessed by the CJEU first, in 2015, in *Schrems I* and later on, in 2020, in *Schrems II* whereby the Court invalidated the newest legal foundation for data transfers between the EU and the U.S., the *Privacy Shield.* In the next Chapter an analysis of the Court's conclusions in *Schrems II* will be carried out, as well as an assessment of the consequences for data transfers to the U.S., in particular transfers based on Standard Contractual Clauses (SCCs).

[170] BIGNAMI, Francesca – op cit., p. 20 *supra* note 82.

Chapter III. *Schrems II* and its implications for data transfers to the U.S.

As previously mentioned, the first case that the CJEU listened to regarding data transfers to the U.S. was *Schrems I*, which outcome led to the invalidation of Decision 2000/520/EC or the *Safe Harbour Privacy Principles*, – the legal foundation for EU-U.S. data transfers since the early 2000s up until 2015. What spurred *Schrems II* was the revelation by the DPC – to which Mr. Schrems had initially filed a complaint questioning the legality of data transfers to the U.S. – that Facebook Ireland relied on SCCs for data transfers to Facebook Inc. and not on *Safe Harbour*.[171] Subsequently, Mr. Schrems reformulated his complaint asking for the suspension of data transfers to the U.S. arguing that surveillance laws required "Facebook Inc. to make the personal data transferred to it available to certain United States authorities, such as the National Security Agency (NSA) and the Federal Bureau of Investigation (FBI)" which, in Mr. Schrems view, undermined Articles 7, 8 and 47 of the CFR and the legality of Decision 2010/87 on Standard Contractual Clauses (SCCs) in force at the time,[172] but since then repealed by Decision 2021/914.[173]

Considering the new complaint lodged by Mr. Schrems and the issues raised regarding the legality of Decision 2010/87 on SCCs, the DPC filed a complaint to the High Court of Ireland so the matter be referred to the CJEU.[174] Although initially the main point of contention was the legality of Decision 2010/87, the fact that Facebook brought up *The Privacy Shield Decision* to argue for the legality of the Decision 2010/87 insofar as in the latest adequacy decision the Commission found American laws to provide an adequate level of protection so the legality of transfers pursuant to Decision 2010/87 should not be an issue either,[175] turned the case into an assessment of both legal frameworks and eventually led to the invalidation of *The Privacy Shield Decision*.

In what follows, an analysis of the Court's arguments will be carried out in order to bring to light the shortcomings of U.S. surveillance laws, as well as the lack of protections

[171] *Schrems II*, §54.; SCHREMS, MAX – op cit., p. 110 *supra* note 46.
[172] *Schrems II*, §55.; Commission Decision of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC of the European Parliament and of the Council, OJ L 39, 12.2.2010, p. 5–18. [hereinafter: "Decision 2010/87"].
[173] Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council, OJ L 199, 7.6.2021, pp. 31–61. [hereinafter: "Decision 2021/914"].
[174] *Schrems II*, §57.; SCHREMS, MAX – op cit., p. 110.
[175] SCHREMS, Max – op cit., p. 111.; *Schrems II*, §66.

offered to non-U.S. persons but expected under EU law. A subsequent discussion about SCCs-based transfers and their utility considering U.S. surveillance will ensue.

1. The Court's ruling in *Schrems II*: the invalidation of Privacy Shield

The Court deemed that U.S. laws did not provide an adequate level of protection as per Article 45 of the GDPR and invalidated *The Privacy Shield Decision* on three grounds.

First, the Court found that U.S. laws presented issues in light of the principle of proportionality and considering limitations to fundamental rights as provided for in the CFR, particularly, to Article 7 pertaining to the "respect for private and family life" and Article 8 relating to the "protection of personal data".[176] Indeed, according to Article 52 of the CFR, "any limitation on the exercise of the rights and freedoms recognised by this Chapter must be provided for by law and respect the essence of those rights and freedoms".[177] As a result, any law restricting fundamental rights should itself "define the scope of the limitation on the exercise of the rights concerned", feature "clear and precise rules governing the scope and application of the measure in question and imposing minimum safeguards", as well as "in what circumstances and under which conditions a measure providing for the processing of such data may be adopted, thereby ensuring that the interference is limited to what is strictly necessary".[178]

Nevertheless, neither E.O. 12333 nor Section 702 of FISA provide for an equivalent to Article 52(1) of the CFR or any of the other proportionality requirements pointed out by CJEU. Indeed, the Court concluded that "Section 702 of FISA does not indicate any limitations on the power it confers to implement surveillance programmes for the purposes of foreign intelligence or the existence of guarantees for non-US persons potentially targeted by those programmes".[179] As was illustrated *supra*, there is indeed a lack of safeguards for non-U.S. persons under Section 702 and even more so in E.O. 12333. Regarding the protections guaranteed by PPD-28, the Court found that they were insufficient in the context of EU law as "PPD-28 does not grant data subject actionable

[176] *Schrems II*, §168-180.
[177] *Schrems II*, §174; CFR, Art. 51(1).
[178] ibid., § 175-176.
[179] Schrems II, §180.

rights before the courts against the US authorities",[180] and doesn't limit the bulk collection of data in transit authorised by E.O. 12333, which is not subjected to judicial review.[181]

Secondly, the Court found that there were no legal remedies available to data subjects or any means for data subjects to enforce their rights under U.S. law, contrary to what Article 45 of the GDPR requires for a country to qualify as providing an adequate level of protection, and to Article 47 of the Charter pertaining to the "right to an effective remedy and to a fair trial".[182] As the Court underlined, access to legal remedies is integral to the rule of law and, in matters of data protection, it is paramount that data subjects are able "to have access to personal data relating to him or her, or to obtain the rectification or erasure of such data"[183] – all rights that are guaranteed by Articles 15, 16 and 17 of the GDPR.[184]

As the High Court of Ireland stated in its reference for preliminary ruling, the Fourth Amendment to the Constitution of the U.S., "which constitutes, in United States law, the most important cause of action available to challenge unlawful surveillance, does not apply to EU citizens" and "the NSA's activities based on E.O. 12333 are not subject to judicial oversight and are not justiciable".[185] On the other hand, surveillance programs authorised by Section 702 of FISA, although lacking in terms of judicial review compared to "traditional" FISA orders, are subject to FISC oversight prior to their authorisation by the Attorney General or DNI.

Finally, and directly linked to the lack of legal remedies, the Court raised concerns regarding the impartiality of the Privacy Shield Ombudsperson Mechanism – the solution found by U.S. authorities during the *Privacy Shield* negotiations for the lack of legal remedies available to non-U.S. person – whose objective was to "ensure that individual complaints are properly investigated and addressed" in an independent manner.[186] Although the incumbent Secretary of State John Kerry reassured that the mechanism would allow EU authorities "to submit request on behalf of EU individuals regarding U.S. signals intelligence practices" and appointed Under Secretary of State, Catherine A. Novelli as Ombudsperson reassuring that Mrs. Novelli was "independent from the U.S.

[180] ibid., §181.
[181] ibid., §183.; citing *Privacy Shield Decision*, Annex VI.
[182] ibid.§187-192.; GDPR, Art.45(2)(a).; CFR, Art. 47.
[183] ibid., §187.
[184] GDPR, Art. 15-17.
[185] ibid., § 65.
[186] Schrems II, §195.; *Privacy Shield Decision*, recital 117.

intelligence community" and reporting directly to the Secretary of State,[187] the Court found that the Ombudsperson lacked impartiality as Mrs. Novelli was "an integral part of the U.S. State Department" and therefore of the government of the United States.[188] Furthermore, the Ombudsperson didn't have the power to hold U.S. intelligence accountable by taking binding decisions, nor did the mechanism envision any legal safeguards for data subjects,[189] such as "access to the data relating to them and to have such data rectified or erased, or that the Ombudsperson would award compensation to persons harmed by a surveillance measure."[190]

While the Court invalidated *Privacy Shield* due to its incompatibility "with Article 45(1) of the GDPR, read in light of Articles 7, 8 and 47 of the Charter",[191] it noted that this didn't prevent cross-border transfers from occurring as in the absence of an adequacy decision data transfers were still possible pursuant to Article 46 and 49 of the GDPR.[192]

2. The Court's ruling in *Schrems II*: the case of Standard Contractual Clauses (SCCs)

In addition to invalidating *Privacy Shield*, the Court also ruled on the validity of Decision 2010/87 on SCCs, upholding it.[193] Although it emphasised that due to their "inherently contractual nature" SCCs do not have the power to bind public authorities in third countries, it is possible for controllers and processors, in the absence of an adequacy decision, to supplement SCCs with "additional safeguards" so as to ensure "compliance with the level of protection required under EU law", as per Article 46(1) and recitals 108 and 114 of the GDPR, in circumstances where the SCCs adopted by the Commission may not suffice.[194] Indeed, as the Court noted "standard data protection clauses adopted by the Commission on the basis of Article 46(2)(c) of the GDPR are solely intended to provide contractual guarantees that apply uniformly in all third countries to controllers and processors established in the European Union, and, consequently, independently of the

[187] *Privacy Shield Decision*, Annex III.
[188] Schrems II, §195.
[189] ibid., §196.; Opinion of Advocate General Saugmandsgaard ØE delivered on 19 December 2019. *Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems*. Request for a preliminary ruling from the High Court (Ireland), EU:C:2019:1145, §338. [hereinafter: "Opinion of the Advocate General"].
[190] Opinion of the Advocate General, §338.
[191] *Schrems II*, §198-201.
[192] ibid., §202.
[193] ibid., §148.
[194] ibid., §131-133.

level of protection guaranteed in each third country."[195] The onus falls therefore on the controller and processor "to verify, on a case-by-case basis" with the recipient of the data whether the third country offers an equivalent level of protection as that provided for by EU Law.[196] On the other hand, if SCCs are not supplemented by additional safeguards and if the law of the third country undermines the protection guaranteed by the clauses, "the controller or processor, or failing that, the competent supervisory authority, are required to suspended or end the transfer of personal data to the third country concerned."[197]

Although, Decision 2010/87 has since been repealed by Decision 2021/914, the Court's statements regarding the use of SCCs still apply. In a situation where businesses and public entities acting as data importers or exporters are expected to implement additional safeguards in order to transfer data to the United States, or for that matter to any third country not possessing an adequacy decision agreement with the EU, the EDPB has issued recommendations on how to best proceed in this regard.[198] It is therefore valuable to consider Decision 2021/914 and the EDPB recommendations in an analysis regarding the extent to which the personal information of EU data subjects can or not be protected when it is transferred to the U.S.

3. Data transfers post-*Schrems II*

Due to their low cost and quick implementation method, standard contractual clauses approved by the Commission have been, even prior to the Court's ruling in *Schrems II*, one of the main preferred means to transfer data to third countries.[199] Essentially, when the parties to a data transfer agree to use SCCs as their legal basis, they are binding themselves to "an additional set of default legal requirements" guaranteeing the protection of data subjects beyond the borders of the EEA.[200] According to a recent survey

[195] ibid. §133.
[196] ibid. §134.; Opinion of the Advocate General, §126.
[197] ibid., §135.
[198] EDPB – Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data [online]. Version 2.0. 18 June 2021. p. 3. [hereinafter: "Recommendations 01/2020"].
[199] ARMINGAUD, Claude-Étienne, COMPARET Laure, SELOSSE Violaine – **EU Data Protection: standard contractual clauses may have been confirmed by the CJEU, but at what price?** [online]. K&L Gates. 17 July 2020. [accessed: 21 June 2022]. Available at: <URL: https://www.klgates.com/eu-data-protection-standard-contractual-clauses-may-have-been-confirmed-by-the-cjeu-but-at-what-price-07-17-2020>.; BRADFORD, Laura, ABOY, Mateo, LIDDELL, Kathleen – Standard contractual clauses for cross-border transfers of health data after *Schrems II*. Journal of Law and Biosciences [online]. Vol 8, nº 1 (2021), p.10.
[200] BRADFORD, Laura [et al.] – op cit., p. 20.

of 292 companies conducted by *DIGITALEUROPE*, 85% confirmed they relied on SCCs for data transfers to third countries, while only 5% said they rely on binding corporate rules, derogations and adequacy decisions, with 75% of those companies having their headquarters in Europe and 13% in the U.S.[201]

3.1 Decision 2021/914 on SCCs

Decision 2021/914 was adopted by the Commission less than a year after *Schrems II*, providing not only updated standards for data transfers reflecting GDPR requirements, but also embodying new advancements in the digital economy and the CJEU's findings in *Schrems II*.[202] In their joint opinion prior to the adoption of the Decision, both the EDPB and the EDPS welcomed the Commission's efforts in accommodating "new and more complex processing operations" and in addressing "the effects of the laws of the third country of destination on the data importer's compliance with the clauses, and in particular how to deal with binding request from public authorities in the third country for disclosure of the personal data transferred."[203] Both supervisory bodies also commended the inclusion of supplementary measures referenced in the EDPB's recommendations.[204]

Overall, Decision 2021/914 establishes 18 clauses that stipulate legal obligations for the data exporter ("the controller or processor transferring the personal data to a third country") and the data importer ("the controller or processor receiving the data"),[205] thereby "granting enforceable GDPR rights to third parties and subject to the oversight of the EU data protection authorities",[206] and guaranteeing "a level of protection essentially equivalent to that guaranteed within the Union".[207] In other words, the SCCs grant data subjects the right to "invoke and enforce" the Clauses as third-party beneficiaries.[208] As such, the Clauses cannot be modified but they can be included "in a wider contract" and

[201] DIGITALEUROPE, BUSINESSEUROPE, ERT, ACEA – **Schrems II Impact Survey Report** [online]. Brussels: 2022, p.5,8.
[202] Decision 2021/914, recital 6 *supra* note 173.; EDPB, EDPS – Joint opinion 2/2021 on the European Commission's Implementing Decision on standard contractual clauses for the transfer of personal data to third countries for the matters referred to in Article 46 (2)(c) of Regulation (EU) 2016/679 [online]. 14 January. 2021. p.7.
[203] EDPB, EDPS – op cit., p. 7.; Decision 2021/914, recital 18.
[204] EDPB, EDPS – op cit., pp.7-8.
[205] Decision 2021/214, recital 3.
[206] CAMPAGNUCCI, Marcelo, ABOY, Mateo, MINSSEN, Timo – Cross-Border Transfers of Personal Data after Schrems II: Supplementary Measures and New Standard Contractual Clauses (SCCs). Nordic Journal of European Law [online]. nº2 (2021), p. 43.
[207] Decision 2021/214, recital 11.
[208] ibid., clause 3.

additional safeguards are welcomed "provided that they do not contradict, directly or indirectly, the standard contractual clauses or prejudice the fundamental rights or freedoms of data subjects."[209]

One of the novelties of the new SCCs compared to the previous clauses pursuant to Decision 2010/87 is that they have a "modular approach" where the general clauses are thought through in the light of different four cross-border transfer scenarios called "modules" wherein specific obligations are expected for each type of transfer.[210] Decision 2021/914 lays out four modules: module one dealing with transfers from a controller to another controller, module two broaching the subject of transfers from a controller to a processor, module three providing a set of rules for transfers from a processor to another processor and, finally, module four dealing with transfers from a processor to a controller.[211] As a reminder, "controller" is a term used by the GDPR to refer to "the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data", as opposed to a data processor who is "a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller."[212]

Another added value brought by the latest Decision is clause 7, an optional "docking clause" allowing additional parties who were not initially part of the agreement to become a party later "either as a data exporter or as a data importer by completing the Appendix and signing Annex I.A." to the Decision.[213]

Of note is clause 6, binding the data importer and exporter to a "description of the transfer(s)" specified in Annex I.B,[214] requiring that for all types of transfer the parties must identify the "categories of data subjects whose personal data is transferred", the "categories of personal data transferred", whether it involves sensitive data, the "frequency of the transfer", the "nature of the processing" and what purpose it will serve,

[209] ibid., recital 3, clause 2.; PETROLI, Mallory – **New Standard Contractual Clauses Under the GDPR** [online]. The National Law Review. 9 August 2021. [accessed: 21 June 2022]. Available at: <URL: https://www.natlawreview.com/article/new-standard-contractual-clauses-under-gdpr>.
[210] EDPB, EDPS – op cit., p. 6.; PETROLI, Mallory – op cit.
[211] ibid.; Decision 2021/214.
[212] GDPR, Art. 4(7), Art. 4(8).
[213] Decision 2021/914, clause 7.; CAMPAGNUCCI, Marcelo [et al.] – op cit., p. 44 *supra* note 206.
[214] Decision 2021/914, clause 6.

as well as for how long the imported data will be retained and whether it will be subjected to further processing from other entities or (sub-) processor once imported.[215]

Clause 9 addresses the use of sub-processors for module two and module three transfers, clause 11 provides for the means of redress available to data subjects when invoking a third-party beneficiary right, clause 12 deals with the liability of the parties arising from the obligations pursuant to the clauses, and clause 13 clarifies which supervisory authority will oversee compliance depending on the type of transfer.[216] Section IV, comprising clauses 16 to 18 deal, respectively, with procedural obligations relating to the termination of the contract, the Member State's law governing the Clauses, and the choice of forum and jurisdiction.[217]

In light of the subject matter of this thesis and to better understand to what extent the SCCs may protect data subjects from U.S. surveillance laws closer attention will be paid to clause 8 laying out the data protection safeguards that all parties must implement prior to a transfer, clause 10 which lays out the rights that may be invoked by data subjects, clause 14 dealing with situations where local laws interfere with compliance with the clauses and, finally, clause 15 which sets out the steps the data importer must take if public authorities in the third country gain access to the transferred data.

