



**RIGA
GRADUATE
SCHOOL OF
LAW**

Right to private life under the scope of mass surveillance: differences in approaches to the implementation of the principle of proportionality in the jurisprudence of the CJEU and the ECtHR

BACHELOR THESIS

AUTHOR:

Valērija Ruta Hartmane
LL.D. 2020/2021 year student
student number B020010

SUPERVISOR:

Julia Emtseva

LL.M.

DECLARATION OF HONOUR:

I declare that this thesis is my own work, and that all references to, or quotations from, the work of others are fully and correctly cited.

(Signed)

ABSTRACT

Mass surveillance in a digital age prompts a new domain of challenge in the balancing act of the interest of national security and the right to privacy. The Thesis examines the clash between national security imperatives and the right to privacy by employing mainly a comparative approach. The author establishes the following research question: what are the approaches on implementing a principle of proportionality of the ECtHR in the case of Big Brother Watch and the CJEU in the case of Schrems I and Schrems II?

The examination of landmark cases illuminates the need for safeguarding measures and a proactive approach to privacy protection. The main prerequisites for finding the balance between respective interests, *inter alia*, intervention with one's privacy shall be strictly necessary and safeguarded on all levels by adequate mechanisms.

Keywords: mass surveillance; right to privacy; Schrems I; Schrems II; Big Brother Watch case; the principle of proportionality.

SUMMARY

The first chapter “Concept of Private Life in Realm of Mass Surveillance” explores notions of mass surveillance and private life and their consequent interplay. It establishes that mass surveillance mainly concerns national security interests that largely intervene with one’s right to private life. The notion of privacy shall be seen as an umbrella concept also encompassing such narrative as personal data. The author in the respective chapter establishes the concept of tradeoff, namely, the need for a balancing act for a fair trade of interests. Consequently highlighting the importance of trust, particularly in the matter of the public sector’s intervention with one’s privacy. The first chapter also includes a description of a regulatory landscape of both concepts, mainly, drawing an emphasis on Article 8 of the ECHR and Article 7 and Article 8 of the EUCFR, outlining the necessity to employ the principle of proportionality.

The second chapter “Analysis of the CJEU judgment in Schrems I and Schrems II cases” examines the CJEU approach applying the principle of proportionality in two landmark cases – Schrems I and Schrems II. Both cases concern data transfer from the EU to the US and the issue of a possible intervention with the EU citizens’ personal data due to the US mass surveillance activities highlighted by Snowden’s revelations. Analysis of cases highlighted the need for an adequate level of safeguarding measures for privacy protection, emphasizing that mass surveillance can be exercised only when strictly necessary. Furthermore, emphasizes the need for a clear and precise regulatory framework. The implications of judgments outlined: (1) the need for pro-active regulatory intervention to safeguard the right to privacy in a rapidly advancing technological era; (2) practical burdens faced by the commercial activity holders in the absence of a unified regulatory framework governing personal data transfers; (3) international relations importance in safeguarding the right to privacy outside one’s jurisdiction.

The third chapter “Analysis of the ECtHR judgment Big Brother Watch and Others v. the UK” covers the analogous analysis to one exercised in the second chapter with an aim to observe similarities and differences in the courts’ approaches in the implementation of the principle of proportionality. Moreover, it provides a subsequent comparison outlining interesting novelties that can be observed via the ECtHR judgment. Consequently highlights the main prerequisites employed by the principle of proportionality to reach a balance between the interest of national security and privacy. The author outlines the main respective requirements for such action (non-exclusive list): (1) interference shall be exercised in accordance with law; (2) it shall possess a legitimate aim; (3) it shall be strictly necessary; (4) parties involved in data transfers shall ensure an adequate level of safeguard; (5) process of mass surveillance shall be foreseeable; (6) when possible less intrusive measures shall be placed.

Overall, the Thesis is comprised of three primary chapters, along with thirteen sub-chapters and three tertiary sub-chapters. The overarching aim of the Thesis is to explore the principle of proportionality, specifically focusing on achieving equilibrium between the imperatives of national security and the preservation of the right to privacy.

TABLE OF CONTENTS

Summary.....	I
Table of Contents	II
List of Acronyms and Abbreviations.....	IV
Introduction	1
1. Concept of private life in realm of mass surveillance	4
1.1. Notions of mass surveillance and privacy	4
1.2. Governing mass surveillance and privacy	7
1.3. Finding balance between interests under mass surveillance and one’s right to privacy. 12	
1.3.1. Pro-surveillance camp	13
1.3.2. Pro-privacy camp.....	14
1.3.3. Tradeoffs – balancing interests.....	15
2. Analysis of the CJEU judgement in Schrems I and Schrems II cases.....	19
2.1. Facts of the Schrems I case.....	19
2.2. CJEU approach in Schrems I – finding proportionality	22
2.3. Implications of the Schrems I	27
2.4. Facts of the Schrems II case	29
2.5. CJEU approach in Schrems II – finding proportionality	30
2.6. Implications of the Schrems II.....	35
3. Analysis of the ECtHR judgment Big Brother Watch and Others v. the UK	38
3.1. Facts of the Big Brother Watch case	38
3.2. ECtHR approach in Big Brother Watch – finding proportionality	39
3.3. Implications of the Big Brother Watch case	45
3.4. Comparison of the CJEU and ECtHR approaches.....	46
Conclusion	48
Bibliography	52
Annex 1. General Data Protection Regulation	66
Annex 2. Charter of Fundamental Rights of the European Union	68
Annex 3. European Convention on Human Rights	69
Annex 4. International Covenant on Civil and Political Rights	70
Annex 5. Universal Declaration of Human Rights.....	71
Annex 6. Infographic - Terrorism in the EU	72
Annex 7. Banksy mural “One Nation Under CCTV”	73
Annex 8. PRISM/US-984XN Overview	74
Annex 9. Treaty of the Functioning of the European Union	80

Annex 10. Directive 95/46/EC	81
Annex 11. Safe Harbor decision.....	83
Annex 12. The Foreign Intelligence Surveillance Act of 1978.....	85
Annex 13. Standard Contractual Clauses decision.....	94
Annex 14. Schrems II preliminary questions	95
Annex 15. Privacy Shield decision.....	97
Annex 16. Regulation of Investigatory Powers Act 2000	99

LIST OF ACRONYMS AND ABBREVIATIONS

Big Brother Watch	The European Court of Human Rights (Grand Chamber). Big Brother Watch and Others v. the United Kingdom, nos. 58170/13, 62322/14 and 24960/15, 25 May 2021.
CCTV	Closed-circuit television
CIA	Central Intelligence Agency
CJEU	Court of Justice of the European Union
CSPs	Communications service providers
Directive 95/46/EC	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, 281 OJ L § (1995)
DMA	Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act) (Text with EEA relevance), 265 OJ L § (2022)
DPC	Irish Data Protection Commissioner
DSA	Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act) (Text with EEA relevance), 277 OJ L § (2022)
E.O. 12333	Executive Order 12333 United States Intelligence Activities
ECHR	Convention for the Protection of Human Rights and Fundamental Freedoms (1950) (European Convention on Human Rights)
ECtHR	European Court of Human Rights
EDPB	European Data Protection Board
EDPS	European Data Protection Supervisor
EU	The European Union
EUCFR	Charter of the Fundamental Rights of the European Union
EUDPA	European Data Protection Authorities
EUIPO	The European Union Intellectual Property Office
FBI	Federal Bureau of Investigation
FISA	The Foreign Intelligence Surveillance Act
GA	The United Nations General Assembly
GCHQ	Government Communications Headquarters

GDPR	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) (Text with EEA Relevance)
HIPPA	Health Insurance Portability and Accountability Act of the United States
IC Code	Interception of Communications Code of Practice
ICCPR	International Covenant on Civil and Political Rights
IPA	The Investigatory Powers Act 2016
IPT	The Investigatory Powers Tribunal
NSA	The United States National Security Agency
OECD	The Organisation for Economic Cooperation and Development
OHCHR	Office of the United Nations High Commissioner for Human Rights
PPD-28	Presidential Policy Directive 28 (“PPD- 28”), issued on 17 January 2014 (used in the context of Schrems II case)
Privacy Shield decision	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 (notified under document C(2016) 4176) (Text with EEA relevance), 207 OJ L § (2016)
Safe Harbour decision	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 and related frequently asked questions issued by the US Department of Commerce (notified under document number C(2000) 2441) (Text with EEA relevance.), 215 OJ L § (2000)
SCC	Standard Contractual Clauses
SCC decision	2010/87/: 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 (notified under document C(2010) 593) (Text with EEA relevance), 039 OJ L § (2010)
Schrems I	CJEU judgement C- 362/14 - Maximillian Schrems v. Data Protection Commissioner & Digital Rights Ireland Ltd
Schrems II	CJEU judgement C-311/18 - Data Protection Commissioner v. Facebook Ireland Limited and Maximillian Schrems
TEU	Treaty on European Union
TFEU	Treaty on the Functioning of the European Union
UDHR	Universal Declaration of Human Rights

UK The United Kingdom
UN United Nations
US The United States of America

INTRODUCTION

Snowden's revelations in 2013, exposing public authorities' abuse of a right to privacy on a large scale through extensive mass surveillance activities, constituted a fundament for a digital age's battle between the imperative of national security and the fundamental right to privacy. Moreover, the increase in terrorist attacks in Europe during the 2000s and current Europe's exposure to significant geopolitical security threats, such as Russia's aggression escalating into an act of war in Ukraine, have further intensified the tension surrounding the impetus to enhance national security. Hence, increasing the probability of violating the paramount human right – right to privacy.

Alongside clash of the security and privacy interests, it is important to acknowledge the transformative impact of technological advancements on the concept of privacy. In particular, such progress has propelled the emergence of personal data as a pivotal aspect within the realm of privacy. The personal data is now being actively utilized as an asset to drive financial gains in both private and public sectors. Such activity particularly is evident in a trans-Atlantic data transfers among the EU and the US. Hence, a bilateral dilemma among the interest of national security and privacy incorporates commercial activity holders. Consequent emergence of multiparty relationship increases the need of a clear and synergetic regulatory approach. Thus, the main legal problem lies in the application of the principle of proportionality to strike a balance between national security, privacy rights, and commercial interests, thereby aiming to effectively safeguard personal data.

The author applied a doctrinal research method. When analyzing legal provisions governing mass surveillance and privacy, primarily, Article 8 of the ECHR and Article 7 and Article 8 of the EUCFR, analytical approach was applied via the textual interpretation method to outline the literal meaning of the norms and the teleological interpretation method to underline the aim of the norms. In the spectrum of the non-doctrinal method, the author for interpretation of the norms applied analytical approach to underline mass surveillance's impact on the notion of private life. Moreover, employing analytical approach by analyzing the implications of the ECtHR and CJEU judgments in such realms as political, economic, and others.

Under the paradigm of the doctrinal research method, the author applied a comparative approach by analyzing the ECtHR Grand Chamber's judgment in the case of *Big Brother Watch and Others v. the UK* and the CJEU judgments in the cases of *Maximillian Schrems v. Data Protection Commissioner & Digital Rights Ireland Ltd* and *Data Protection Commissioner v. Facebook Ireland Limited and Maximillian Schrems*. Upon outlining various hurdles faced within the relationship involving mass surveillance and privacy, the author seeks to explore how disputes arising from mass surveillance infringements are seen before courts. Specifically, viewing courts' practices in the matter of balancing the needs of mass surveillance and privacy, namely, viewing the approach on the application of the proportionality principle and analyzing both courts' outlooks on the inherent legitimacy of mass surveillance.