3.1.1. Close-up: clause 8 "data protection safeguards"

Clause 8 establishes several obligations to ensure that, before transferring data outside the EEA, data exporters made "reasonable efforts to determine" that data importers have implemented the necessary "appropriate technical and organisational measures" guaranteeing the protection of personal data as required by the Clauses.[218]

A. Module one: transfer from controller to controller

In the case of cross-border transfers between controllers, data protection safeguards include the implementation of nine measures, starting with "purpose limitation" – i.e. the processing of data only for specific purposes which must be clearly outlined by both the data exporter and data importer according to Annex I.B to the Decision.[219] Any further processing beyond what was agreed by the parties as per Annex I.B must be either based

[215] ibid., Annex I.B.
[216] ibid., clause 9, clause 11-clause13.
[217] ibid., clauses 16-18.
[218] Decision 2021/914, clause 8.
[219] ibid., module one, §8.1.

on consent from the data subject, limited to a derogation for the purposes of "administrative, regulatory or judicial proceedings" or to protect "the vital interests of the data subject or of another natural person."[220]

Other safeguards include "transparency" concerning the availability to the data subject, pursuant to clause 10 dealing with data subject rights, of the identity and contact details of the data importer, the categories of personal data being processed and whether onwards data transfers to third parties are to be expected and for what purposes,[221] as well as "accuracy and data minimisation" ensuring that the data being transferred is correct, relevant and limited to the purposes of processing.[222] In addition, data should be stored only for the duration and purpose of the processing ("storage limitation") and subsequently be subject to "technical or organisation measures to ensure compliance" once the retention period is over such as erasure or anonymisation.[223]

To ensure "security of processing" during the transmission, both the data importer and data exporter must "implement appropriate technical and organisational measures" – some of which are suggested in Annex II of the Decision and include pseudonymisation and encryption of personal data among others, – as well as "take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subject".[224] These steps are necessary to ensure data protection in the event of a personal data leak i.e., the "accidental or unlawful destruction, loss alteration, unauthorised disclosure or access" of data – in which circumstance, the data importer shall notify either the data exporter and the competent supervisory authority or the data subject depending on the level of severity of the breach, which is measured by the risk to data subjects' rights and freedoms.[225] Data importers should also ensure that anyone taking part in the processing activities "have committed themselves to confidentiality or are under an appropriate obligation of confidentiality."[226] These measures are the consolidation of Section 2 of Chapter IV of the GDPR entitled "security of personal data" where we can find, at times word by word as in Decision 2021/914, how the security of personal data should be ensured (Article 32)

[220] ibid., clause 8, Module one, §8.1.
[221] ibid., §8.2.
[222] ibid., §8.3.
[223] ibid., §8.4.
[224] ibid., §8.5(a).
[225] ibid., §8.5(a)(d)(e)(f).
[226] ibid., §8.5(c).

as well as the steps and conditions to notify a breach of personal data to the supervisory authority or the data subject (Articles 33 and 34 respectively).[227]

Regarding "sensitive data" additional safeguards must be implemented by the data importer according to the sensibility of the data processed and the risks of a data breach.[228] Sensitive data include information concerning "racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions or offences." [229]

Transfers of data to other entities located in the third country of the controller acting as data importer or to another third country ("onward transfers") are prohibited where the third party is not subjected to the SCCs.[230] Exceptions to this rule are only permitted in six instances: where an adequacy decision has been adopted by the Commission as per Article 45 of the GDPR regarding the third country the data importer wishes to transfer data to;[231] if the third party has implemented appropriate safeguards or binding corporate rules as per Article 46 and 47 of the GDPR;[232] if the third party has concluded an agreement with the data importer guaranteeing "the same level of data protection" as the clauses and a copy of said agreement is given to the data exporter;[233] or, much like paragraphs of Article 49 of the GDPR pertaining to "derogations for specific situations", when the onward transfer is relevant for legal proceedings, the protection of "the vital interests or the data subject or of another natural person", or if "explicit consent" is obtained by the data subject authorizing the onward transfer.[234]

Finally, the data importer should make sure that any processing activity happens strictly under its instructions, and both the data importer and the data exporter should be able to prove compliance with the SCCs by documenting processing activities, and in the

[227] GDPR, Art. 32-34.
[228] Decision 2021/914, clause 8, module one, §8.6.
[229] ibid.
[230] ibid. §8.7.
[231] ibid. §8.7(i).
[232] ibid. §8.7(ii).
[233] ibid. §8.7(iii).
[234] ibid. §8.7(iv)-§8.7(vi).; GDPR, Art. 49(1)(a)(e)(f).

case of the controller acting as importer, making such documentation available to the supervisory authority on request. [235]

B. Module two: transfer from controller to processor

In the case of cross-border transfers from a controller to a processor similar obligations to module one must be observed, in particular, requirements pertaining to purpose limitation, transparency, accuracy, security of processing and additional safeguards related to the processing of sensitive data; however, they may take different forms at times. For instance, subclause 8.1 of this module sets out specific instructions related to the role of the data importer acting as a processor: the data importer "shall process the personal data only on the documented instructions from the data exporter".[236] As such, contrary to the "purpose limitation" obligation under module one, data importers must strictly stick to processing personal data according to the purposes defined by both parties in Annex I and explained *supra*, "unless on further instructions from the data exporter."[237] There is not, therefore, the possibility of further processing based on the consent of the data subject, or any other exception as envisioned by subclause 8.1 of module one.

Regarding transparency, data exporters should make available to the data subject, when requested, a copy of the clauses as well as the Appendix.[238] As for accuracy, data importers should promptly notify the data exporter whenever personal information is inaccurate or has become obsolete and work with the data exporter "to erase or rectify the data".[239]

Contrary to module one, module two is stricter regarding the duration of processing activities, stipulating that processing shall "only take place for the duration specified in Annex I.B,[240] while the timely constraint for transfers from a controller to anther in module one, besides those set out by both parties in Annex I.B, is that data importers should not keep information "for no longer than necessary for the purpose(s)" of processing.[241] In addition, once processing ceases, data importers acting as processors should "delete all personal data processed on behalf of the data exporter and certify to the

[235] Decision 2021/914, clause 8, module one, §8-8.9.
[236] Decision 2021/914, clause 8, module two, §8.1.
[237] ibid., §8.2.
[238] ibid., §8.3.
[239] ibid., §8.4.
[240] ibid., §8.5.
[241] ibid., module one, §8.4.

data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies."[242]

As for safeguards relating to the security of processing, they are very similar to the ones mentioned above for module one, with the exceptions that module two specifies that whenever pseudonymisation is used to ensure data security from personal data breaches, "the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter."[243]

When considering sensitive data, the data importer must comply strictly with "the specific restrictions and/or additional safeguards described in Annex I.B" and therefore agreed upon by both parties,[244] while that for module one, the parties have some leeway and are not necessarily bound by the conditions agreed in Annex I.B.[245] In the case of onward transfers, the same obligations are expected from a transfer between a controller and a processor as from one between controllers with the difference that the data importer acting as the processor doesn't have the authority to ask for the consent of the data subject before an onward transfer to a third party.[246]

Transfers under module two are also stricter in terms of safeguards related to "documentation and compliance". In the same way that in module one the controller acting as a data importer must document processing activities, the same happens in transfers pursuant to module two; however, the processor acting as the data importer in module two is also expected to "make available to the data exporter all information necessary to demonstrate compliance" and "allow for and contribute to audits of the processing activities".[247] Audits may be organised by the data exporter or an independent auditor and "may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice."[248] Furthermore, documents relaying the processing activities of the data importer and information demonstrating compliance shall be made available "to the competent supervisory authority on request."[249]

[242] ibid., module two, §8.5.
[243] ibid., §8.6.
[244] ibid., §8.7.
[245] ibid., module one, §8.6.
[246] ibid, module two, §8.8; module one, §8.7.
[247] ibid., module one, §8.9; module two §8.9(b)(c).
[248] ibid., module two, §8.9(d).
[249] ibid., §8.9(e).

C. Module three: transfer from processor to processor

The technical and organisational measures for cross border transfers between processors are almost identical to module two obligations with the exception that, in this instance, the data exporter acts as intermediary between the controller and the data importer, as such the data importer "acts as processor under the instructions of its [the data exporter's] controller(s)".[250] As a consequence the data importer can only process personal data "on documented instructions from the controller, as communicated to the data importer by the data exporter, and any additional documented instructions from the data exporter" and failing that the data exporters is under the obligation to notify the controller.[251]

D. Module four: transfer processor to controller

On the fourth and final module regarding data protecting safeguards, Decision 2021/914 is very curt, setting out only "instructions", "security of processing" and "documentation and compliance" subclauses. Here, again, it is emphasised that the processor, this time acting as the data exporter, can only process data "on documented instructions from the data importer acting as its controller"; however, the data importer cannot restrict the data exporter in its obligations under the GDPR, particularly in matters of sub-processing or in the cooperation with supervisory authorities.[252] Once processing activities end, the data exporter shall return or "delete all personal data processed on behalf of the data importer and certify to the data importer that it has done so".[253]

3.1.2 Close-up: clause 10 "data subject rights"

Regarding data subject rights, most obligations fall upon the data controller. As such, in cross-border transfers from controller to controller the data importer should answer, with the help of the data exporter if necessary, and within a month, "any enquiries and requests it receives from a data subject relating to the processing of his/her personal data and the exercise of his/her rights under these Clauses".[254] This includes, informing the data subject if their personal data is being processed and making a copy of it available to the data subject, inform the data subject of whether their data was subjected to an onward transfer and, if yes, provide the contact of the recipients and the purpose of the onward

[250] ibid., module three, §8.1(a).
[251] ibid., §8.1(b)(c).
[252] ibid., module four, §8.1(a)(c).
[253] ibid., §8.1(d).
[254] ibid., clause 10, module one (a).

transfer and, finally, controllers should be able to provide information as to "the right to lodge a complaint with a supervisory authority in accordance with clause 12(c)(i)".[255] Besides this, the rectification and erasure of data where the data subject withdraws consent or objects to the processing of information for "direct marketing purposes" should be ensured.[256] In addition, automated processing of the transferred data by the data importer without explicit consent of the data subject is prohibited as it would produce legal effects – except where the domestic laws of the country authorise it, but only if the same laws provide for "suitable measures to safeguard the data subject's rights and legitimate interests."[257]

If the transfer entails the transmission of data from a controller to a processor, the processor acting as data importer should notify the data exporter of requests received by data subjects and only answer if it was authorised to do so by the data exporter.[258] So as to efficiently answer requests, both parties should identify the technical and organisational measures, as set out in Annex II, facilitating the data importer's assistance in answering requests.[259]

When it comes to module three transfers between processors, the processor acting as data importer must follow the same steps as the module two data importer processor with the difference that in addition to notifying the processor acting as data exporter, it may also have to notify the controller of requests received by data subjects.[260] As for module four transfers between a processor and a controller, both parties must work together in responding to data subjects "under the local law applicable to the data importer or, for processing by the data exporter in the EU, under Regulation (EU) 2016/679."[261]

3.1.3 Close-up: clause 14 "local laws and practices affecting compliance with the Clauses"

According to clause 14, and in all modules of transfer, the parties must "warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any

[255] ibid., (b)(i).
[256] ibid. §(b)(ii)(iii), (c).
[257] ibid., (d).
[258] ibid., clause 10, module two, (a).
[259] ibid., clause 10, module two, (b).
[260] ibid., clause 10, module three, (a), (b).
[261] ibid., clause 10, module four.

requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses."[262]

This clause is among the novelties introduced by Decision 2021/914, and it was commended by both the EDPB and EDPS for addressing issues raised by the CJEU in *Schrems II*.[263] Indeed, clause 14 takes into account the argument made by the Court that each transfers should be assessed on a "case-by-case basis" by underlining that parties must consider legislation applicable to the *processing* activities specific to the transferred data.[264] In addition to this, it incorporates the notion that access by public authorities is only acceptable if it is in line with the principle of proportionality,[265] – as it emphasises that laws requiring disclosure or access by public authorities do not necessarily infringe the clauses if they "do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) Regulation (EU) 2016/679", according to which data subjects' rights may be restricted only in a series of instances such as to safeguard national security, defence and public security.[266]

In the assessment required by clause 14 both parties should consider, (1) "the specific circumstances of the transfer", i.e., "the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred"; (2) "the laws and practices of the third country of destination", particularly laws requiring disclosure or authorising access by public authorities; and (3) additional "contractual, technical or organisational safeguards" that may reinforce protections guaranteed by the clauses during transmission or processing activities in the third country.[267]

Clause 14 also requires the data importer to notify the data exporter if the legal situation in the third country changes after the conclusion of the contract, and laws and practices no longer fall within the clauses' requirements.[268] If this is the case, and if the

[262] ibid., clause 14(a).
[263] EDPB, EDPS – op cit., p. 7.
[264] *Schrems II*, §134.; Decision 2021/914, clause 14(b).
[265] *Schrems II*, §172-176.
[266] Decision 2021/914, clause 14(a).; GDPR, Article 23(1).
[267] Decision 2021/914, clause 14(b).
[268] ibid., clause 14(e).

data exporter has reason to believe that the data importer is no longer apt to comply with the clauses then "appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality)" should be put in place. If, on the other hand, the implementation of supplementary measures is not possible then the data exporter shall suspend the transfer (in the case of module three transfers, this decision must be taken by the controller).[269] In this instance, the competent supervisory authority also has the power to instruct the data exporter to suspend the transfer.[270] This is another instance where the influence of *Schrems II* can be observed as the CJEU stated that data transfers to third countries whose laws don't offer an equivalent level of protection may still occur, but only if they are supplemented with additional safeguards.[271]

3.1.4. Close-up: clause 15 "obligations of the data importer in case of access by public authorities"

For all module transfers, two obligations arise if personal data has been accessed by public authorities: notify the data exporter and if necessary to the data subject, and review the legality of the request and data minimisation.[272] A notification by the data importer is necessary if it "receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses", or if it "becomes aware of any direct access by public authorities to personal data transferred".[273] If authorities or laws preclude the data importer from communicating about the disclosure or access, it should do everything in its power to either obtain a waiver or provide "as much relevant information as possible on the requests received" where the laws of the third country permit it.[274]

The second step expected of the data importer is to verify if the public authority has the power to issue such a request and challenge it or appeal if it concludes that there are "reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity".[275] This legal assessment shall be documented and made available to the data exporter, where the laws of the third country permit it, and if requested by the

[269] ibid., clause 14(f).
[270] ibid.
[271] *Schrems II*, §131-133.
[272] Decision 2021/914, clause 15.1, 15.2.
[273] ibid., clause 15.1(a).
[274] ibid., clause 15.1(b)(c).
[275] ibid., clause 15.2(a).

competent supervisory authority.[276] Furthermore, when replying to the requested disclosure, "the data importer agrees to provide the minimum amount of information permissible".[277]

All in all, the requirements and obligations expected of parties to the SCCs are quite extensive. Data importers and exporters do not only have to be prepared management-wise prior and during data transfers by implementing technical and organisational safeguards, but they must also be ready to assess third countries' laws (as it is the case for data exporters) and domestic laws (in the case of data importers) in order to verify compliance with the clauses and respond accordingly if obligations cannot be complied with. This assessment, known in the privacy protection landscape as a "Transfer Impact Assessment" (TIA),[278] is for all intents and purposes a similar evaluation to the one conducted by the Commission prior to the adoption of an adequacy decision pursuant to Article 45 of the GDPR. The EDPB itself emphasised that an important step in identifying the applicable law to the data transfer in question entails the evaluation of "different aspects of the legal system of that third country, e.g., the elements listed in Article 45(2) GDPR".[279]

Even though Annex II to Decision 2021/914 sets out some examples of technical and organisational safeguards that can be implemented by both parties, such pseudonymisation and encryption, "measures for the protection of data during storage" or "measures for ensuring data minimisation", these are for the most part general in character even though the explanatory note in the Annex underlines that measure "must be described in specific (and not generic) terms".[280] As the CJEU didn't specify what it understood by "additional safeguards", nor does the GDPR, the EDPB adopted recommendations on supplementary measures reflecting the new standards set by Decision 2021/914 and *Schrems II* to help data exporters in their task.[281]

[276] ibid., clause 15.2(b).
[277] ibid., clause 15.2(c).
[278] TAYLORWESSING – **Transfer Impact Assessment Tool (TIA tool)** [online]. [accessed: 27 June, 2022]. Available at: <URL: https://www.taylorwessing.com/en/campaigns/de/transfer-impact-assessment-tool>.
[279] Recommendations 01/2020, p. 16, §37 *supra* note 198.
[280] Decision 2021/314, Annex II.
[281] EDPB – Recommendations 01/2020 *supra* note 198.