To establish a framework for comparison, the author outlines similarities and differences between named cases. All three precedents are regarded as landmark cases in personal data regulation and are based on Snowden's revelations. *Schrems I* and *Schrems II* cases are based on

a preliminary rulings which concerned the assessment of whether the US ensured an adequate level of safeguard for the right to privacy under the Safe Harbor decision and Privacy Shield decision respectively, both with an aim to regulate EU-US personal data transfers. The cases of Schrems I and Schrems II are intricately interconnected, thereby analyzed in close proximity to establish more in-depth analysis. The Big Brother Watch case similarly assessed the UK's domestic mass surveillance regulatory landscape's adequacy to safeguard one's privacy once such activities are conducted. The major difference is the judicial body overseeing the proceedings, namely, the CJEU and the ECtHR. Nevertheless, the aforementioned distinction does not possess the gravity of significance to override factual equivalence. Moreover, the author deliberately chose to compare two different court approaches in order to establish a more impartial and encompassing evaluation of the necessary approach when applying the principle of proportionality. Moreover, the comparative approach was applied when analyzing the European Union's legal spectrum and the European Council's legal landscape and the consequent implications of the judgments.

Upon the expressed, the author in this Thesis put forward following research question: what are the approaches on implementing a principle of proportionality of the ECtHR in the case of Big Brother Watch and the CJEU in the case of Schrems I and Schrems II? Thus, the main aim of the Thesis is to establish what are the prerequisites of finding the balance between the interest of national security and of safeguard of a right to privacy. Subsequently reaching such objectives as: firstly, establishing what are the interest of each subject that should be balanced, secondly, examining regulatory landscape of the governance of such relationship, thirdly, observing courts' approaches employing the principle of proportionality in order to draw the main prerequisites of a fair balance.

As the Thesis concerns various issues, the author draws following limitations. Regarding mass surveillance regulations, the author does not describe or review any specific national regulations on mass surveillance that would go outside the scope of the cases analyzed. As mass surveillance amounts to a matter of national security there is no unified approach, hence, every practice should be assessed on a case-by-case basis.

Additionally, it must be noted that mass surveillance, also endangers other human rights and freedoms, such as freedom of information and expression and the right to a fair trial and freedom of religion, the right not to be discriminated and others. Furthermore, narrowing the umbrella notion of privacy specifically to the notion of personal data. Regarding an assessment of the right to privacy, the author views Article 8 of the ECHR and Article 7, and Article 8 of the EUCFR.

Furthermore, the author establishes Schrems I, Schrems II, and Big Brother Watch case analysis limitations. The author will put focus on the courts application of the principle of proportionality. No other aspects neither substantive nor procedural matters will be thoroughly examined.

The Thesis consists of three main chapters. The first chapter consists of three sub-chapters and three third-level sub-chapters where the author explores the concepts of mass surveillance and privacy and their consequent interplay. Furthermore, the author establishes a governing framework of such notions. The first chapter also provides a description of the main arguments of both interest

advocates introducing a concept of a tradeoff of interest which mirrors the concept of a balancing act under proportionality. Thus, outlining the main loopholes and barriers faced within such a task.

The second chapter consists of six sub-chapters as it involves the analysis of the Schrems I and Schrems II cases. The author at the beginning of the second chapter describes the grassroots event applicable to all cases analyzed – Snowden’s revelations. Consequently proceeding with an analysis of the Schrems I case and its implications mirroring such an approach also for the examination of the Schrems II case.

The third chapter consists of four sub-chapters with the main aim to analyze the Big Brother Watch case, simultaneously, regarding similar matters addressed in the Schrems I or Schrems II, the author provides a comparison. Nevertheless, for a more comprehensive outlook on the employed approaches of both courts, the author under the last sub-chapter provides a more thorough comparison.

1. CONCEPT OF PRIVATE LIFE IN REALM OF MASS SURVEILLANCE

To lay foundations for subsequent examination of the Schrems I, Schrems II and Big Brother Watch cases, the author primarily explores the concepts of private life and mass surveillance. These notions are interlinked, as the act of mass surveillance, which is commonly referred to as a bulk interception, constitutes a significant intrusion into an individual's private life. It is crucial to distinguish the key pillars of each concept in order to gain a more nuanced understanding of their respective implications in such synergetic relationship. The delicate balance between national security imperatives using mass surveillance and the protection of individuals' right to privacy presents a formidable challenge, requiring careful consideration of the competing interests at stake.

1.1. Notions of mass surveillance and privacy

Mass surveillance is an action usually exercised within the interest of national security which includes monitoring of internet and telecommunications in a large scale without sufficient grounds of any wrongdoing.¹ The tools used for such interception have grown alongside the technological advancement and digitalization, enabling governments to surveil individuals or collectives on a larger, more comprehensive level.² Such surveillance instruments include *inter alia*:

- 1) bulk data interception, which concerns both physical data storage units, such as hard drives and cloud storage units;
- 2) Internet Communication Technology surveillance, which detects the data movement on social media platforms and in communication platforms, for example, in WhatsApp;
- 3) geo-location and remote sensing, which analyses data that is gathered via global positioning system (GPS), including also surveillance cameras and satellite data;
- 4) biometrics, which uses unique personal information of an individual, for example, fingerprint or facial recognition;
- 5) Internet of Things, which comprises modern household technology, for example, home assistant Alexa or smart fridges; home safety and alarm systems;

¹ Mass surveillance is not officially defined as a specific term in any international treaties, as primarily it is to be defined on a national level. For a more detailed explanation, please, refer to the definition provided by Privacy International – a well-respected NGO advocating specifically for the right to private life in the intersection of modern-day technologies – which states that: “Mass surveillance uses systems or technologies that collect, analyze, and/or generate data on indefinite or large numbers of people instead of limiting surveillance to individuals about which there is reasonable suspicion of wrongdoing, (...) governments can capture virtually all aspects of our lives.” See Amnesty International. “Easy Guide to Mass Surveillance,” March 18, 2015. Available on: <https://www.amnesty.org/en/latest/campaigns/2015/03/easy-guide-to-mass-surveillance/>. Accessed April 10, 2023. It also must be noted that the definition of national security varies for each state, for example, in the ECtHR case of *Liberty and Others v. United Kingdom*, the ECtHR analyzing domestic applicable law, also drew attention to the definition of national security (activities) as stated in the *Interception of Communications Act 1985*: “which threaten the safety or well-being of the State, and which are intended to undermine or overthrow Parliamentary democracy by political, industrial or violent means.” See *Liberty and Others v. the United Kingdom*, No. 58243/00 (ECtHR July 1, 2008), §27.

² Stephen Graham and David Wood, “Digitizing Surveillance: Categorization, Space, Inequality,” *Critical Social Policy* 23, no. 2 (May 1, 2003): 228, <https://doi.org/10.1177/0261018303023002006>.

6) telecommunication wiring, which intercepts, for example, incoming and outgoing calls.³

Mass surveillance, especially in the digital era has become a controversial and polarizing issue due to concerns over privacy, civil liberties, and government overreach⁴ and lack of consensus and clarity regarding the legitimacy of mass surveillance.⁵ Thus, two camps of thought emerge⁶ - some argue that mass surveillance is necessary to prevent terrorism and other threats to national security,⁷ whilst others argue that it violates basic human rights (mainly right to privacy)⁸ and can be abused by governments for political purposes.⁹

The task of offering a clear and concise definition of privacy is complicated by its intricate and multifaceted nature, as well as its integration across a diverse range of disciplines such as sociology, politics, law, and economics.¹⁰ Moreover, the challenge becomes more difficult when distinguishing what is public and what is private on Internet, as characterized by the professor Gary T. Marx “murky conceptual waters.”¹¹ The concept of privacy is an umbrella term that encompasses various notions, *inter alia*, environmental issues,¹² surveillance,¹³ reputation,¹⁴ and

³ H. Akın Ünver, “Politics of Digital Surveillance, National Security and Privacy” (Centre for Economics and Foreign Policy Studies, 2018), <https://www.jstor.org/stable/resrep17009>; Nuala O’Connor, Alethea Lange, and Ali Lange, “Privacy in the Digital Age,” *Great Decisions*, 2015, 20, <https://www.jstor.org/stable/44214790>.

⁴ Graham and Wood, “Digitizing Surveillance.”

⁵ Anthony Dworkin, “Surveillance, Privacy, and Security: Europe’s Confused Response to Snowden” (European Council on Foreign Relations, 2015), 1, <https://www.jstor.org/stable/resrep21543>.

⁶ Of course, there are also those in academia and in practice who take the middle way – advocate for the balance of both interests, See Chapter “Tradeoffs – balancing interests.”

⁷ Ross Anderson, “Surveillance or Privacy?,” in *Security Engineering* (John Wiley & Sons, Ltd, 2020), 909–63, <https://doi.org/10.1002/9781119644682.ch26>; Barton Gellman, “NSA Broke Privacy Rules Thousands of Times per Year, Audit Finds,” *Washington Post*, August 15, 2013, sec. National Security. Available on: https://www.washingtonpost.com/world/national-security/nsa-broke-privacy-rules-thousands-of-times-per-year-audit-finds/2013/08/15/3310e554-05ca-11e3-a07f-49ddc7417125_story.html. Accessed April 10, 2023.

⁸ As the ECtHR put it in the case of Big Brothers Watch: “[E]ven the mere storing of data relating to the private life of an individual amount to an interference within the meaning of Article 8.” See case Big Brother Watch and Others v. the United Kingdom, No. 58170/13, 62322/14, 24960/15 (ECtHR [GC] May 25, 2021), §330.

⁹ David Lyon, “Surveillance, Snowden, and Big Data: Capacities, Consequences, Critique,” *Big Data and Society* 1, no. 2 (2014), <https://doi.org/10.1177/2053951714541861>; David Lyon, “Surveillance Culture: Engagement, Exposure, and Ethics in Digital Modernity,” 2017; Mark Andrejevic, “Big Data, Big Questions| The Big Data Divide,” *International Journal of Communication* 8, no. 0 (June 16, 2014): 17, <https://ijoc.org/index.php/ijoc/article/view/2161>. See Chapter “Tradeoffs – balancing interests.”

¹⁰ Kobbi Nissim and Alexandra Wood, “Is Privacy Privacy?,” *Philosophical Transactions: Mathematical, Physical and Engineering Sciences* 376, no. 2128 (2018): 3, <https://www.jstor.org/stable/26601760>; Helen Nissenbaum, *Privacy in Context: Technology, Policy, and the Integrity of Social Life* (Stanford: Stanford University Press, 2009), <http://www.sup.org/books/title/?id=8862>.

¹¹ This is especially evident in the case of profiling involving data mining activities, for example, for the establishment of a database, usually, also commonly employed during mass surveillance Gary T. Marx, “Murky Conceptual Waters: The Public and the Private,” *Ethics and Information Technology* 3, no. 3 (September 1, 2001): 157–69, <https://doi.org/10.1023/A:1012456832336>; Shraddha Kulhari, “Data Protection, Privacy and Identity: A Complex Triad,” in *Building-Blocks of a Data Protection Revolution*, 1st ed., The Uneasy Case for Blockchain Technology to Secure Privacy and Identity (Nomos Verlagsgesellschaft mbH, 2018), 27, <https://www.jstor.org/stable/j.ctv941qz6.7>.

¹² See case Hatton and Others v. the United Kingdom [GC], which refers to the quality of the environmental surroundings of an individual that might be harmful to one’s wellbeing, is perceived by the ECtHR as impacting that individual’s private life. Hatton and Others v. the United Kingdom, No. 36022/97 (ECtHR [GC] July 8, 2003), §96.

¹³ See case Szabó and Vissy v. Hungary, also referring to an issue of mass surveillance as being in a violation of a right to private life. Szabó and Vissy v. Hungary, No. 37138/14 (ECtHR January 12, 2016), §52.