3.2 The EDPB Recommendations on supplementary measures

In its recommendations the EDPB suggests a six-step approach to evaluate the level of protection of third countries and to implement the necessary supplementary measures for data transfers.[282] It advises to (1) "know your transfers" much in the sense of not only knowing the country of destination, but also ensuring accuracy and data minimisation; (2) "verify the transfer tool your transfer relies on"; (3) assess the third countries' laws and practices so as to evaluate if there is anything undermining "the effectiveness of the appropriate safeguards of the transfer tools you are relying on, in the context of your specific transfers"; (4) "identify and adopt supplementary measures" if, in step three, the data exporter finds reason to believe that the laws and practices of the third country don't provide for an equivalent level of protection as found in the EEA; (5) "take any formal procedural steps" required of the supplementary measures; and (6) "re-evaluate" the level of protection of personal data in the third country.[283] In what will ensue, we will primarily focus on steps three and four of the assessment process as outlined by the Board.

Regarding data transfers to the U.S. some recommendations are particularly important. Much like Clause 14, the EDPB clarifies that, as opposed to the general scope of an adequacy decision, an assessment of a country's level of protection in light of Article 46 requires an evaluation of the laws and practices applying *specifically* to the data that is being transferred.[284] Therefore, notwithstanding the Court's findings in *Schrems II* regarding U.S. surveillance laws, data exporters may still transfer data to the U.S. in two scenarios: either they implement additional technical, organisational or contractual safeguards, or they are able to prove that the scope of Section 702 of FISA does not apply to the specific circumstance of the data transfer in question, which entails that data exporters review "objective, reliable, verifiable and preferably publicly available information" including information forwarded by the data importer.[285]

In fact, the latter assessment appears to take from Clause 14(b)(ii) of Decision 2021/914 pertaining to the assessment of local laws and practices and, particularly, its explanatory note where the Commission states that, as part of the assessment of local laws, "documented practical experience with prior instances of requests for disclosure

[282] ibid., p. 4.
[283] ibid., p. 4.
[284] ibid., p. 14, §32.
[285] ibid., p. 20.

from public authorities, or the absence of such requests" are not enough.[286] Instead, these documented experiences must be complemented with "objective elements" meaning that the data importer and data exporter's evaluation must be "corroborated and not contradicted by publicly available or otherwise accessible, reliable information on the existence or absence of requests [for disclosure of data] within the same sector and/or the application of the law in practice such as case law and reports by independent oversight bodies".[287]

Namely the data exporter should seek to find out, first, if there is a "legal prohibition" or "wide restrictions" on revealing information about U.S. authorities requests for access data,[288] as the notification of the data exporter and the data subject by the data importer is required pursuant to Decision 2021/914.[289] Secondly, the data exporter must assess if the data importer "has received requests for access to data from U.S. public authorities in the past" and, if the answer is yes, whether it was prohibited "from providing information about such requests".[290] Finally, it should evaluate whether publicly available information "on U.S. case law and reports from oversight bodies, civil society organisations, and academic institutions reveal data importers of the same sector" have been asked beforehand to divulge data that is similar to the personal information being transferred by the public authorities.[291] If this assessment fails, the data exporter can only proceed with the transfer if it implements supplementary safeguards ensuring the protection of the data.

Given that *Schrems II* has brought to light the lack of proportionality of Section 702 and E.O. 12333 and keeping in mind the wide-reaching capacities of U.S. surveillance programs, as well as the cooperation that is expected of electronic communication service providers for the collection of data, as was already pointed out in Chapter II of this thesis, it may be inferred that the likelihood that data transferred to the U.S. falls within the scope of either Section 702 or E.O. 12333 is high, and therefore that supplementary safeguards will have to be implemented in almost all transfer circumstances to ensure an equivalent level of protection to the one found in the EEA.

[286] ibid., p. 15, §34.; Decision 2021/914, Clause 14(b)(ii).
[287] ibid.
[288] Recommendations 2020/01, p. 20.
[289] Decision 2021/914, clause 15, §15.1.
[290] Recommendations 2020/01, p. 20.
[291] ibid., p. 21.

The EDPB suggests three kinds of supplementary measures: technical, contractual, and organisational safeguards and envisions several hypothetical transfer scenarios where effective safeguards are correctly implemented, as opposed to cases where safeguards cannot ensure an appropriate level of protection.

Among the technical safeguards, the Board suggests both encryption and pseudonymisation. In cases where data is stored in a hosting service provider located in a third country, the Board recommends strong encryption "conform to the state-of-the-art", "robust against cryptanalysis" and whose algorithm is backed up by a "software without known vulnerabilities" and verified, for instance, by certification as conform "to the specification of the algorithm".[292] However, the key to the encrypted data should be in the possession of the data exporter or "an entity trusted by the exporter in the EEA or under a jurisdiction offering an essentially equivalent level of protection to that guaranteed within the EEA."[293] Encryption is also an effective way to circumvent the collection of data in transit by public authorities during the transmission process.[294] This is the case, for instance, for Upstream collection.

As for pseudonymisation, which according to the GDPR entails "the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information",[295] the EDPB emphasises that the effectiveness of this technique depends on the additional information being in exclusive possession of the data exporter or of an "entity trusted by the exporter in the EEA or under a jurisdiction offering an essentially equivalent level of protection to that guaranteed within the EEA" as well as the quality of the algorithm or repository allowing the reestablishment of the link between the data and the individual.[296] As in some instances it is easy to pierce together a person's identity by linking the pseudonymised data with other elements such as the physical, social, cultural or economic characteristics of the individual, or their use of the internet or location, data importers should conduct "a thorough analysis of the data in question" so as to ensure that public authorities in the third country are unable to identify the data subject by cross-referencing information.[297]

[292] ibid., p.30, §84.
[293] ibid.
[294] ibid., p.32, §90.
[295] GDPR, Art. 4(5).
[296] Recommendations 2020/01, p. 31, §85.
[297] ibid.

Besides technical safeguards, another supplementary measure recommended by the EDPB is the incorporation of additional contractual clauses agreed upon by the parties and complementing the SCCs adopted by the Commission. This may include clauses stipulating that the transfer will only take place after the implementation of a specific technical measure,[298] or clauses requiring more transparency from the data importer such as the listing of legal constraints that it is submitted to, under what conditions it is expected to provide information to public authorities and whether it has willingly created any "back doors or similar programming that could be used to access the system and/or personal data."[299] Reinforced audits of not only the data importer but also of sub-processors to evaluate whether public authorities have accessed data may also be included as part of transparency measures.[300] Lastly, the Board recommends the adoption of clauses extending the exercise of data subjects' rights, such as an obligation to notify the data subject in cases where public authorities in the third country have potentially accessed personal information, as this would give an opportunity to the data subject to contact the exporter or lodge a complaint to the supervisory authority.[301]

Finally, some of the organisational measures suggested by the EDPB to ensure data minimisation include the implementation of audits and disciplinary measures related to strict confidentiality and data access policies.[302] Therefore it is recommended to apply "strict data security and data privacy policies, based on EU certification or codes of conducts or on international standards (e.g. ISO norms) and best practices (e.g. ENISA)".[303] Indeed, the establishment of "data protection certification mechanisms and of data protection seals and marks for the purpose of demonstrating compliance" is encouraged by the GDPR.[304] The most well-known certification mechanisms and standards are the ones developed by the International Organization for Standardization (ISO), which developed standards for information security management systems (ISMS), known as ISO 27001, as well as privacy information management systems (PIMS), known as ISO 27701.[305] While ISO 27001 establishes standards for risk-management relating to data security threats such as "loss or unauthorised access" and suggests the

[298] ibid., pp. 36-37, §103.
[299] ibid., pp. 37-38, §106, 109.
[300] ibid., p. 39, §111-112.
[301] ibid., p. 42, §124-125.
[302] ibid., p. 45, §137-138.
[303] ibid., p. 46, §141.
[304] GDPR, Art. 42(1).
[305] BRADFORD, Laura [et al.] – op cit., p.31 *supra* note 199.

implementation of "policies, procedures and staff training",[306] ISO 27701 sets standards, policies and procedures to help organisations comply with the GDPR by assisting them with internal and third-party audits "resulting in detailed proof of compliance with the standard."[307] To be effective both certifications should be implemented together.[308] Together, they show "a commitment to a suite of state-of-the-art protocols and standards for data processing".[309]

4. The limits of SCCs and the future for data transfers to the U.S.

After the Court's ruling in *Schrems II*, SCCs have emerged as the main legal basis for data transfers across the Atlantic. There is no doubt, at least on paper, that SCCs provide significant safeguards to protect the personal information of data subjects when those protections are lacking in third countries as they ensure that all parties taking part in the transfer and in the processing of data outside EEA borders comply with data protection principles guaranteed by the GDPR such transparency, data minimisation, data accuracy, storage limitation and confidentiality.[310] By granting third-party beneficiaries rights to data subjects, the SCCs enable data subjects to invoke obligations and requirements pursuant to the Clauses when lodging a complaint to a supervisory authority. Most of all, they constraint data exporters to conduct a Transfer Impact Assessment prior to transferring data to risk countries. However, can we without a doubt conclude that SCCs are an effective mechanism to transfer personal data to the U.S. in the absence of an adequacy decision?

The question of safely transferring data to the U.S. is a sensible one. As was discussed in Chater II, U.S. Intelligence have enormous capabilities to collect and process personal data under E.O. 1233 and Section 702 of FISA. Furthermore, electronic service providers are required by law to collaborate with U.S. intelligence but prohibited from revealing such requests,[311] as the Verizon FISA Court Order leaked by Edward Snowden in June 2013 emphasised. Such restrictions compromise, for instance, obligations of

[306] ISMS.ONLINE – **Understanding ISO 27001** [online]. [accessed: 26 June 2022]. Available at: <URL: https://www.isms.online/iso-27001/>.
[307] ISMS.ONLINE – **ISO 27701 – The Standard for Privacy Information Management** [online]. [accessed: 26 June 2022]. Available at: <URL: https://www.isms.online/iso-27701/>.
[308] ibid.
[309] BRADFORD, Laura [et al.] – op cit., p.31.; citing LAUCHAUD, Eric - ISO/IEC 27701 Standard: Threats and Opportunities for GDPR Certification [online]. SSRN Electronic Journal. 2020. p.17.
[310] GDPR, Art. 5.
[311] BIGNAMI, Fransceca, RESTA Giorgio – Transatlantic Privacy Regulation: Conflict and Cooperation. Law and Contemporary Problems [online]. Vol. 78, nº 4 (2015), p. 252.

notification pertaining to clause 15, and although the Obama administration declassified documents revealing the inner workings of surveillance operations, these have been related to Section 215 authorising the surveillance of U.S. citizens, with only very few concerning the functioning of Section 702 authorised surveillance programs.[312] Furthermore, doubts as to the effectiveness of additional safeguards such as encryption can be raised when we consider NSA's technical tools such as the Bullrun project – a classified program allowing the NSA to circumvent encryption and that "actively engages US and foreign IT industries to covertly influence and/or overtly leverage their commercial products' designs" as well as "insert vulnerabilities into commercial encryption systems".[313]

What Canto Moniz phrased in regards to *Schrems I* seems to apply as well to *Schrems II:* "the effects of the Schrems case law transcend the adequacy of the U.S. as a "third country" and impact the regime of data transfers itself, mainly the issue of guaranteeing "continued protection", that is to say, that even after the data transfer, data subjects keep benefiting of the fundamental rights and guarantees arising from EU Law."[314] Indeed, the issue seems to be that U.S. surveillance laws and data protection guaranteed by EU law seem to be, at the moment, inherently irreconcilable. Cross-border transfers are therefore, for the most part, dependent on the implementation of technical, organisational, and contractual measures by data exporters and data importers. In effect, it appears that the U.S. is "structurally inadequate" and "the data transfer regime, both on the basis of adequacy decision or on the basis of "appropriate safeguards" only creates an illusion of protection of the data subject".[315]

Almost two years after *Schrems II*, the EU and the U.S. have reached a new agreement on a new "Trans-Atlantic Data Privacy Framework" which will form the basis of a future adequacy decision following the issuance of an Executive Order by the U.S.

[312] MEDINE, David [et al.] – op cit., p.3 *supra* note 63.
[313] BALL James, BORGER Julian, GREENWALD Glenn – **Revealed: how US and UK spy agencies defeat interne privacy and security** [online]. The Guardian. 6 September 2013. [accessed: 1 July 2022]. Available at: <URL: https://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security>.
[314] CANTO MONIZ, Graça – op cit., p. 26 *supra* note 51 [original text: "os efeitos do caso Schrems transcendem a adequação dos EUA enquanto "país terceiro" e atingem o core do regime das transferências, designadamente a intenção de garantir a "continuidade da proteção", isto é, que mesmo depois de transferidos os dados pessoais o titular continuará a beneficiar dos direitos fundamentais e das garantias a que tem direito na EU"].
[315] ibid., p. 268.

president.[316] The agreement includes "a new set of rules and binding safeguards to limit access to data by U.S. intelligence authorities to what is necessary and proportionate to national security", the oversight of procedures adopted by U.S. intelligence, as well as "a new two-tier redress systems" including a "Data Protection Review Court" whose role will be to hear complaints of EU data subjects regarding access to their data by U.S. Intelligence.[317] In addition, "strong obligations" regarding the processing of data transferred from the EU will be expected of U.S. compagnies based on a "requirement to self-certify" their compliance with the new agreement through the U.S. Department of Commerce.[318] Finally, both superpowers agreed on "specific monitoring and review mechanisms".[319]

At first sight the new agreement seems to provide a solution to a lot of the Court's arguments in *Schrems II*, namely compliance with the principle of proportionality and the availability of legal remedies for data subjects. Can this new framework bring hope for the future of data transfers between the U.S. and the EU?

Reacting to the new development, the EDPB welcomed "the commitments made by the U.S. to take 'unprecedented' measures" and emphasised that the evaluation of any future legal agreement will particularly focus on whether collection of data for national security purposes "is limited to what is strictly necessary and proportionate", whether the redress mechanism will indeed offer data subjects access to effective remedy and fair trial, be able to take binding decisions regarding U.S. intelligence elements, or ensure "judicial remedy against this authority's decision or inaction".[320]

In a reaction to this new development, Mr. Schrems underlined that it was still too early to draw conclusions as the agreement is strictly political and awaits legal drafting, but reassures that if after a legal analysis by EU and US legal experts the future adequacy decision still fails to meet requirements guaranteed by EU law, he won't hesitate to

[316] EUROPEAN COMMISSION – **European Commission and United States Joint Statement on Trans-Atlantic Data Privacy Framework** [online]. Brussels: Press release, 20 March 2022. [accessed: 27 June 2022]. Available at: <URL: https://ec.europa.eu/commission/presscorner/detail/en/ip_22_2087>.
[317] EUROPEAN COMMISSION – **Trans-Atlantic Data Privacy Framewor**k [online]. Brussels: Factsheet, 25 March 20222. [accessed: 27 June 2022]. Available at: <URL: https://ec.europa.eu/commission/presscorner/detail/en/FS_22_2100>.
[318] ibid.
[319] ibid.
[320] EDPB – **Statement 01/2022 on the announcement of an agreement in principle on a new Trans-Atlantic Data Privacy Framework** [online]. 6 April 2022. p. 2.

challenge it once again.[321] In an open letter two months after the announcement, the privacy activist expressed his scepticism as, in his eyes, the main problem lies in U.S. surveillance programs themselves and the bulk collection they enable.[322] Mr. Schrems also pointed out that the expected executive order that will implement new data protection standards in the U.S. might backfire, as such legal instruments don't usually confer third-party rights.[323] In addition, Mr. Schrems also raised concerns regarding the Data Protection Review Court and questioned its independence from the executive branch.[324] Concerns relating to how data subjects might invoke complaints before the Data Protection Review Court, in a context where surveillance orders are more often than not secret, was another issue raised by both Mr. Schrems and other privacy experts.[325]

On a more positive note, the GDPR-compliant certification mechanism based on a seal of approval by the U.S. Department of Commerce was commended, with privacy experts stating that the mechanism would come as a "great relief" for data exporters who would no longer need to conduct a Transfer Impact Assessment prior to data transfers to the U.S. as GDPR-compliant American business would be evident. [326] In the meantime, and in the long term, the matter of legal certainty regarding data transfers to the U.S. is characterised by a question mark. One that only the future will be able to answer.

[321] SCHREMS, Max – **"Privacy Shield 2.0"? – First Reaction by Max Schrems** [online]. Noyb. 25 March 2022. [accessed: 27 June 2022]. Available at: <URL: https://noyb.eu/en/privacy-shield-20-first-reaction-max-schrems>.
[322] SCHREMS, Max – **Open Letter on the Future of EU-US Data Transfers** [online]. Noyb. 23 May 2022. [accessed: 27 June 2022]. Available at: <URL: https://noyb.eu/en/open-letter-future-eu-us-data-transfers>.
[323] ibid.
[324] ibid.
[325] ibid.; VON DEM BUSSCHE, Axel Frhr., VOIGT, Paul, SCHMALENBERGER, Alexander – **Trans-Atlantic Data Privacy Framework (TADPF) - the road ahead** [online]. TaylorWessing. 4 April 2022. [accessed: 28 June 2022]. Available at: <URL: https://www.taylorwessing.com/en/insights-and-events/insights/2022/04/trans-atlantic-data-privacy-framework---the-road-ahead>.
[326] VON DEM BUSSCHE, Axel Frhr [et al.] – op cit.

Chapter IV. Foreign surveillance operated by Member States

The Snowden leaks revealed the domestic and foreign surveillance apparatus of the U.S., but it also marked the start of a closer scrutiny of surveillance practises conducted within EU borders by Member States. Not only did the leaks reveal that the U.S. surveillance targeted European leaders,[327] but they also exposed the cooperation between European intelligence services and American Intelligence.[328] Indeed, Member States such as Sweden, Germany and France are known to exchange intelligence information with their American counterparts.[329]

Although the EU's response to the American mass surveillance was one of condemnation,[330] a study sponsored by the European Parliament a few months following the Snowden leaks revealed that quite a few EU intelligence services used similar surveillance techniques as the U.S. including the interception of data as they flow past.[331] As a matter of fact, the study described the bulk collection of data as "a relatively widespread feature of surveillance by several EU member states, namely the UK, Sweden, France and Germany".[332]

It is to better understand in what ways foreign surveillance operated by Member States is similar or different from that conducted by the United States that this section will provide a non-exhaustive analysis of some of the surveillance measures in force in Sweden, Germany, and France, with a particular focus on the latter as the main case-study.

---

[327] CHASE, Jefferson – **Merkel testifies on NSA spying affair** [online]. DW. 16 February 2017. [accessed: 17 July 2022]. Available at: <URL: https://p.dw.com/p/2XfPe>.
[328] ibid.: SEIBT, Sébastien – **How Denmark became the NSA's listening post in Europe** [online]. France 24. 01 June 2021. [accessed: 17 July 2022]. Available at: <URL: https://www.france24.com/en/technology/20210601-how-denmark-became-the-nsa-s-listening-post-in-europe>.
[329] BIGO, Didier, CARRERA, Sergio, HERNANZ, Nicholas [et al.] – **National programmes for mass surveillance of personal data in EU Member States and their compatibility with EU law** [online]. Directorate-General for Internal Policies, Policy Department C: Citizens Rights and Constitutional Affairs. Brussels: European Parliament, 2013. p.20.; BIGNAMI, Fransceca, RESTA Giorgio – op cit., p. 256 *supra* note 311.; ARTICLE 29 WORKING PARTY – **Working Document on surveillance of electronic communications for intelligence and national security purposes** [online]. 5 December 2014. p.9.
[330] REDING, Viviane – **Speech – Mass surveillance is unacceptable – U.S. action to restore trust is needed now** [online]. European Parliament: Civil Liberties Committee hearing on Data Protection and U.S. Surveillance. Speech/13/1048. 9 December 2013. [accessed: 17 July 2022]. Available at: <URL: https://ec.europa.eu/commission/presscorner/detail/es/SPEECH_13_1048>.
[331] BIGO, Didier [et al.] – op cit., p. 24 *supra* note 329.
[332] ibid.

1. Case-study: France's foreign surveillance practices and laws

As of 2013, France was the second country in Europe operating "the second-most important intelligence data collection and processing centre (…) after the UK" and ranked "fifth in the world of metadata collection after the US, the UK, Israel and China".[333] Like the U.S., the French intelligence services are made up of a variety of agencies administrated by different ministries. The agency in charge of foreign intelligence is the Direction générale de la sécurité extérieure (DGSE) administered by the Ministry of Armed Forces ("Ministère des Armées), as opposed to its counterpart, the Direction générale de la sécurité intérieure (DGSI) tasked with domestic intelligence, and under the jurisdiction of the Ministry of Interior ("Ministère de l'Intérieur").[334]

Although provisions relating to the protection of national security and defence, as well as electronic surveillance are codified since 2012 in the Code de la Sécurité Intérieure (CSI), it was only with law nº 2015-912 of 24 July 2015 ("loi du 24 juillet 2015"), in a context where France was in high alert after the Charlie Hebdo attacks of 7 January 2015, that surveillance practices which were for a long time conducted outside a legal framework were codified, thereby subjecting intelligence gathering to the authorisation of the Prime Minister (PM) and the oversight of an independent administrative authority, the Commission nationale de contrôle des techniques de renseignement (CNCTR).[335]

Indeed, prior to 2015, France was already operating a network of signals intelligence gathering very similar to the United States' with members of the French Intelligence Community confirming to the National Defence and Armed Forced Committee at the National Assembly, "the existence of a metadata intelligence centre" at the DGSE headquarters in Paris, enabling the agency to collect and process "internet flows, social network and phone communications."[336] After the Snowden leaks, the newspaper *Le Monde* reported that metadata from phone communications and internet usage were being collected without any legal framework from various interception sites,

[333] ibid., p. 63.
[334] ibid.; VIE PUBLIQUE – **Renseignement français: quelle organisation et quel cadre légal?** [online]. 13 May 2022. [accessed: 02 July 2022]. Available at: <URL: https://www.vie-publique.fr/eclairage/272339-renseignement-francais-quel-cadre-legal>.
[335] VIE PUBLIQUE – op cit.
[336] BIGO, Didier [et al.] – op cit., p. 63 *supra* note 329. citing ASSEMBLÉÉ NATIONALE – Commission de la défense nationale et des forces armées, Comptes-rendus n° 52, 54, 55, 56, 59 et 62 des réunions du 12 février, 13 février, 19 février, 20 février, 26 février et 13 mars 2013. Available at: <URL: https://www.assemblee-nationale.fr/14/cr-cdef/12-13/index.asp>.

satellites and underwater fiber-optic cables, and stored in a supercomputer occupying three underground floors at the DGSE headquarters, thereby allowing the DGSE to target individuals via their name, on request by other intelligence services – much like the use of selectors by the NSA.[337] In 2014, further reports claimed that one of the main communication service providers in France, Orange, was cooperating with the DGSE to facilitate the collection and interception of data without any legal control.[338] The 2015 amendment to the CSI formally codified this cooperation in Article L851-1 which authorises the government to collect, from electronic service providers, "information or documents processed or retained by their network or electronic communication services", including telephone numbers, connections to electronic communication services, the location of communication devices, as well as any incoming or outcoming communication from the target person, its duration and data – information that should always be available to the CNCTR.[339]

Overtime, more amendments to the CSI were introduced. Law nº 2017-1510 reinforced surveillance practices for domestic security purposes and the fight against terrorism by enabling the interception of communications via electromagnetic waves ("communications hertziennes"), and law nº2021-998 on the prevention of terrorist attacks and intelligence reinforced the interception of communications via satellite.[340]

Overall, surveillance measures, be domestic or foreign, are codified under Book VIII ("Livre VIII") of the CSI, and are authorised by the PM after the issuance of an opinion by the CNCTR.[341] Although the opinions of the CNCTR are not binding, they

[337] FOLLOROU, Jacques, JOHANNÈS Franck – **Révélations sur le Big Brother français** [online]. Le Monde. 04 July 2013. [accessed: 02 July 2022]. Available at: <URL: https://www.lemonde.fr/societe/article/2013/07/04/revelations-sur-le-big-brother-francais_3441631_3224.html>.; BIGO, Didier [et al.] – op cit., pp. 63-64.
[338] FOLLOROU, Jacques – **Espionnage: comment Orange et les services secrets coopèrent** [online]. Le Monde. 20 March 2014. [accessed: 02 July 2022]. Available at: <URL: https://www.lemonde.fr/international/article/2014/03/20/dgse-orange-des-liaisons-incestueuses_4386264_3210.html>.
[339] Code de la sécurité intérieur, Art. L851-1. [hereinafter: "CSI"]. (original text: "peut être autorisé le recueil, auprès des opérateurs de communications électroniques (…) les informations ou documents traités ou conservés par leurs réseaux ou services de communications électroniques, y compris les données techniques relatives à l'identification des numéros d'abonnement ou de connexion à des services de communications électroniques, au recensement de l'ensemble des numéros d'abonnement ou de connexion d'une personne désignée, à la localisation des équipements terminaux utilisés ainsi qu'aux communications d'un abonné portant sur la liste des numéros appelés et appelants, la durée et la date des communications.").
[340] VIE PUBLIQUE – op cit.; LOI nº 2017-1510 du 30 octobre 2017 renforçant la sécurité intérieur et la lutte contre le terrorisme (SILT), JORF n° 0255 du 31 octobre 2017.; LOI nº 2021-998 du 30 juillet 2021 relative à la prévention d'actes de terrorisme et au renseignement, JORF n° 0176 du 31 juillet 2021.
[341] CSI, Art. L821-1.

have weight as the Conseil d'État or the Council of State – France's supreme administrative court and the main legal adviser of the executive and legislative branches[342] – can be sized by the CNCTR when the PM goes against the opinion issued, after which point the authorisation is suspended until the Conseil d'État rules on the matter (except in instances of duly justified emergencies and where the surveillance authorisation has immediate effect).[343]

Regarding foreign surveillance techniques, which are codified under Chapter IV "measures relating to the surveillance of foreign electronic communications" of Title V pertaining to "intelligence gathering techniques subject to authorisation ", Article L854-1 authorises the "surveillance of communications that are sent or received from abroad" for the purposes of "defending and promoting the fundamental interests of the Nation" pursuant to Article L811-3 i.e. preserving "national independence, the integrity of the territory and national defence; major interests of foreign policy, compliance with European and international commitments undertaken by France and the prevention of any form of foreign interference; France's economic, industrial and scientific interest; the prevention of terrorism" as well as preventing any threat to public order, organised crime and the proliferation of weapons of mass destruction.[344] The targeting of communications with a domestic link are excluded from this authorisation if they do not originate from abroad or are already subject to an authorisation pursuant to Article L852-1 dealing with the interception of domestic electronic communications.[345]

Concretely, the PM must first designate, by a "reasoned decision" ("decision motivée"), a "network of electronic communications" wherein the interception of information originating from or received abroad is authorized.[346] The second step in the foreign surveillance procedure is the processing of intercepted data which may follow two different types of processing: the "non-individualised processing of intercepted metadata" ("l'exploitation non individualisée des données de connexion interceptées"), in other words, the collection of metadata in bulk; or the processing of "intercepted communications or metadata" ("exploitation de communications, ou de seules données

[342] CONSEIL D'ETAT – **Les missions du Conseil d'État** [online]. [accessed: 06 July 2022]. Available at: <URL: https://www.conseil-etat.fr/qui-sommes-nous/le-conseil-d-etat/missions>.
[343] CSI, Art. L821-1.
[344] ibid., Art. L854-1, Art. L811-3.
[345] ibid., Art. L854-1.
[346] ibid., Art. L854-2, I.

de connexion"), specific to an individual or group.[347] Both kinds of processing are authorized by the PM after the submission of a "reasoned request" ("demande motivée") by members of the cabinet or their delegates.[348] Depending on the type of processing, the elements that must figure in the reasoned request differ. While in both instances members of the cabinet or delegates must specify in what manner or what aspects of the nation's interests the processing of data will help to safeguard, the reasons behind the request, and the intelligence services in charge of processing operations, non-individualised processing of intercepted metadata requires additional details about "the type of automated processing and its purpose" and, in the case of intercepted communications or metadata relating to an individual, further information about either the geographical scope or the individual(s) and organisation(s) being targeted is mandatory. In addition, in the latter case, the CNCTR is required to issue an opinion prior to the authorization, while that isn't necessary for bulk collection of metadata.[349] An additional difference between the two types of processing activities is that while the authorization for the processing of non-individualised metadata is limited to one year, the authorization for processing intercepted communications or metadata is restricted to a maximum four months.[350]

The CSI also stipulates that data collected can be exchanged within the network of intelligence service ("services spécialisé de renseignement"),[351] and sets limits to the retention of information: communications which were already subject to processing should be destroyed within 12 months and up to a maximum of 4 years after collection,[352] while that metadata should be destroyed up to 6 years after collection.[353]

As for the oversight of these procedures, besides supervising processing operations and issuing an opinion prior to the authorisation of processing activities of

[347] ibid., Art. L854-2, II-III.; DEPRAU, Alexis – **Quelques précisions sur la surveillance des communications éléctroniques internationales** [online]. Le Blog de Droit Admnistratif. 06 July 2018. [accessed: 07 July 2022]. Available at: <URL: https://blogdroitadministratif.net/2018/07/06/quelques-precisions-sur-la-surveillance-des-communications-electroniques-internationales/>.
[348] CSI, Art. L854-2, II-III.
[349] ibid.
[350] ibid.
[351] ibid., Art. L854-6.; for more information about the elements of the French intelligence services see ACADÉMIE DU RENSEIGMENT – **Les services spécialisés de renseignement** [online]. [accessed: 09 July 2022]. Available at: <URL: http://www.academie-renseignement.gouv.fr/services.html>.
[352] CSI, Art. L854-5.
[353] ibid.

individualised communications or metadata and sizing the Council of State in the case where the PM goes against the opinion issued, the CNCTR also receives complaints.[354]

1.1 American and French surveillance: a comparative analysis

1.1.1. The conduct of surveillance operations

Surveillance techniques implemented by both French and American intelligence services are very similar. Both jurisdictions authorise "general" bulk collection of data as well as more "individualised" targeting of communications. In the same way that E.O. 12333 authorises the collection of data in transit and Section 702 enables the Attorney General and the DNI to authorise programs such as PRISM and Upstream based on the designation of a selector related to the targeted person, Chapter IV of the CSI authorises the collection of metadata in bulk, as well as the collection of the content of communications and metadata specific to individuals or groups.[355] In addition, intelligence services of both countries cooperate with communication service providers to obtain access to personal data as described above, and disseminate data among intelligence services following certain conditions.[356]

However, both systems diverge in the procedure leading up to authorised surveillance: while Section 702 attributes the authorisation of surveillance to the Attorney General and DNI with the approval of the FISC, the CSI splits the process in a two-step procedure consisting, first, of the designation, by the PM, of a network of communications that can be the object of targeting and, secondly, the processing of the intercepted data within that network – which must be requested by the ministers concerned and confirmed by the PM.

It can be argued that by fragmenting the procedure, French law is clearer in the types of surveillance, and data processing that are to be expected; as opposed to Section 702 which broadly authorises "the targeting of persons reasonably believed to be located outside the United States" without ever elaborating on the specific methods (now known after the Snowden leaks).[357] Nonetheless, given that both collection and processing activities pursuant to Chapter IV of the CSI are subject to the authorisation of the PM with no control *a priori* of the oversight body, the CNCTR, in contrast to the control

[354] ibid., Art. L854-9.
[355] ibid., Art. L854-2, II-III.
[356] ibid., Art. L854-6.; E.O. 12333, §2.3.
[357] 50 USC §1881a.

exercised by the FISC in the case of Section 702, it can be contended that French law has its shortcomings.