¹⁴ See cases Axel Springer Ag v. Germany, No. 39954/08 (ECtHR [GC] February 7, 2012); Bédat v. Switzerland, No. 56925/08 (ECtHR [GC] March 29, 2016).

many other.¹⁵ Thus, for example, ECtHR acknowledges as the right to private life is impossible to define its relevance in specific context shall be analyzed.¹⁶

Due to its broad scope, privacy can be perceived both as a fundamental right and a fundamental freedom.¹⁷ Primarily, privacy is categorized as a right, which is a legally acknowledged entitlement that provides individuals with specific benefits, such as safeguarding their physical and social integrity and identity¹⁸ via abstaining from an unlawful interference with their personal and family life, their home and correspondence.¹⁹ However, it can also be perceived as a freedom, if narrowed to a precise perspective in the context of mass surveillance, it would be a freedom from an unreasonable search.²⁰ The author encourages to adopt a broader perspective on the concept of privacy, especially when dealing with mass surveillance, given the existence of various privacy-related domains that could be affected. Specifically, avoiding a narrow interpretation of privacy, for instance, limiting it to the right to avoid surveillance in the workplace. The author further will focus on personal data as a sub-field of privacy, given its critical importance in the context of mass surveillance activities. By considering personal data as the minimum scope of privacy, the author seeks to illuminate the significant privacy risks that arise from the interception and use of such data, which is also the key spectrum in the case analysis provided further.²¹

Before outlining regulatory approaches on mass surveillance and privacy, one shall understand notions associated to the activities of data gathering which consequently intervene with one's personal data. The foundational notions - personal data and processing of data – former being a data set that is attributable to the specific individual and thus can be used to identified that specific individual;²² later standing for an activity that uses such personal data, for example, collecting,

¹⁵ The struggle of defining privacy or putting it in a standardized box has been also highlighted by the ECtHR case law. For example, privacy under Article 8 of the ECHR can refer to, for instance, same-sex partnership matters as in the recent case of *Fedotova and Others v. Russia*, where the ECtHR noted that private life:” is a broad concept that does not lend itself to the exhaustive definition and encompasses the right to personal development,” or it can also concern data collection of employees use of the telephone as in the case of *Mazur v. the Republic of Moldova and Russia*. See cases *Fedotova and Others v. Russia*, No. 40792/10, 30538/14, 43439/14 (ECtHR [GC] January 17, 2023); *Mozer v. the Republic of Moldova and Russia*, No. 11138/10 (ECtHR [GC] February 23, 2016).

¹⁶ The ECtHR made such an observation in the case *Niemietz v. Germany*, which concerned a lawyer who complained that a search of his office, whilst criminal proceedings were pending, interfered with his private life. The European Court of Human Rights (Second Section Committee). *Niemietz v. Germany*, No. 13710/88 (ECtHR December 16, 1992).

¹⁷ Jed Rubenfeld, “The Right of Privacy,” *Harvard Law Review* 102, no. 4 (1989): 737–807, <https://doi.org/10.2307/1341305>. Regarding freedoms, the right to private life may also be Seen in conjunction with freedom of thought, conscience, and religion, for example, See the following cases *Folgerø and Others v. Norway*, No. 15472/02 (ECtHR [GC] June 29, 2007); *Abdi Ibrahim v. Norway (communiquée)*, No. 15379/16 (ECtHR September 20, 2016); *T.c. v. Italy*, No. 54032/18 (ECtHR May 19, 2022).

¹⁸ For example, See case *Denisov v. Ukraine*, No. 76639/11 (ECtHR [GC] September 25, 2018), §95.

¹⁹ *Ibid.*

²⁰ For example, See case *Mustafa Sezgin Tanrikulu v. Turkey* where ECtHR finds a violation of Article 8 regarding lack of legal basis for mass interception (communication), breaching individual's freedom of communication. *Mustafa Sezgin Tanrikulu v. Turkey*, No. 27473/06 (ECtHR July 18, 2017).

²¹ See Chapter “Analysis of the CJEU judgement in Schrems I and Schrems II cases” and Chapter “Analysis of the ECtHR judgment Big Brother Watch and Others v. the UK.”

²² For example, See Article 4(1) of the GDPR. See Annex 1.

storing, recording data.²³ Additionally, for fuller picture, author invites one to be acquainted with notions of profiling and data mining. Data profiling is an action of data processing which creates a “profile” of an individual.²⁴ Data mining is a process of analyzing the collected data, to form such profile, for example, analyzing data from the individual’s digital footprint to establish patterns, thus, predicting possible outcomes or activities of an individual.²⁵ Governments (their substituted intelligence and security agencies) are faced with large amounts and sophisticated digital data, thus they employ data mining, namely, automated data analysis, in order to establish such patterns.²⁶ Such activities under mass surveillance possess different levels of the interference with one’s personal data,²⁷ for example, ADM processes are considered of the highest risk of the infringement of the right to privacy,²⁸ hence are imperative to keep in mind.

1.2. Governing mass surveillance and privacy

For a government to exercise action of mass surveillance, it shall be based on a legitimate aim, by lawful means and with the necessity in the society, additionally, safeguarded via proportionate means.²⁹ Such perspective is also established by the UN via GA’s Resolution No. 68/167 which invites States to establish an effective domestic oversight instruments and view protection of international human rights also in the light of: “the surveillance of communications, their interception and the collection of personal data, including mass surveillance.”³⁰

It is largely in the hands of a State to establish mass surveillance regulatory mechanism as there is no universal treaty to abide by.³¹ From author’s perspective, as the data (its collection) is a filament of a world wide web, it is the digital age’s greatest challenge in the realm of human rights to establish cohesive regulatory framework, as one’s data travels outside of specific jurisdiction, hence, is in greater threat of its jeopardy. The author provides outlook on domestic regulatory approaches, particularly, of the US and the EU as they are of a particular relevance to the analysis of the Schrems I, Schrems II and Big Brother Watch cases.

²³ For example, *See* Article 4(2) of the GDPR. *See* Annex 1.

²⁴ Former is best explained, in authors, view by Mireille Hildebrandt who defines profiling as: “(…) the process of ‘discovering’ patterns in data in databases that can be used to identify or represent a human or nonhuman subject (individual or group) and/or the application of profiles (sets of correlated data) to individuate and represent an individual subject or to identify as a member of a group (which can be an existing community or a ‘discovered category’).” Mireille Hildebrandt, “Profiling and the Identity of the European Citizen,” in *Profiling the European Citizen: Cross-Disciplinary Perspectives*, ed. Mireille Hildebrandt and Serge Gutwirth (Dordrecht: Springer Netherlands, 2008), 19, https://doi.org/10.1007/978-1-4020-6914-7_15. For further explanation *see* Article 4(4) of the GDPR. *See* Annex 1.

²⁵ S. Brinkhoff, “Big Data Data Mining by the Dutch Police: Criteria for a Future Method of Investigation,” *European Journal for Security Research* 2, no. 1 (April 1, 2017): 57–69, <https://doi.org/10.1007/s41125-017-0012-x>.

²⁶ *Ibid.*

²⁷ *See* the further analysis Chapter “Analysis of the ECtHR judgment Big Brother Watch and Others v. the UK.”

²⁸ *See* the further analysis Chapter “Analysis of the CJEU judgement in Schrems I and Schrems II cases” and Chapter “Analysis of the ECtHR judgment Big Brother Watch and Others v. the UK.”

²⁹ For example, *See* Section 2 of the Investigatory Powers Act 2016 (and such in a whole) of the UK. Investigatory Powers Act 2016 (King’s Printer of Acts of Parliament). Available on: <https://www.legislation.gov.uk/ukpga/2016/25/part/1/enacted>. Accessed April 1, 2023.

³⁰ *Ibid.*, Section 2 sub-section 4(c).

³¹ *See* Chapter “Analysis of the ECtHR judgment Big Brother Watch and Others v. the UK.”

Europe possesses the most in-depth and rather strict personal data regulation framework fostering coordinated variety of capitalism, namely, reflecting such capitalism form that seeks to combine market-oriented principles with government's intervention³² – primarily GDPR,³³ EUCFR,³⁴ DMA,³⁵ DSA,³⁶ ECHR.³⁷ The U.S. establishes liberal variety of capitalism,³⁸ possessing free-market approach also in the sphere of data movement, fostering such opportunities as full alienability³⁹ and free data flow.⁴⁰ Hence, the data regulation as such is not existent and is rather fragmented, addressing specific fields, for example, HIPAA regulates health data privacy and portability.⁴¹

³² Varieties of capitalism are political concepts that describe forms of capitalist economies upholding the narrative that capitalism possesses subfields. Personal data in a digital age is also regarded as currency and used in commercial activities, which especially can be observed in reading analysis of Schrems I and Schrems II cases where the Safe Harbor and Privacy Shield agreement primarily described agreements for commercial activities which involved data transfers. Such a concept greatly influences policy, namely, establishing regulations that are, for example, stricter on personal data rights, hence establishing barriers for commercial activities – a coordinated variety of capitalism. It is also interesting to note China's approach, which is considered to foster an organized verity of capitalism due to its isolationism policy and establishment of a Great China Firewall that suppresses data mobility (in both directions), nevertheless, Brussels Effect has traveled to the East, influencing also China's Data Security Law, Personal Information Protection Law and Cybersecurity Law. Data Security Law of the People's Republic of China, September 1, 2021. Personal Information Protection Law of the People's Republic of China, November 1, 2021. Cybersecurity Law of the People's Republic of China, June 1, 2017. David Soskice and Wetenschappelijke Raad Voor Het Regeringsbeleid, "Varieties of Capitalism; Varieties of Reform," in *Aftershocks*, ed. Anton Hemerijck, Ben Knapen, and Ellen van Doorne, Economic Crisis and Institutional Choice (Amsterdam University Press, 2009), 133–42, <http://www.jstor.org/stable/j.ctt46mtqx.16>.

³³ GDPR is a successor of Directive 95/46/EC. It is perceived as the most detailed and robust personal data regulation worldwide. Both of these regulatory frameworks are relevant for the case analysis provided further. 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, 281 OJ L § (1995). Available on: <http://data.europa.eu/eli/dir/1995/46/oj/eng>. Accessed February 23, 2023. (Directive 95/46/ec). 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) (Text with EEA Relevance)." Available on: <https://eur-lex.europa.eu/eli/reg/2016/679/oj>. Accessed February 23, 2023. (GDPR).

³⁴ Article 7, Article 8 and Article 47 of the EUCFR. See Annex 2.

³⁵ Even though regulating the market (and its competition rules), it largely defines data collection rules. See Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act) (Text with EEA relevance), 265 OJ L § (2022). Available on: <http://data.europa.eu/eli/reg/2022/1925/oj/eng>. Accessed February 23, 2023.

³⁶ Similarly as DMA, DSA also aims to protect one's private life in the context of illegal advertising and disinformation. See Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act) (Text with EEA relevance), 277 OJ L § (2022). Available on: <http://data.europa.eu/eli/reg/2022/2065/oj/eng>. Accessed February 23, 2023.

³⁷ Preamble and Article 8 of the ECHR. See Annex 3.

³⁸ Soskice, David, and Wetenschappelijke Raad Voor Het Regeringsbeleid. "Varieties of Capitalism; Varieties of Reform." In *Aftershocks: Economic Crisis and Institutional Choice*, edited by Anton Hemerijck, Ben Knapen, and Ellen van Doorne, 133–42. Amsterdam University Press, 2009. <http://www.jstor.org/stable/j.ctt46mtqx.16>.

³⁹ The ability to get rid of something (you can give away all your data through a contract).

⁴⁰ Franz-Stefan Gady, "EU/U.S. Approaches to Data Privacy and the 'Brussels Effect': A Comparative Analysis," *Georgetown Journal of International Affairs*, 2014, 12–23, <http://www.jstor.org/stable/43773645>; Paul M. Schwartz and Daniel J. Solove, "Reconciling Personal Information in the United States and European Union," *California Law Review* 102, no. 4 (2014): 877–916, <http://www.jstor.org/stable/23784355>.