1.1.2. Procedural requirements

Regarding procedural requirements, the heads of the executive in both countries – the PM in the case of France, and the Attorney General and DNI in matters of justice and intelligence for the United States – are required to motivate surveillance measures prior to their implementation. Section 702 requires the submission of a certification to be reviewed and approved by the FISC according to FISA standards, while Chapter IV of the CSI mandates that the PM issues a "reasoned decision" designating a network of electronic communications for targeting, and that ministers or delegates present a "reasoned request" prior to processing activities.[358]

Although the CSI is silent on the criteria or elements constituting the "reasoned decision", the procedure prior to the processing of intercepted data by French intelligence services is more detailed due to it demanding more precisions of the ministers or delegates requesting the authorisation, especially concerning individualised processing of communications. In contrast, certification requirements laid out in Section 702 are more akin to a process of demonstration to ensure that non-U.S. persons will not be intentionally targeted – such is the aim of minimisation and targeting procedures, as well as guidelines for limitations. In this sense, at least regarding processing activities and excluding the "reasoned decision" issued by the PM, French law is clearer and provides for more legal certainty.

In this sense, and even though Chapter IV of Title V is more lenient than the other Chapters in the same title pertaining to domestic surveillance, we can say that Chapter IV meets Title I of FISA ("traditional" FISA) and Section 702 halfway: it provides for both general data collection and individualised targeting. Indeed, as was pointed out in Chapter II of this thesis, Title I of FISA requires the Attorney General or Federal Officer to designate a targeted person and the facilities subject to surveillance prior to surveillance authorisation.[359]

[358] 50 USC §1881a. (g)(1).; CSI, Art. L854-2.
[359] USC §1804(a)(3)(4).

1.1.3 Review and oversight

Both American and French law establish authorities responsible for reviewing surveillance measures: the FISC, which is a judicial body, and the CNCTR, an independent administrative authority. While the FISC reviews and approves certifications authorising foreign surveillance programs *a priori* by issuing a court order, the CNCTR acts more as an authority overseeing the whole processing process, observing "permanent, complete and direct access" to the information collected and transmitted by intelligence services, and with the capacity to control the "technical devices" ("dispositifs techniques") implemented through authorisations and decisions.[360]

As opposed to the FISC, which can issue binding orders requesting the government to make changes to certifications in the case of non-conformity with FISA standards,[361] the CNCTR's opinion is only warranted in a single case regarding foreign surveillance: the authorisation of processing activities pertaining to metadata and communications and when addressing recommendations for compliance to the PM; however, these are only enforceable by the Conseil d'Etat.[362]

Nevertheless, the most striking difference between the two bodies is the fact that contrary to the FISC whose only function is to review and approve certification, the CNCTR is empowered to hear complaints – although its powers are severely limited in this regard. Indeed, the CNCTR can only notify the plaintiff that it has "proceeded to carry out the necessary checks"; it "cannot confirm or deny" the implementation of surveillance measures,[363] which raises questions as to whether it qualifies as providing an effective redress – something which the CJEU reproached to the U.S. in *Schrems II* regarding the treatment of EU data subjects.

1.1.4 Differences in treatment

Finally, both France and the U.S. distinguish between surveillance measures applicable, on the one hand, to nationals and people residing in their territory, and on the other, non-nationals, with surveillance measures applicable to nationals being more detailed and offering more safeguards than the more lenient targeting in matters of foreign surveillance of non-nationals. In the same way that the authorisation of surveillance measures under

[360] CSI, Art. L854-9.
[361] 50 USC § 1881a.(i)(3).
[362] CSI, Art. L854-9.
[363] ibid.

Title I of FISA are conditioned to the identification of the targeted person, the premises targeted and the determination of a link between the target and its status as a foreign agent or power,[364] French law applicable to surveillance of nationals is as detailed regarding the conduct of surveillance operations. For instance, regarding the collection of domestic data directly from electronic service providers, the CSI defines the specific categories of data that can be the object of such collection (i.e. subscription number, the location of device used for communications, the data and duration of communication) and specifies that the target for collection must be designated.[365] As for the bulk collection of domestic data in transit and the subsequent automated processing, the authorisation is limited to terrorist prevention purposes and always subject to the opinion of CNCRT.[366] Conversely, the opinion of the CNCRT is not mandated prior to the bulk data collection of foreign targets, except in matters of individualised targeting.[367]

Differences in treatment can also be found regarding the duration of authorised surveillance. While the authorisation for the processing of data pertaining to French nationals is limited to two months with the possibility of renewal,[368] the processing of non-individualised foreign metadata is fixed to one year, and individualised targeting of communications and metadata is limited to four months.[369]

2. A practice that extends to other Member States

2.1 Sweden

France is not the only Member State whose surveillance practices are reminiscent of the United States'. Like France, Sweden collects the content of communication as well as metadata.[370] Indeed, the agency responsible for intercepting signals intelligence, the National Defense Radio Establishment (FRA), is authorised by the Act 2008:717 on Signals Intelligence in Defence Intelligence Operations to "monitor all cable-bound communications traffic into and out of Sweden, including emails, text messages and telephone calls".[371] Communication service providers operating the infrastructure are legally bound to transfer data through "specific 'interaction' points" so they can be

[364] 50 USC §1804(a)(3)(4).
[365] CSI, Art. L851-1.
[366] ibid., Art. L851-3.
[367] ibid., Art. L854-2.
[368] ibid., Art. L851-3.
[369] ibid., Art. L854-2.
[370] BIGO, Didier [et al.] – op cit., p. 22 *supra* note 329.
[371] ibid., p.58.

captured by the FRA.[372] As it is the case for surveillance authorised by Section 702 of FISA, authorisation for signals intelligence collection conducted by the FRA is issued by an intelligence court, the Underrättelsedomstolen – UNDOM, in the form of "sweeping" warrants "not limited to a specific individual."[373] The similarities with Section 702 and Chapter IV of Title V of the CSI only grow when we consider that Swedish nationals are awarded more protection than their foreign counterparts; indeed, "the FRA is prohibited from the collection of signals that have both a sender and a recipient located in Sweden" and the only type of domestic surveillance allowed is in the context of criminal investigations when there is a "'reasonable suspicion' of serious offenses".[374]

2.2 Germany

Germany's Federal Intelligence Service, the Bundesnachrichtendienst (BND), also conducts surveillance operations on a large scale, collecting and processing data to safeguard against "'threats to German interests' from abroad".[375] Along with other intelligence services such as the Military Counterintelligence Service (the Militärischen Abschirmdienst (MAD)), and the Federal Office for the Protection of the Constitution (the Bundesamt für Verfassungsschutz (BfV)), the BND is able to intercept, by selecting a "keyword", up to 20% of foreign communications in transit thanks to "a service capable of directly connecting to digital traffic nodes".[376] The majority of interception takes place in Frankfurt, where "the biggest node in Germany – and, according to certain figures, in the world" is located: the DE-CIX (German Commercial Internet Exchange) and is processed in BND headquarters.[377] Germany's foreign surveillance activities are regulated by the G-10 Law, which authorises intelligence services to "operate warrantless automated wiretaps of domestic and international communications for specific purposes such as the fight against terrorism or the protection of the Constitution".[378]

Although for many years foreign intelligence activities were carried out with no regard for the right of confidentiality for persons living outside Germany's jurisdiction,

[372] ibid., p.58. citing KLAMBERG, Mark – FRA and the European Convention on Human Rights - A Paradigm Shift in Swedish Electronic Surveillance Law. Nordic Yearbook of Law and Information Technology [online]. Bergen 2010. pp. 96-134.
[373] BIGO, Didier [et al.] – op cit., p.61.
[374] PRIVACY INTERNATIONAL – **The Right to Privacy in Sweden** [online]. Human Rights Committee 116th Session. 2016. p.4.
[375] BIGO, Didier [et al.] – op cit., p. 68.
[376] ibid.
[377] ibid.
[378] ibid., p.71.

the 2016 amendment to the BND Act introduced "the necessity criterion" for the surveillance of EU citizens; however, the monitorisation of the communications from non-nationals remains without legal safeguards.[379] Much like Section 702 of FISA, there's a discrepancy in treatment between German citizens and legal residents of Germany, who are awarded the protection of the G-10 Act, and foreigners: be it citizens of other EU member states whose surveillance is authorised according to "the necessity criterion", or, at the bottom of the chain, third country citizens and even people legally residing in the EU but not possessing EU citizenship, who do not have the same protection as the other persons mentioned.[380] Despite the 2016 amendment of the BND Act excluding the economic surveillance of persons abroad and "the deliberate collection of data on heads of governments of other EU countries",[381] the fact remains that there is, without a doubt, a double standard in German surveillance law, much like U.S., French and Swedish laws.

More recently, the difference in treatment between German nationals and non-nationals regarding surveillance was addressed by the Federal Constitutional Court in the 2020 landmark case *1 BvR 2835/17*, where the it stated that, according to international human rights law, the rule of law and democracy, public authorities are expected to respect the fundamental rights of all persons, including people living outside Germany and EU borders.[382] However, this "does not lead to an obligation of public authorities to ensure the protection of individuals who are in foreign jurisdictions".[383] In other words, while public authorities must exercise a "control over the rights of persons" ensuring the respect of the rights of foreigners in their action,[384] "these obligations apply only to the relationship between the individual and the German state" and, arguably, in matters of electronic surveillance only.[385]

---

[379] ROJSZCZAK, Marcin – Extraterritorial Bulk Surveillance after the German BND Act Judgement. Cambridge University Press [online]. Vol. 17, nº 1 (2021), p. 66.
[380] ibid., p. 67
[381] ibid.
[382] Bundesverfassungsgericht, Judgment of the First Senate of 19 May 2020. 1 BvR 2835/17. §89-§94. [accessed: 12 July 2022]. [hereinafter: "1 BvR 2835/17"].
[383] ROJSZCZAK, Marcin – op cit., p.69.; 1 BvR 2835/17, §101-102.
[384] ibid., p.70. citing ÇALI, Başak – **Has "Control over rights doctrine" for extra-territorial jurisdiction come of age? Karlsruhe, too, has spoken, now it's Strasbourg's turn** [online]. EJIL:Talk!. 21 July 2020. [accessed: 12 July 2022]. Available at: <URL: https://www.ejiltalk.org/has-control-over-rights-doctrine-for-extra-territorial-jurisdiction-come-of-age-karlsruhe-too-has-spoken-now-its-strasbourgs-turn/>.
[385] ROJSZCZAK, Marcin – op cit., p. 70.; citing KREBS, David - **Global dangers and national obligations: Extraterritorial protection obligations in the Basic Law: The BND judgment and the**

3. A double standard? The position of the CJEU and the ECtHR

Although a certain standard regarding the protection of personal information of EU data subjects is required of the U.S. in the context of data transfers, foreign surveillance operations conducted by Member States are as worrying as the programs authorised by Section 702 and E.O. 12333. It can be argued that the capacities available to Member States in terms of budget, work force and technical capacities are more modest than the means available to the U.S.;[386] however, the truth is that surveillance for the interests of protecting national security and data protection seem to be two ideas at war with each other outside as much as much as inside EU borders.

For the EU, the main issue seems to reside in EU primary law itself, according to which "national security remains the sole responsibility of each Member State",[387] therefore making national security an exclusive competence and domain where EU law cannot interfere. Furthermore, pertaining to Article 276 TFEU, the CJEU has no jurisdiction "to review the validity or proportionality" of law enforcement measures and police operations, as well as concerning "the maintenance of law and order and the safeguarding of internal security".[388] Such a state of affairs raises questions as to the influence of *Schrems II* in national surveillance laws of Member States.

Despite the constrains imposed by primary law, the CJEU has ruled on the legality of obligations imposed on communication service providers regarding the collection and retention of data for intelligence purposes pursuant to Directive 2002/58, also known as the e-Privacy Directive (as opposed to ruling on public authorities' surveillance practices and their legality with regards to EU law, which it cannot do).[389] In *Privacy International*, the Court found that national legislation requiring service providers to disclose traffic and

---

debate about a "supply chain law" [online]. Verfassungsblog. 4 July 2020. [accessed: 12 July 2022]. Available at: <URL: https://verfassungsblog.de/globale-gefahren-und-nationale-pflichten/>.; MILLER, Russel A. – **The German Constitutional Court Nixes Foreign Surveillance** [online]. Lawfare. 27 May 2020. [accessed: 12 July 2022]. Available at: <URL: https://www.lawfareblog.com/german-constitutional-court-nixes-foreign-surveillance>.

[386] BIGO, Didier [et al.] – op cit., p. 21.

[387] TEU, Art. 4.

[388] Consolidated version of the Treaty on the Functioning of the European Union, OJ C 326, 26.10.2012, pp. 47–390, Article 276.; ROJSZCZAK, Marcin – op cit., p. 61. *supra* note 379

[389] ROJSZCZAK, Marcin – op cit., p. 61; SAJFERT, Juraj – **Bulk data interception/retention judgements of the CJEU – A victory and a defeat for privacy** [online]. European Law Blog. 26 October 2020. [accessed: 11 July 2020]. Available at: <URL: https://europeanlawblog.eu/2020/10/26/bulk-data-interception-retention-judgments-of-the-cjeu-a-victory-and-a-defeat-for-privacy/>.; Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), OJ L 201, 31.7.2002, pp. 37–47. [hereinafter: "ePrivacy Directive"].

location data to intelligence services "by means of general and indiscriminate transmission exceeds the limits of what is strictly necessary and cannot be considered justified, within a democratic society, as required by Article 15(1) of Directive 2002/58", and that such national provisions are unlawful.[390]

However, in *La Quadrature du Net and Others,* a case brought to the Conseil d'Etat by a number of French NGOs active in data protection and later referred to the CJEU, the Court seemed to backtrack on its previous statement, arguing that France's national provisions might indeed bind service providers to "retain, generally and indiscriminately traffic and location data" in the interests of safeguarding national security, but only in the context of a "genuine and present or foreseeable" threat and with the caveat that such authorisation be subject to review by a court or an independent administrative body possessing binding power.[391] Furthermore, the Court saw no obstacle regarding individualised targeting for national and public security purposes and combatting serious crime, if the authorised surveillance relies "on the basis of objective and non-discriminatory factors" including the identification of a target, the geographical scope and is limited in time.[392] As for situations where service providers are constrained by the government to engage in "automated analysis and real-time collection" of metadata, the same conditions apply (i.e. prior identification of a real, genuine and foreseeable threat to national security) with the added detail that such surveillance practices can only be instituted where the government has "a valid reason to suspect that they are involved in one way or another in terrorist activities".[393]

Although *La Quadrature du Net* narrowed the Court's statement in *Privacy International* and provided some leeway to France, and by extension to Member States' governments in authorising service providers to retain metadata, collect data in real-time and tolerate automated analysis for national security and criminal investigation purposes, the French government did not welcome the CJEU's reasoning. Indeed, at the time of the

---

[390] Judgment of the Court (Grand Chamber) of 6 October 2020. *Privacy International v Secretary of State for Foreign and Commonwealth Affairs and Others.* Request for a preliminary ruling from the Investigatory Powers Tribunal – London, Case C-623/17. EU:C:2020:790. §81-82.

[391] Judgment of the Court (Grand Chamber) of 6 October 2020. *La Quadrature du Net and Others v Premier ministre and Others.* Requests for a preliminary ruling from the Conseil d'État (France) and Cour constitutionnelle (Belgium). Joined Cases C-511/18, C-512/18 and C-520/18. EU:C:2020:791.§137-139, §168.

[392] ibid. §147-151, §165, §168.

[393] ibid., §192.

ruling, a source close to the government contended that the Court's conclusions threatened France's "constitutional identity", thus implicitly stating that the Court was acting *ultra vires* as national security is an exclusive national competence.[394] Despite the government's concerns, the Conseil d'État declined to comment on whether the CJEU was acting *ultra vires* in its 21 April 2021 ruling reviewing the conclusions of the CJEU in *La Quadrature du Net*. However, it did emphasise that "the French Constitution remains the supreme norm within the French national legal system" – indirectly underlining that limits or considerations imposed by the EU's highest jurisdiction will come second, and second only, to national law. Even so, it reassured that an assessment of national security threats would be carried out "from time to time" by the Government and reviewed by an administrative court, including the introduction in French law of an independent binding opinion prior to the use of personal data for intelligence purposes.[395]

While the arm's wresting between national governments and the CJEU regarding the use of personal data as well as metadata for intelligence and national security purposes promises to continue, another legal avenue regarding this matter can be found in the European Court of Human Rights (ECtHR) who has more potential in shaping Member States' surveillance laws than the CJEU, as the scope of the Convention "is not excluded from the area of national security", and the ECtHR has jurisdiction to rule on the lawfulness of the parties' surveillance programs, be them national or foreign, considering the human rights guaranteed by the Convention.[396] Although the majority of cases the ECtHR has heard concern domestic surveillance, it has also ruled on the legality of foreign surveillance measures of Germany, the UK and Sweden.