⁴¹ Health Insurance Portability and Accountability Act of 1996 (HIPAA) June 28, 2022. Available on: <https://www.cdc.gov/phlp/publications/topic/hipaa.html>. Accessed February 23, 2023.

Even though Europe possesses great legal instruments to safeguard one's privacy, when data interception action is taken, via the notion of wide margin of application granted to the state by judicial authorities,⁴² as it concerns a matter of national security, the States are those carrying all the gravity to ensure fair tradeoff between one's privacy and overall security.

On the other hand, right to privacy is extensively governed on all of the levels – international, regional and national⁴³. Right to privacy on international level is governed by the ICCPR under Article 17⁴⁴ which mirrors the UDHR Article's 12 wording,⁴⁵ where right to privacy alongside outlined aspects adds respect towards one's honor.⁴⁶ As the privacy is a multifaced notion, regarding its vulnerability in the spectrum of digital advancement, the UN established the Human Rights Council Resolution on the right to privacy in the digital age (Doc. A/HRC/28/L.27, 24 March 2015) upon the Snowden revelations⁴⁷ condemning the practices of mass surveillance.⁴⁸ Consequently, the UN Special Rapporteur on the right to privacy issued "Principles underpinning privacy and the protection of personal data" specifically taking into account problems arising from processing personal data whilst using information and communication technologies.⁴⁹

As the mass surveillance amounts to processing personal data, for example, an action of collecting personal data via communication surveillance, such UN principles are also applicable to mass surveillance activities. The established guiding principles incorporate, *inter alia*, legality,

⁴² Michael R. Hutchinson, "The Margin of Appreciation Doctrine in the European Court of Human Rights," *The International and Comparative Law Quarterly* 48, no. 3 (1999): 638–50, <http://www.jstor.org/stable/761320>.

⁴³ Author in this chapter will not analyze any specific national regulation providing safeguards to privacy (*see* such in further case analysis).

⁴⁴ Article 17 of the ICCPR. *See* Annex 4.

⁴⁵ Even though UDHR is a soft law instrument possessing a secondary nature, it is regarded as a grassroots legal instrument for codified human rights on the international level the UN. Article 12 of the UDHR. *See* Annex 5.

⁴⁶ *Ibid.*

⁴⁷ *See* Chapter "Facts of the Schrems I case."

⁴⁸ OHCHR. "A/HRC/51/17: The Right to Privacy in the Digital Age." Accessed May 9, 2023. Available on: <https://www.ohchr.org/en/documents/thematic-reports/ahrc5117-right-privacy-digital-age>. Accessed April 10, 2023.

⁴⁹ Such an instrument is of a secondary nature, nevertheless, is a great guiding tool for states regarding adherence to international regulations and thus establishing more uniform international standards. OHCHR. "A/77/196: Principles Underpinning Privacy and the Protection of Personal Data." Accessed May 9, 2023. Available on: <https://www.ohchr.org/en/documents/thematic-reports/a77196-principles-underpinning-privacy-and-protection-personal-data>. Accessed April 10, 2023.

lawfulness, legitimacy,⁵⁰ consent,⁵¹ transparency,⁵² proportionality, minimization⁵³ and others.⁵⁴ The author draws emphasis on the principle of proportionality, as it is an essential concept employed by the judicial bodies when evaluating whether a breach of private life have occurred.⁵⁵ The proportionality also showcases the interlinkage among all principles and can be seen as a supervisory principle which oversees, for example, whether the principle of minimization is employed to meet the purpose of data processing which is showcased under the principle of legality.⁵⁶

On regional level, viewing Europe, rights to privacy can be found, for example, in ECHR and in EUCFR.⁵⁷ The ECHR showcases right to privacy in Article 8, which primarily establishes for the High Contracting Parties a negative obligation not to intervene with one's private, family life, home and correspondence.⁵⁸ Nevertheless, Article 8 of the ECHR also possess a positive obligation, namely, respect for private life, for example, obliging High Contracting Parties to

⁵⁰ The first three notions are combined under one principle, namely, the principle of legality, lawfulness, and legitimacy outlines the need for compliance with regulations at force, with an emphasis on the respect for the privacy and dignity of the data subjects. The legitimate grounds outlining the legality of personal data processing – consent; law; public interests; legitimate interests; vital interests; mandate to public authority; recognition of the subject before public authority. *Ibid.*, pp. 4-6. See also Steven Feldstein, “Distinguishing Between Legitimate and Unlawful Surveillance,” *The Global Expansion of AI Surveillance* (Carnegie Endowment for International Peace, 2019), JSTOR, <http://www.jstor.org/stable/resrep20995.6>.

⁵¹ The principle of consent requires a data controller to receive an expression of a subject to be legally bound by such intervention in private life. This is the main loophole – an indiscriminate collection of data on individuals without any type of knowledge or consent. *Ibid.*, pp. 6-7.

⁵² The principle of transparency obliges the controller to furnish subjects with clear and comprehensive details regarding the processing of their personal information. Some of the information required to be provided to individuals is the aim and purpose of the processing; legal grounds; the identity of the controller; the recipient; information on rights to a subject; information on complaint procedure; the existence of the ADM process and others. *Ibid.*, p.9.

⁵³ The principle possessing a mitigating effect is the principle of minimization. It showcases the aim to limit the data at all times in order to achieve the aim and purpose and where possible to use less intrusive means. *Ibid.*, p.10. See also Anneliese Roos, “Core Principles of Data Protection Law,” *The Comparative and International Law Journal of Southern Africa* 39, no. 1 (2006): 113, <https://www.jstor.org/stable/23253014>.

⁵⁴ The UN principles also include the principle of purpose; principle of fairness; the principle of quality; the principle of responsibility; the principle of security.

⁵⁵ See the further analysis in the Chapter “Analysis of the CJEU judgement in Schrems I and Schrems II cases” and Chapter “Analysis of the ECtHR judgment Big Brother Watch and Others v. the UK.”