In *Weber and Saravia v. Germany*, the ECtHr ruled that the monitorisation of telecommunications authorized by G-10 did not infringe the right to privacy or the right to freedom of expression as guaranteed by the ECHR, as the legislation provided for the

---

[394] KAYALI, Laura – **France seeks to bypass EU top court on data retention** [online]. Politico. 3 March 2021. [accessed: 19 August 2022]. Available at: <URL: https://www.politico.eu/article/france-data-retention-bypass-eu-top-court/>.; ALEXANDRU, Valentina – **What France's reaction to the CJEU ruling on data retention could mean for the EU's future** [online]. European Studies Review. 17 March 2021. [accessed: 19 August 2022]. Available at: <URL: https://europeanstudiesreview.com/2021/03/17/what-frances-reaction-to-the-cjeu-ruling-on-data-retention-could-mean-for-the-eus-future>.

[395] CONSEIL D'ETAT – **Connection data: the Council of State conciliates the implementation of European Union law and the effectiveness of the fight against terrorism** [online]. 21 April 2022. [accessed: 19 August 2022]. Available at: <URL: https://www.conseil-etat.fr/en/news/connection-data-the-council-of-state-conciliates-the-implementation-of-european-union-law-and-the-effectiveness-of-the-fight-against-terrorism-and>.

[396] ROJSZCZAK, Marcin – op cit., p. 62 *supra* note 379.

necessary safeguards.[397] By contrast, in the final ruling by the Grand Chamber (GC) in *Centrum för Rättvisa v. Sweden*, the ECtHR held that Sweden's Signals Intelligence Act infringed Article 8 of the ECHR pertaining to the right to privacy on the grounds that it wasn't sufficiently clear on the destruction of "intercepted material which did not contain personal data", that the privacy of individuals was compromised when data was shared with other foreign intelligence agencies, and due to "the absence of an effective *ex post facto* review".[398]

However, and perhaps most important for our analysis, was the GC's assessment in *Big Brother Watch and Others v. the United Kingdom*,[399] where it confirmed the previous findings in the 2018 ruling, i.e. that bulk collection of communications didn't infringe the right to privacy as States Parties had a "margin of appreciation" with regards to bulk collection for the interests of protecting national security; however, this not preclude them from adopting "minimum safeguards" so as to prevent abuses, including the setting out of: (1) the nature of the offenses leading to collection, (2) the identification of the categories of people targeted, (3) the duration of the interception of data, (4) the procedure to follow with regards to collection and retention (5) procedures regarding the transmission of data to other entities and (6) measures relating to the erasure of data.[400] Following the previous assessment, the GC underlined that bulk collection was "a valuable technological capacity to identify new threats in the digital domain";[401] however, it made the distinction – based on States Parties' surveillance practices – between "targeted interception" and "bulk interception".[402] While the former is deployed by States "for the purposes of investigating crime", the latter is used "for the purposes of foreign intelligence gathering", the prevention of cyberattacks, terrorism and counter-espionage.[403]

Of note was also the procedure set out by the GC for States Parties to follow in order to prevent abuses when collecting data in bulk, i.e. for the purposes of foreign

[397] ibid., pp. 57-58.; ECtHR, *Weber and Saravia v Germany*. No 37138/14, 29 June 2006. §137-138, §151-153.; ECHR, Art. 8, Art. 10.
[398] ECtHR Grand Chamber, *Centrum för Rättvisa v. Sweden*. No. 35252/08, 25 May 2021. [accessed: 12 July 2022]. Available at: <URL: https://hudoc.echr.coe.int/fre?i=001-210078>.
[399] ECtHR Grand Chamber, *Big Brother Watch and Others v. the United Kingdom*. No. 58170/13, 62322/14 24960/15, 25 May 2021. [hereinafter: "*Big Brother Watch v. UK*"]. This case was spurred by multiple NGOs acting against the UK government and its mass surveillance practices after the Snowden leaks.
[400] ibid., §274.
[401] ibid., §323.
[402] ibid., §345.
[403] ibid.

intelligence gathering, which includes the minimal safeguards outlined *supra*, with the added conditions that (1) bulk interception should be subject to "end-to-end safeguards" based on continuous assessment at the national level, (2) that "supervision and independent *ex post facto* review" is implemented, and that there is (3) clear authorization and oversight.[404] Interestingly, in paragraph 351 the Court remarks that "bulk interception should be authorised by an independent body; that is, a body which is independent of the executive",[405] which is something that, as we have seen in our analysis of France's foreign surveillance measures, will require changes to the CSI, as bulk collection programs are authorised by the PM himself only. Furthermore, the GC invoked the use of "strong selectors" as "one of the most important steps in the bulk interception process", but that their use should be justified "with regard to the principles of necessity and proportionality" by intelligence services,[406] and the availability of "effective remedy" before a body that is independent of the executive, be it judicial or administrative.[407] The influence of the Snowden leaks, U.S. foreign surveillance operations and the consequent *Schrems* case law is therefore undeniable.

For all intents and purposes, the matter of whether a conciliation is possible between data protection and national security interests promises to be an ongoing debate in the EU as the amendment proposed by the Council to the new e-Privacy Regulation suggests. Indeed, after years of deadlock regarding discussions in the Council concerning the replacement of the 2002 ePrivacy Directive, an amendment to Article 2 of the proposed ePrivacy Regulation and pertaining to its material scope, i.e. "the processing of electronic communications data", "the use of electronic communications services" and "information related to the terminal equipment of end users", [408] and particularly to its second paragraph, introduced a "broad national security exception" following efforts led mainly by France,[409] where we can read (the Council's amendment is transcribed in italics):

[404] ibid., §348-350.
[405] ibid., §351.
[406] ibid., §353, §355.
[407] ibid., §357-359.
[408] Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications). COM/2017/010 final - 2017/03 (COD). Art. 2(2)(a).
[409] CHRISTAKIS, Theodore, PROPP, Kenneth – **How Europe's Intelligence Services Aim to Avoid the EU's Highest Court – and What It Means for the United States** [online]. Lawfare. 8 March 2021.

> "This Regulation does not apply to: (a) activities which fall outside the scope of Union law, *and in any event measures, processing activities and operations concerning national security and defence, regardless of who is carrying out those activities whether it is a public authority or a private operator acting at the request of a public authority*."[410]

This amendment does not only show how cooperation with communication service providers is perceived as essential by Member States in order to obtain access to personal data, but also that they do not wish that EU data protection laws interfere with national security concerns and surveillance operations – which is ironic, given that in the context of data transfers to non-EU countries, states such as the U.S are expected to comply with data protection standards.

[accessed: 17 July 2022]. Available at: <URL: https://www.lawfareblog.com/how-europes-intelligence-services-aim-avoid-eus-highest-court-and-what-it-means-united-states>.

[410] COUNCIL OF THE EUROPEAN UNION – **Préparation du trilogue** [online]. 2017/0003 (COD). 28 March 2022. p.17. [accessed: 17 July 2022]. Available at: <URL: https://data.consilium.europa.eu/doc/document/ST-7458-2022-INIT/x/pdf>.

Conclusion

Coming back to our research question "*In a context where the GDPR and the Schrems case law reshaped data transfers standards, is it possible to ensure the protection of personal data when it is transferred to the United States given its surveillance laws authorising large scale surveillance programs*", we may conclude that although the SCCs adopted by the Commission pursuant to Decision 2021/914 are a solution for controllers and processors wishing to transfer data to the U.S. in the absence of an adequacy decision, they are not always a viable option, as their effectiveness is dependent on the specific circumstance of the transfer.

Indeed, although SCCs legally bind the data exporter and the data importer to implement safeguards protecting personal data prior and during the transfer, require that the data exporter respond to data subjects' requests regarding processing activities concerning their personal data, preclude the automated processing of data without the consent of the data subject, and ensure that the data exporter conducts a thorough assessment of local laws applicable to the a specific transfer prior to transmission, the requirements arising from the SCCs – management and organisational wise – may give rise to doubts as to whether the benefits of the transfer outweigh its costs. Even more so when we consider the possibility of the transfer falling under Section 702 of FISA after transmission and, consequently, the data importer being unable to disclose to the data exporter, as required by the SCCs, the request for access to data issued by U.S. authorities – as cooperation between U.S. intelligence and communication service providers often take place under a confidentiality principle. Data exporters and importers have the option to implement additional safeguards as suggested by the Court in *Schrems II* and the EDPB; however, it is not always clear if these measures are enough to prevent U.S. intelligence from accessing personal data, as the NSA allegedly possesses technical capacities to circumvent technical safeguards such as encryption.

Consequently, it appears that the hurdles likely to arise from transferring data on the basis of SCCs, and that threaten the effectiveness of safeguards ensuring a level of protection equivalent to the EU, concern mostly U.S. surveillance laws themselves. Only an active effort by the U.S. either to grant more protections to non-U.S. persons, such as access to legal remedy for people whose data has been accessed by U.S. intelligence, or an effort to amend FISA to introduce limitations to Section 702 of FISA, will be a solution

to this data transfer conundrum. Considering the new Trans-Atlantic Data Privacy Framework, the most recent agreement on transfer principles between the Commission and the Biden Administration, it seems that the U.S. has opted for the former option and made a few concessions, but a full assessment will only be possible when the political agreement takes the form of a legal text, and the Commission adopts an adequacy decision pursuant to Article 45 of the GDPR.

Nonetheless, the U.S. might not be the only one expected to make space for additional protections in their surveillance operations. In fact, Member States such as France, Sweden and Germany employ similar surveillance techniques as the U.S. and authorise the interception of communications and metadata in bulk. Although this surveillance was for a time conducted in secret and outside a legal framework, as we have pointed out in our case study of France's surveillance laws, and much like it was the case for the U.S. until the FISA amendments Act of 2008, with time the conduct of surveillance operations started to be regulated.

The question of whether there is a double standard in the perception of U.S. surveillance operations and obligations arising from EU law regarding the implementation of data protection requirements, as opposed to surveillance programs implemented by Member States is a relevant one. Although primary law precludes the EU from interfering in national security matters and restricts the CJEU in adjudicating on the proportionality of surveillance measures for the purposes of protecting national security, its latest rulings concerning Member States governments' cooperation with communication service providers for the collection of data, has Member States such as France trembling and taking on a defensive stance – which raises questions as to whether the CJEU is as powerless as primary law says it is. As for the more recent case-law of the ECtHR, *Big Brother Watch and Others v. the United Kingdom* seems to be bringing *Schrems II* requirements to Member States' domestic legal order by setting out procedural requirements to ensure minimum safeguards regarding foreign intelligence gathering in bulk.

Having come to the end of our analysis, it is clear that the issue which renders data transfers to the U.S. so difficult, and that ultimately led to two CJEU landmark rulings invalidating two adequacy decisions adopted by the Commission, i.e., the unproportionally of American surveillance laws, is something that cannot be quickly fixed. Not only because it requires of another jurisdiction to make significant changes to

its laws and long-time held practices, but also due to the fierce and prideful culture regarding the protection of national security that permeates every layer of American society, even more so since the September 11th attacks. Recent terrorist attacks in European soil have also pushed Member States to toughen up their security measures and strengthen foreign surveillance to fight against terrorist threats. While that in the EU data protection rules guard against possible abuses of power, and the matter of the treatment of foreign surveillance targets has recently started to be a subject of discussion, the same does not apply to the U.S. What is clear is that on both sides of the Atlantic, at least from the point of view of the executive and legislative branch, data protection seems to come second to national security concerns, which prompts the question: with technology advancing rapidly and security threats taking different forms and moving to other spheres such as the cyberspace, intelligence services' capacities to intercept, collect and process personal data will only grow to keep up with this new reality – how far and what part of our lives are we willing to sacrifice in the future for the sake of national security?

Bibliography

Laws, Statutes, and other relevant documents with legal value

BARR, William P. – Minimization procedures used by the National Security Agency in connection with the acquisition of foreign intelligence information pursuant to Section 702 of the Foreign Intelligence Surveillance Act of 1978, as amended [online]. Office of the Director of National Intelligence (ODNI): 16 Sept. 2019 (declassified 26 April 2021). [accessed: 08 June 2022]. Available at: <URL: https://www.intel.gov/assets/documents/702%20Documents/declassified/20/2020_Cert_NSA%20Minimization%20Procedures_10.19.2020.pdf>.

Charter of Fundamental Rights of the European Union, OJ C 326/391, 26.10.2012, pp. 391–407. [accessed: 14 June 2022]. Available at: <URL: http://data.europa.eu/eli/treaty/char_2012/oj >.

Code de la sécurité intérieur. [accessed: 02 July 2022]. Available at: <URL: https://www.legifrance.gouv.fr/codes/section_lc/LEGITEXT000025503132/LEGISCTA000030934655/#LEGISCTA000030934655>. ["CSI"].

Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles, OJ L 215, 25.8.2000, pp. 7–47. [accessed: 15 June 2022]. Available at: <URL: http://data.europa.eu/eli/dec/2000/520/oj>. ["Safe Harbour Privacy Principles"].

Commission Decision of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC of the European Parliament and of the Council, OJ L 39, 12.2.2010, pp. 5–18. [accessed: 16 June 2022]. Available at: <URL: http://data.europa.eu/eli/dec/2010/87/oj>. ["Decision 2010/87"].

Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield, OJ L 207, 1.8.2016, pp. 1–112. [accessed: 15 June 22]. Available at: <URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2016.207.01.0001.01.ENG>. ["Privacy Shield Decision"].

Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council, OJ L 199, 7.6.2021, pp. 31–61. [accessed: 16 June 2022]. Available at: <URL: http://data.europa.eu/eli/dec_impl/2021/914/oj>. ["Decision 2021/914"].

Consolidated version of the Treaty on European Union, OJ C 326, 26.10.2012, pp. 13–390. [accessed: 10 July 2022]. Available at: <URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A12012M%2FTXT>.

Consolidated version of the Treaty on the Functioning of the European Union, OJ C 326, 26.10.2012, pp. 47–390. [accessed: 10 July 2022]. Available at: <URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A12012E%2FTXT>.

Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), OJ L 201, 31.7.2002, pp. 37–47. [accessed: 11 July 2022]. Available at: <URL: http://data.europa.eu/eli/dir/2002/58/oj>. ["ePrivacy Directive"].

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281, 23.11.1995, pp. 31–50. [accessed: 15 June 2022]. Available at: <URL: http://data.europa.eu/eli/dir/1995/46/oj>.

EDPB – Guidelines 05/2021 on the Interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR [online]. 18 Nov. 2021. p. 4. [accessed: 15 June 2022]. Available at: <URL: https://edpb.europa.eu/our-work-tools/documents/public-consultations/2021/guidelines-052021-interplay-between-application_en>.

EDPB – Guidelines 3/2018 on the territorial scope of the GDPR (Article 3) [online]. Version 2.1. 12 November 2019. [accessed: 14 June 2022]. Available at: <URL: https://edpb.europa.eu/our-work-tools/documents/public-consultations/2018/guidelines-32018-territorial-scope-gdpr-article_en>.

EDPB – Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data [online]. Version 2.0. 18 June

2021. [accessed: 21 June 2022]. Available at: <URL: https://edpb.europa.eu/system/files/2021-06/edpb_recommendations_202001vo.2.0_supplementarymeasurestransferstools_en.pdf >.

EDPB, EDPS – Joint opinion 2/2021 on the European Commission's Implementing Decision on standard contractual clauses for the transfer of personal data to third countries for the matters referred to in Article 46 (2)(c) of Regulation (EU) 2016/679 [online]. 14 January. 2021. [accessed: 21 June 2022]. Available at: <URL: https://edpb.europa.eu/our-work-tools/our-documents/edpbedps-joint-opinion/edpb-edps-joint-opinion->.

European Convention for the Protection of Human Rights and Fundamental Freedoms as amended by Protocols Nos. 11,14 and 15 supplemented by Protocols Nos. 1,4, 6, 7, 12, 13, and 16. Council of Europe. 1953. [accessed: 14 June 2022]. Available at: <URL: https://www.echr.coe.int/documents/convention_eng.pdf>. ["ECHR"].

Executive Order 12333 "United States Intelligence Activities", as amended by Executive Orders 13284 (2003), 13355 (2004) and 13470 (2008). [accessed: 10 June 2022]. Available at: <URL: https://dpcld.defense.gov/Portals/49/Documents/Civil/eo-12333-2008.pdf >. ["E.O. 12333"].

Foreign Intelligence Surveillance Act of 1978 (FISA), Sec. 102, 50 USC § 1802, 25 October 1978. [accessed: 01 June 2022]. Available at: <URL: https://www.govinfo.gov/content/pkg/STATUTE-92/pdf/STATUTE-92-Pg1783.pdf#page=1>.

Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2008 (FAA), Sec. 702, 50 USC § 1881, 10 July 2008. [accessed: 01 June 2022]. Available at: <URL: https://www.congress.gov/110/plaws/publ261/PLAW-110publ261.pdf>. ["50 USC § 1881a."].

LOI nº 2017-1510 du 30 octobre 2017 renforçant la sécurité intérieur et la lutte contre le terrorisme (SILT), JORF n° 0255 du 31 octobre 2017. [accessed: 06 July 2022]. Available at: <URL: https://www.legifrance.gouv.fr/eli/loi/2017/10/30/INTX1716370L/jo/texte>.

LOI nº 2021-998 du 30 juillet 2021 relative à la prévention d'actes de terrorisme et au renseignement, JORF n° 0176 du 31 juillet 2021. [accessed: 06 July 2022]. Available at: <URL: https://www.legifrance.gouv.fr/eli/loi/2021/7/30/INTD2107675L/jo/texte>.

Presidential Policy Directive – Signals Intelligence Activities [online]. The White House Office of the Press Secretary. 17 January 2014. [accessed: 11 June 2022]. Available at: <URL: https://obamawhitehouse.archives.gov/the-press-office/2014/01/17/presidential-policy-directive-signals-intelligence-activities>. ["PPD-28"].

Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications). COM/2017/010 final - 2017/03 (COD). [accessed: 17 July 2022]. Available at: <URL: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52017PC0010&from=EN>.

Protect America Act of 2007, Public Law. No. 110-55; 121 Stat. 552. 50 USC 1805b. 5 August 2007. [accessed: 01 June 2022]. Available at: <URL: https://www.congress.gov/110/plaws/publ55/PLAW-110publ55.pdf>. ["Protect America Act of 2007"].

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119, 4.5.2016, p. 1–88. Available at: <URL: https://eur-lex.europa.eu/eli/reg/2016/679/oj>. ["GDPR"].

U.S. Constitution, Amendment. IV. Available at: <URL: https://www.senate.gov/civics/resources/pdf/US_Constitution-Senate_Publication_103-21.pdf >.

Case-law

Bundesverfassungsgericht, Judgment of the First Senate of 19 May 2020. 1 BvR 2835/17. §94. [accessed: 12 July 2022]. Available at: <URL: http://www.bverfg.de/e/rs20200519_1bvr283517en.html>.

ECtHR Grand Chamber, *Big Brother Watch and Others v. the United Kingdom.* No. 58170/13, 62322/14 24960/15, 25 May 2021. [accessed: 12 July 2022]. Available at: <URL: https://hudoc.echr.coe.int/fre?i=001-210077>. ["*Big Brother Watch v. UK*"].

ECtHR Grand Chamber, *Centrum för Rättvisa v. Sweden.* No. 35252/08, 25 May 2021. [accessed: 12 july 2022]. Available at: <URL: https://hudoc.echr.coe.int/fre?i=001-210078>.

ECtHR, *Weber and Saravia v Germany*. No 37138/14, 29 June 2006. § 155 [accessed: 12 July 2022]. Available at: <URL: https://hudoc.echr.coe.int/fre?i=001-76586>.

Judgement of the Court (Grand Chamber) of 6 October 2015, *Maximilian Schrems v. Data Protection Commissioner*. Reference for preliminary ruling from the High Court (Ireland), EU:C:2015:650, Case C-362/14. [accessed: 15 June 2022]. Available at: <URL: https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:62014CJ0362>. ["*Schrems* I"].

Judgement of the Court of November 2003. *Criminal Proceedings against Bodil Lindqvist*. Reference for a preliminary ruling: Göta hovrätt-Sweden., EU:C:2003:596, Case C-101/01. Available at: <URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62001CJ0101>. ["*Bodil Lindqvist*"].

Judgment of the Court (Grand Chamber) of 16 July 2020. *Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems*. Request for a preliminary ruling from the High Court (Ireland)., EU:C:2020:559, Case C-311/18. [accessed: 15 June 2022]. Available at: <URL: https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:62018CJ0311>. ["*Schrems II*"].

Judgment of the Court (Grand Chamber) of 6 October 2020. *La Quadrature du Net and Others v Premier ministre and Others*. Requests for a preliminary ruling from the Conseil d'État (France) and Cour constitutionnelle (Belgium). Joined Cases C-511/18, C-512/18 and C-520/18. EU:C:2020:791.§168. [accessed: 11 July 2022]. Available at: <URL: https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:62018CJ0511>.

Judgment of the Court (Grand Chamber) of 6 October 2020. *Privacy International v Secretary of State for Foreign and Commonwealth Affairs and Others*.
Request for a preliminary ruling from the Investigatory Powers Tribunal – London, Case C-623/17. EU:C:2020:790. §81-82. [accessed: 11 July 2022]. Available at: <URL: https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:62017CJ0623>.

Opinion of Advocate General Saugmandsgaard ØE delivered on 19 December 2019. *Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems*. Request for a preliminary ruling from the High Court (Ireland), EU:C:2019:1145, §338 [accessed: 17 June 2022]. Available at: <URL: https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:62018CC0311>.

United States v. United States Dist. Ct., 407 U.S. 297 (1972) [accessed: 30 May 2022]. Available at: <URL: https://supreme.justia.com/cases/federal/us/407/297/>. ["*Keith*"].

Academic articles

BIGNAMI, Francesca – European Versus American Liberty: Comparative Privacy Analysis of Antiterrorism Data Mining. Boston College Law Review [online]. Vol 48, nº 3 (2007), pp. 609-698. [accessed: 19 May 2022]. Available at: <URL: https://lawdigitalcommons.bc.edu/bclr/vol48/iss3/3/>.

BIGNAMI, Fransceca, RESTA Giorgio – Transatlantic Privacy Regulation: Conflict and Cooperation. Law and Contemporary Problems [online]. Vol. 78, nº 4 (2015), pp. 231-266. [accessed: 01 July 2022]. Available at: <URL: https://www.jstor.org/stable/43920638>.

BOYNE, Shawn M. – Data Protection in the United States. The American Journal of Comparative Law [online]. Vol. 66, nº1 (2018), pp. 299–343. [accessed: 06 September 2022]. Available at: <URL: https://www.researchgate.net/publication/326257651_Data_Protection_in_the_United_States>.

BRADFORD, Laura, ABOY, Mateo, LIDDELL, Kathleen – Standard contractual clauses for cross-border transfers of health data after *Schrems II*. Journal of Law and Biosciences [online]. Vol 8, nº 1 (2021), pp.1-36. [accessed: 23 June 2022]. Available at: <URL: https://doi.org/10.1093/jlb/lsab007>.

CAMPAGNUCCI, Marcelo, ABOY, Mateo, MINSSEN, Timo – Cross-Border Transfers of Personal Data after Schrems II: Supplementary Measures and New Standard Contractual Clauses (SCCs). Nordic Journal of European Law [online]. nº2 (2021), pp. 37-49. [accessed: 21 June 2022]. Available at: <URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3951085>.

CANTO MONIZ, G. – A Extraterritorialidade do Regime Geral de Proteção de Dados Pessoais da União Europeia: Manifestações e Limites. Lisbon: Faculdade de Direito Universidade Nova de Lisboa, 2018. PhD Dissertation. Available at: <URL: https://run.unl.pt/handle/10362/89180>.

JAYCOX, Mark. M – No Oversight, No Limits, No Worries: A Primer on Presidential Spying and Executive Order 12,333. Harvard National Security Journal [online]. Vol 12 (2021), pp. 58-115 [accessed: 10 June 2022]. Available at: <URL: https://harvardnsj.org/2021/02/no-oversight-no-limits-no-worries-a-primer-on-presidential-spying-and-executive-order-12333/#_authftn1>.

KLAMBERG, Mark – FRA and the European Convention on Human Rights - A Paradigm Shift in Swedish Electronic Surveillance Law. Nordic Yearbook of Law and Information Technology [online]. Bergen 2010. pp. 96-134. [accessed: 01 July 2022]. Available at: <ULR: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1558843>.

KRIS, David S. – On the Bulk Collection of Tangible Things. Journal of National Security Law & Policy [online]. Vol. 7, nº 2 (2014), pp. 209-295. [accessed: 13 June 2022]. Available at: <URL: https://jnslp.com/2014/05/08/on-the-bulk-collection-of-tangible-things/>.

LAUCHAUD, Eric - ISO/IEC 27701 Standard: Threats and Opportunities for GDPR Certification [online]. SSRN Electronic Journal. 2020. 23p. [accessed: 26 June 2022]. Available at: <URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3521250>.

LYON, David – Surveillance, Snowden, and Big Data: Capacities, consequences, critique. Big Data & Society [online]. SAGE journals. 2014. pp.1-13. [accessed: 29 April 2022]. Available at: <URL: https://doi.org/10.1177/2053951714541861>.

MARGULIES, Peter – Global Cybersecurity, Surveillance, and Privacy: The Obama Administration's Conflicted Legacy. Indiana Journal of Global Legal Studies [online]. Vol. 24, nº. 2 (2017), pp. 459-496. [accessed: 11 June 2022]. Available at: <URL: https://www.jstor.org/stable/10.2979/indjglolegstu.24.2.0459>.

MCDERMOTT Yvonne – Conceptualising the right to data protection in an era of Big Data. Big Data & Society [online]. SAGE journals. 2017. pp. 1-7. [accessed: 14 June 2022]. Available at: <URL: https://doi.org/10.1177/2053951716686994>.

RATNER, Adrienne – Warrantless Wiretapping: The Bush Admnistration's Failure to Jam an Elephant into a Mousehole. Hastings Constitutional Law Quarterly [online]. Vol 37, nº 1 (2009), pp. 167-198. [accessed: 30 May 2022]. Available at: <URL: https://repository.uchastings.edu/hastings_constitutional_law_quaterly/vol37/iss1/5/>.

ROJSZCZAK, Marcin – Extraterritorial Bulk Surveillance after the German BND Act Judgement. Cambridge University Press [online]. Vol. 17, nº 1 (2021), pp. 53-77. [accessed: 10 July 2022]. Available at: <URL: https://doi.org/10.1017/S1574019621000055 >.

SCHREMS, Max – Comentário ao Acórdão in **Em Foco: O Encarregado de Proteção de Dados**. Fórum de Proteção de Dados [online]. Lisbon: Comissão Nacional de Proteção de Dados, n°7 (2020), pp. 108-120. [accessed: 14 June 2022]. Available at: <URL: https://www.cnpd.pt/media/5kajlbve/forum7_web.pdf>.

SOLOVE, Daniel J. – Data Mining and the Security-Liberty Debate. The University of Chicago Law Review [online]. Vol 75, nº 1 (2008), pp. 343-362. [accessed: 19 May 2022]. Available at: <URL: https://chicagounbound.uchicago.edu/uclrev/vol75/iss1/15>.

Working papers and reports

ARTICLE 29 WORKING PARTY – **Working Document on surveillance of electronic communications for intelligence and national security purposes** [online]. 5 December 2014. [accessed: 07 July 2022]. Available at: <URL: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp228_en.pdf>.

BIGNAMI, Francesca – **The US legal system on data protection in the field of law enforcement. Safeguards, rights and remedies for EU citizens** [online]. Directorate-General for Internal Policies, Policy Department C: Citizens Rights and Constitutional Affairs. Brussels: European Parliament, 2015. 36p. [accessed: 27 May 2022]. Available at: <URL: https://op.europa.eu/en/publication-detail/-/publication/2827ac88-5e04-4a51-93b3-31c092e70760/language-en/format-PDF/source-258313876>.

BIGO, Didier, CARRERA, Sergio, HERNANZ, Nicholas [et al.] – **National programmes for mass surveillance of personal data in EU Member States and their compatibility with EU law** [online]. Directorate-General for Internal Policies, Policy Department C: Citizens Rights and Constitutional Affairs. Brussels: European

Parliament, 2013. 80p. [accessed: 01 July 2022]. Available at: <URL: https://data.europa.eu/doi/10.2861/48584>.

BOWDEN, Caspar – **The US surveillance programmes and their impact on EU citizens' fundamental rights**. Directorate General for Internal Policies Police Department C: Citizens Rights and Constitutional Affairs. Brussels: European Parliament, 2013. 37p. [accessed: 19 May 2022]. Available at: <URL: https://op.europa.eu/s/wYep>.

CLAPPER, R. James [et al.] – **Joint Statement of DNI James Clapper, DIRNSA Gen. Keith Alexander, and DAG James Cole Before the House Permanent Select Committee on Intelligence** [online]. Washington D.C, 29 October 2013. [accessed: 20 May 2022]. Available at: <URL: https://irp.fas.org/congress/2013_hr/102913joint.pdf>.

DIGITALEUROPE, BUSINESSEUROPE, ERT, ACEA – **Schrems II Impact Survey Report** [online]. Brussels: 2022. [accessed: 20 June 20, 2022]. Available at: <URL: https://www.digitaleurope.org/wp/wp-content/uploads/2020/11/DIGITALEUROPE_Schrems-II-Impact-Survey_November-2020.pdf>.

EUROSTAT – **The 2017 results of the International Comparison Program China, US and EU are the largest economies in the world** [online]. 2020. Eurostat Press Office. [accessed. 19 April 2022]. Available at: < URL: https://ec.europa.eu/eurostat/documents/2995521/10868691/2-19052020-BP-EN.pdf/bb14f7f9-fc26-8aa1-60d4-7c2b509dda8e >.

MANYIKA, James [et al.] – **Digital Globalization: The New Era of Global Flows** [online]. McKinsey Global Institute, 2016. p. 4. [accessed: 19 april 2022]. Available at: <URL: https://www.mckinsey.com/~/media/mckinsey/business%20functions/mckinsey%20digital/our%20insights/digital%20globalization%20the%20new%20era%20of%20global%20flows/mgi-digital-globalization-full-report.pdf>.

MEDINE, David [et al.] – **Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act** [online]. Privacy and Civil Liberties Oversight Board. 2014. 196p. Available at: <URL:

https://documents.pclob.gov/prod/Documents/OversightReport/823399ae-92ea-447a-ab60-0da28b555437/702-Report-2.pdf >.

MILDEBRATH, Hendrik – **The CJEU judgment in the *Schrems II* case** [online]. European Parliamentary Research Service. 2020. [accessed: 16 April 2022]. Available at: <URL: https://www.europarl.europa.eu/RegData/etudes/ATAG/2020/652073/EPRS_ATA(2020)652073_EN.pdf>.

PRIVACY INTERNATIONAL – **The Right to Privacy in Sweden** [online]. Human Rights Committee 116th Session. 2016. p.4. [accessed: 10 July 2022]. Available at: <URL: https://privacyinternational.org/sites/default/files/2017-12/HRC_Sweden_0.pdf >.

Addresses, statements, opinions

ARTICLE 29 WORKING PARTY (Art. 29 WP) – **EU – U.S. Privacy Shield – First annual Joint Review** [online]. 20 Nov. 2017. [accessed: 15 June 2022]. Available at: <URL: https://iapp.org/media/pdf/resource_center/Privacy_Shield_Report-WP29pdf.pdf>.

MONACO, Lisa O., INGLIS, John Chris, LITT, Robert S. – **Joint Statement at a hearing concerning "FISA Amendments Act Reauthorization"** [online]. 8 Dec. 2011. [accessed: 05 June 2022]. Available at: <URL: https://www.dni.gov/files/documents/Joint%20Statement%20FAA%20Reauthorization%20Hearing%20-%20December%202011.pdf>.

MUKASEY, Michael B. – **Classified certification of the Attorney General of the United States** [online]. 19 Sept 2008 (declassified 5 May 2014). MDL Dkt. No. 06-1791-VRW. [accessed: 01 June 2022]. Available at: <URL: https://www.dni.gov/files/documents/0505/AG%20Mukasey%202008%20Declassified%20Declaration.pdf>.

REDING, Viviane – **Speech – Mass surveillance is unacceptable – U.S. action to restore trust is needed now** [online]. European Parliament: Civil Liberties Committee hearing on Data Protection and U.S. Surveillance. Speech/13/1048. 9 December 2013. [accessed: 17 July 2022]. Available at: <URL: https://ec.europa.eu/commission/presscorner/detail/es/SPEECH_13_1048>.

THE WHITE HOUSE PRESIDENT GEORGE W. BUSH – **President's Radio Address** [online]. White House Radio. 17 December 2005. [accessed: 01 June 2022]. Available at: <URL: https://georgewbush-whitehouse.archives.gov/news/releases/2005/12/20051217.html>.

WAINSTEIN, Kenneth L. – **Statement of Kenneth L. Wainstein Assistant Attorney General** [online]. United States Senate: Select Committee on Intelligence, 1 May 2007, pp. 6-7. [accessed: 01 June 2022]. Available at: <URL: https://www.justice.gov/sites/default/files/nsd/legacy/2014/07/23/WainsteinTestimony5-01-07SSCI.pdf>.

EDPS – **Opinion 4/2016 on the EU-U.S. Privacy Shield draft adequacy decision** [online]. 30 May 2016. [accessed: 15 June 2022]. Available at: <URL: https://edps.europa.eu/sites/edp/files/publication/16-05-30_privacy_shield_en.pdf>.

Official Websites

ACADÉMIE DU RENSEIGMENT – **Les services spécialisés de renseignement** [online]. [accessed: 09 July 2022]. Available at: <URL: http://www.academie-renseignement.gouv.fr/services.html>.

ASSEMBLÉÉ NATIONALE – Commission de la défense nationale et des forces armées, Comptes-rendus n° 52, 54, 55, 56, 59 et 62 des réunions du 12 février, 13 février, 19 février, 20 février, 26 février et 13 mars 2013. Available at: <URL: https://www.assemblee-nationale.fr/14/cr-cdef/12-13/index.asp>.

CONGRESS.GOV. – **H.R. 6304 – 110th Congress (2007-2008)** [online]. Library of Congress, 2008. [accessed: 29 May 2022]. Available at: <URL: https://www.congress.gov/bill/110th-congress/house-bill/630>.

CONSEIL D'ETAT – **Connection data: the Council of State conciliates the implementation of European Union law and the effectiveness of the fight against terrorism** [online]. 21 April 2022. [accessed: 19 August 2022]. Available at: <URL: https://www.conseil-etat.fr/en/news/connection-data-the-council-of-state-conciliates-the-implementation-of-european-union-law-and-the-effectiveness-of-the-fight-against-terrorism-and>.

CONSEIL D'ETAT – **Les missions du Conseil d'État** [online]. [accessed: 06 July 2022]. Available at: <URL: https://www.conseil-etat.fr/qui-sommes-nous/le-conseil-d-etat/missions>.

COUNCIL OF THE EUROPEAN UNION – **Préparation du trilogue** [online]. 2017/0003 (COD). 28 March 2022. p.17. [accessed: 17 July 2022]. Available at: <URL:https://data.consilium.europa.eu/doc/document/ST-7458-2022-INIT/x/pdf >.

EDPB – **Statement 01/2022 on the announcement of an agreement in principle on a new Trans-Atlantic Data Privacy Framework** [online]. 6 April 2022. [accessed: 28 June 2022]. Available at: <URL: https://edpb.europa.eu/system/files/2022-04/edpb_statement_202201_new_trans-atlantic_data_privacy_framework_en.pdf>.

EUROPEAN COMMISSION – **European Commission and United States Joint Statement on Trans-Atlantic Data Privacy Framework** [online]. Brussels: Press release, 20 March 2022. [accessed: 27 June 2022]. Available at: <URL: https://ec.europa.eu/commission/presscorner/detail/en/ip_22_2087>.

EUROPEAN COMMISSION – **Trans-Atlantic Data Privacy Framewor**k [online]. Brussels: Factsheet, 25 March 20222. [accessed: 27 June 2022]. Available at: <URL: https://ec.europa.eu/commission/presscorner/detail/en/FS_22_2100>.

EUROPEAN COMMISSION – **Why do we need the Charter? The Charter of Fundamental Rights, what it covers and how it related to the European Convention on Human Rights** [online]. [accessed: 14 June 2022]. Available at: <URL: https://ec.europa.eu/info/aid-development-cooperation-fundamental-rights/your-rights-eu/eu-charter-fundamental-rights/why-do-we-need-charter_en>.

EUROPEAN DATA PROTECTION SUPERVISOR – **About** [online]. [accessed: 15 June 2022]. Available at: <URL: https://edps.europa.eu/about-edps_en>.

EUROPEAN DATA PROTECTION SUPERVISOR (EDPS) – **About** [online]. [accessed: 15 June 2022]. Available at: <URL: https://edps.europa.eu/about-edps_en>.

NSA, CSS – **NSA Stops Certain Section 702 "Upstream" Activities** [online]. Press Release. 28 April 2017. [accessed: 17 June 2022]. Available at: <URL: https://www.nsa.gov/Press-Room/Press-Releases-Statements/Press-Release-View/Article/1618699/nsa-stops-certain-section-702-upstream-activities/>.

OFFICE OF THE ATTORNEY GENERAL – **California Consumer Privacy Act (CCPA). Factsheet** [online]. [accessed: 06 September 2022]. Available at: <URL: https://www.oag.ca.gov/system/files/attachments/press_releases/CCPA%20Fact%20Sheet%20%2800000002%29.pdf>.

OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE - **DNI Announces the Declassification of the Existence of Collection Activities Authorized by President George W. Bush Shortly After the Attacks of September 11, 2001** [online]. 21 December 2013. [accessed: 01 June 2022]. Available at: <URL: https://icontherecord.tumblr.com/post/70683717031/today-the-director-of-national-intelligence>.

SAVAGE, Charlie – **Power Wars document: Transit Authority and the 1990 Lawton surveillance memo** [online]. 18 November 2015. [accessed: 11 June 2022]. Available at: <URL: https://charliesavage.com/2015/11/power-wars-document-transit-authority-and-the-1990-lawton-surveillance-memo/>.

THE WORLD BANK – GDP (current US$) – **European Union, United States, China** [online]. World Bank national accounts data, and OECD National Accounts data files. [accessed: 19 April 2022]. Available at: < URL: https://data.worldbank.org/indicator/NY.GDP.MKTP.CD?locations=EU-US-CN>.

UNITED STATES FOREIGN INTELLIGENCE COURT – **About the Foreign Intelligence Surveillance Court** [online]. [accessed: 08 July 2022]. Available at: <URL: https://www.fisc.uscourts.gov/about-foreign-intelligence-surveillance-court>.

News articles and other websites

ALEXANDRU, Valentina – **What France's reaction to the CJEU ruling on data retention could mean for the EU's future** [online]. European Studies Review. 17 March 2021. [accessed: 19 August 2022]. Available at: <URL: https://europeanstudiesreview.com/2021/03/17/what-frances-reaction-to-the-cjeu-ruling-on-data-retention-could-mean-for-the-eus-future>.

ARMINGAUD, Claude-Étienne, COMPARET Laure, SELOSSE Violaine – **EU Data Protection: standard contractual clauses may have been confirmed by the CJEU, but at what price?** [online]. K&L Gates. 17 July 2020. [accessed: 21 June 2022].

Available at: <URL: https://www.klgates.com/eu-data-protection-standard-contractual-clauses-may-have-been-confirmed-by-the-cjeu-but-at-what-price-07-17-2020>.

BALL James, BORGER Julian, GREENWALD Glenn – **Revealed: how US and UK spy agencies defeat interne privacy and security** [online]. The Guardian. 6 September 2013. [accessed: 1 July 2022]. Available at: <URL: https://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security>.

ÇALI, Başak – **Has "Control over rights doctrine" for extra-territorial jurisdiction come of age? Karlsruhe, too, has spoken, now it's Strasbourg's turn** [online]. EJIL:Talk!. 21 July 2020. [accessed: 12 July 2022]. Available at: <URL: https://www.ejiltalk.org/has-control-over-rights-doctrine-for-extra-territorial-jurisdiction-come-of-age-karlsruhe-too-has-spoken-now-its-strasbourgs-turn/>.

CHASE, Jefferson – **Merkel testifies on NSA spying affair** [online]. DW. 16 February 2017. [accessed: 17 June 2022]. Available at: <URL: https://p.dw.com/p/2XfPe>.

CHRISTAKIS, Theodore, PROPP, Kenneth – **How Europe's Intelligence Services Aim to Avoid the EU's Highest Court – and What It Means for the United States** [online]. Lawfare. 8 March 2021. [accessed: 17 July 2022]. Available at: <URL: https://www.lawfareblog.com/how-europes-intelligence-services-aim-avoid-eus-highest-court-and-what-it-means-united-states>.

CORNELL LAW SCHOOL – **Privacy** [online]. [accessed: 14 June 2022]. Available at: <URL: https://www.law.cornell.edu/wex/privacy>.

DEPRAU, Alexis – **Quelques précisions sur la surveillance des communications éléctroniques internationales** [online]. Le Blog de Droit Admnistratif. 06 July 2018. [accessed: 07 july 2022]. Available at: <URL: https://blogdroitadministratif.net/2018/07/06/quelques-precisions-sur-la-surveillance-des-communications-electroniques-internationales/>.

EUROSTAT – **Do you participate in social networks?** [online]. 2021. [accessed: 20 April 2022]. Available at: <URL: https://ec.europa.eu/eurostat/web/products-eurostat-news/-/edn-20210630-1>.

EUROSTAT – Internet usage. **Digital economy and society statistics – households and individuals** [online]. 2021. [accessed: 20 April 2022]. Available at: <URL: https://ec.europa.eu/eurostat/statistics-

explained/index.php?title=Digital_economy_and_society_statistics_-_households_and_individuals#Privacy_and_protection_of_personal_identity>.

FOLLOROU, Jacques – **Espionnage: comment Orange et les services secrets coopèrent** [online]. Le Monde. 20 March 2014. [accessed: 02 July 2022]. Available at: <URL: https://www.lemonde.fr/international/article/2014/03/20/dgse-orange-des-liaisons-incestueuses_4386264_3210.html>.

FOLLOROU, Jacques, JOHANNÈS Franck – **Révélations sur le Big Brother français** [online]. Le Monde. 04 July 2013. [acessed: 02 July 2022]. Available at: <URL: https://www.lemonde.fr/societe/article/2013/07/04/revelations-sur-le-big-brother-francais_3441631_3224.html>.

GELLMAN, Barton; POITRAS Laura – **U.S., British intelligence mining data from nine U.S. Internet companies in broad secret program** [online]. The Washington Post. 2013. [accessed: 29 April 2022]. Available at: <URL: https://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html>.

GREENWALD Glenn – **Xkeyscore: NSA tool collects 'nearly everything a user does on the internet'** [online]. The Guardian. 31 July 2013. [accessed: 19 May 2022]. Available at: <URL: https://www.theguardian.com/world/2013/jul/31/nsa-top-secret-program-online-data>.

GREENWALD, Glenn, MACASKILL, Ewen – **NSA Prism program taps in to user data of Apple, Google and others** [online]. The Guardian. 7 June 2013. [accessed: 29 April 2022]. Available at: <URL: https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data>.

ISMS.ONLINE – **ISO 27701 – The Standard for Privacy Information Management** [online]. [accessed: 26 June 2022]. Available at: <URL: https://www.isms.online/iso-27701/>

ISMS.ONLINE – **Understanding ISO 27001** [online]. [accessed: 26 June 2022]. Available at: < URL: https://www.isms.online/iso-27001/>.

KAYALI, Laura – **France seeks to bypass EU top court on data retention** [online]. Politico. 3 March 2021. [accessed: 19 August 2022]. Available at: <URL: https://www.politico.eu/article/france-data-retention-bypass-eu-top-court/>.

KREBS, David - **Global dangers and national obligations: Extraterritorial protection obligations in the Basic Law: The BND judgment and the debate about a "supply chain law"** [online]. Verfassungsblog. 4 July 2020. [accessed: 12 July 2022]. Available at: <URL: https://verfassungsblog.de/globale-gefahren-und-nationale-pflichten/>.

LEE, Timothy B. – **Report: NSA asked Verizon for records of all calls in the U.S.** [online]. The Washington Post. 5 June 2013. [accessed: 29 April 2022]. Available at: <URL: https://www.washingtonpost.com/news/wonk/wp/2013/06/05/nsa-asked-verizon-for-records-of-all-calls-in-the-u-s/ >.

MACASKILL, Ewen, DANCE, Gabriel – **NSA Files: Decoded. What the revelations mean for you** [online]. The Guardian. 1 November 2013. [accessed: 26 April 2022]. Available at: <URL: https://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded#doc/3>.

MILLER, Russel A. – **The German Constitutional Court Nixes Foreign Surveillance** [online]. Lawfare. 27 May 2020. [accessed: 12 July 2022]. Available at: <URL: https://www.lawfareblog.com/german-constitutional-court-nixes-foreign-surveillance>.

PETROLI, Mallory – **New Standard Contractual Clauses Under the GDPR** [online]. The National Law Review. 9 August 2021. [accessed: 21 June 2022]. Available at: <URL: https://www.natlawreview.com/article/new-standard-contractual-clauses-under-gdpr>.

RISEN, James, LICHTBLAU, Eric – **Bush Lets U.S. Spy on Callers Without Courts** [online]. The New York Times. 16. Dec. 2005. [accessed: 01 June 2022]. Available at: <URL: https://www.nytimes.com/2005/12/16/politics/bush-lets-us-spy-on-callers-without-courts.html>.

SAJFERT, Juraj – **Bulk data interception/retention judgements of the CJEU – A victory and a defeat for privacy** [online]. European Law Blog. 26 October 2020. [accessed: 11 July 2020]. Available at: <URL:

https://europeanlawblog.eu/2020/10/26/bulk-data-interception-retention-judgments-of-the-cjeu-a-victory-and-a-defeat-for-privacy/>.

SCHREMS, Max – **"Privacy Shield 2.0"? – First Reaction by Max Schrems"** [online]. Noyb. 25 March 2022. [accessed: 27 June 2022]. Available at: <URL: https://noyb.eu/en/privacy-shield-20-first-reaction-max-schrems>.

SCHREMS, Max – **Open Letter on the Future of EU-US Data Transfers** [online]. Noyb. 23 May 2022. [accessed: 27 June 2022]. Available at: <URL: https://noyb.eu/en/open-letter-future-eu-us-data-transfers>.

SEIBT, Sébastien – **How Denmark became the NSA's listening post in Europe** [online]. France 24. 01 June 2021. [accessed: 17 July 2022]. Available at: <URL: https://www.france24.com/en/technology/20210601-how-denmark-became-the-nsa-s-listening-post-in-europe>.

TAYLORWESSING – **Transfer Impact Assessment Tool (TIA tool)** [online]. [accessed: 27 June, 2022]. Available at: <URL: https://www.taylorwessing.com/en/campaigns/de/transfer-impact-assessment-tool>.

THE GUARDIAN – **Verizon forced to hand over telephone data – full court ruling** [online]. 6 June 2013. [accessed: 29 April 2022]. Available at: <URL: https://www.theguardian.com/world/interactive/2013/jun/06/verizon-telephone-data-court-order>.

GREENWALD, Glenn – **NSA collecting phone records of millions of Verizon customers daily** [online]. The Guardian. 6 June 2013. [accessed: 29 April 2022]. Available at: <URL: https://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order>.

THE GUARDIAN – **XKeyscore presentation from 2008 – read in full** [online]. 31 July 2013. [accessed: 19 May 2022]. Available at: <URL: https://www.theguardian.com/world/interactive/2013/jul/31/nsa-xkeyscore-program-full-presentation>.

VIE PUBLIQUE – **Renseignement français: quelle organisation et quel cadre légal?** [online]. 13 May 2022. [accessed: 02 July 2022]. Available at: <URL: https://www.vie-publique.fr/eclairage/272339-renseignement-francais-quel-cadre-legal>.

VON DEM BUSSCHE, Axel Frhr., VOIGT, Paul, SCHMALENBERGER, Alexander – **Trans-Atlantic Data Privacy Framework (TADPF) - the road ahead** [online]. TaylorWessing. 4 April 2022. [accessed: 28 June 2022]. Available at: <URL: https://www.taylorwessing.com/en/insights-and-events/insights/2022/04/trans-atlantic-data-privacy-framework---the-road-ahead>.