⁵⁶ Namely, whether the actions meet the necessities or are going beyond defined, moreover, supervising whether means how those actions are exercised are appropriate. *Supra* note 49. One also shall note the OECD Privacy Guidelines which under the Collection Limitation Principle outline that consent and knowledge of the data subject must be obtained when appropriate, consequently, it could be argued that consent or even a minimum of knowledge (as outlined by the UN) is not to be applied for the mass surveillance. However, it must be noted that these Guidelines were established in 1980, even though being benchmark privacy principles agreed upon on an international scale, their outlook does not meet the fast-advancing presence of the digital age and such approach, namely, not adding a minimum consent requirement for the personal data use, would add more to the privacy rights movement resistance. Organisation for Economic Cooperation and Development (OECD), *Guidelines Governing the Protection of Privacy and Transborder Flow of Personal Data*, 23 September 1980. See also David Wright, Paul Hert, and Serge Gutwirth, “Are the OECD Guidelines at 30 Showing Their Age?,” *Commun. ACM* 54 (February 1, 2011): 119–27, <https://doi.org/10.1145/1897816.1897848>; Frederik Zuiderveen Borgesius, Jonathan Gray, and Mireille van Eechoud, “Open Data, Privacy, and Fair Information Principles: Towards a Balancing Framework,” *Berkeley Technology Law Journal* 30, no. 3 (2015): 2073–2131, <https://www.jstor.org/stable/26377585>.

⁵⁷ Article 8 of the ECHR. See Annex 3.

⁵⁸ Article 8 of the ECHR. See Annex 3. *Kroon and Others v. the Netherlands*, No. 18535/91 (ECtHR October 27, 1994), §31.

establish such policies or measures that would secure such positive duty.⁵⁹ Article 8(2) of the ECHR, unlike Article 17 of the ICCPR, inherently establishes grounds for invoking a balancing act, thus, the principle of proportionality.⁶⁰ The grounds which justifies an infringement of privacy under Article 8 of the ECHR constituting a legitimate aim are:

- 1) interests of national security;
- 2) necessity in a democratic society;
- 3) public safety;
- 4) economic well-being of the country;
- 5) prevention of disorder or crime;
- 6) protection of health;
- 7) protection of morals;
- 8) protection of the rights and freedoms of others.⁶¹

For the act of mass surveillance, the legitimate grounds for interfering with one's privacy usually would amount to the national security.⁶² It must be noted, that even though mass surveillance primary is seen as infringing Article 8 of the ECHR, in some instances, such as in protection of a journalistic sources, Article 10 of the ECHR, which protects freedom of expression can be applied.⁶³ For example, in the case of case *Telegraaf Media Nederland Landelijke Media B.V. and Others v. the Netherlands* which concerned a telephone tapping of journalists the ECtHR found a violation on both – Article 8 and Article 10 – noting that the Netherlands did not establish adequate safeguards concerning the monitoring of journalists aimed at ascertaining their sources.⁶⁴

Furthermore exploring Europe's privacy regulative landscape, the EUCFR, in author's opinion, draws more in depth outlook on matter of safeguard of personal data and privacy. Article 7 of the EUCFR analogous to the Article 8 of the ECHR protects one's privacy.⁶⁵ However, the EUCFR expands the borders of mere privacy safeguards and in Article 8 of the EUCFR showcases the protection of one's personal data.⁶⁶ Even though protection of personal data is vested in an autonomous provision, in author's opinion, it should be viewed in conjunction of Article 8 of the EUCFR. The former could not be isolated from latter, as described above, intervention with one's

⁵⁹ *Lozovyye v. Russia*, No. 4587/09 (ECtHR April 24, 2018), §36.

⁶⁰ Article 17 of the ICCPR. *See* Annex 4. Article 8 of the ECHR. *See* Annex 3.

⁶¹ Article 8(2) of the ECHR. *See* Annex 3.

⁶² *Big Brothers Watch* case outlines that the UK for mass surveillance acts in its regulatory legislation RIPA, as grounds of legitimate aim (among national security) established also protection of rights and freedoms of others or protection of crime or disorder. *Big Brother Watch and Others v. the United Kingdom*.

⁶³ A similar approach also was employed in the *Big Brother Watch* case, where the applicants' claimed both abuse of private life and freedom of expression in the instance of the interception of journalist activities, hence jeopardizing investigatory journalism's freedom. *Big Brother Watch and Others v. the United Kingdom*. §52.

⁶⁴ *Telegraaf Media Nederland Landelijke Media B.v. and Others v. the Netherlands*, No. 39315/06 (ECtHR November 22, 2012).

⁶⁵ Article 7 of the EUCFR. *See* Annex 2.

⁶⁶ Article 8 of the EUCFR. *See* Annex 2.

personal data falls within the umbrella notion of privacy.⁶⁷ Regarding the CJEU general practices on the assessment of the proportionality analysis, it has established following pattern of steps to be fulfilled:

- 1) whether the proposed aim has been recognized by the EU Law;
- 2) whether the measures were appropriate to achieve the aim;
- 3) whether there was a necessity to achieve the aim;
- 4) whether the proportionality could be considered *stricto sensu*, namely, whether the burden placed on the individuals was directly proportionate to the objective sought to be achieved.⁶⁸

Consequently, outlining the importance of the engagement with the facts of the case. The CJEU frequently exercises the balancing approach, especially, concerning fundamental right balance against the public interests.⁶⁹

The limitations to Article 7 and Article 8 of the EUCFR are established in the Article 52(1) of the EUCFR,⁷⁰ noting that any limitations must be necessary and proportionate, meeting the genuine interests of the Union based on a legal grounds.⁷¹ The EUCFR meets the same challenge as all of the above mentioned regional or international regulations – no uniform definition of national security. Thus leaving state with a great margin of appreciation when defining such. Nevertheless, further analysis of Big Brother Watch case and Schrems II case outlined that state are under the scrutiny of the supervisory authorities, such as the ECtHR and the CJEU, moreover, in the realm of the EU, its subsequent institutions, to assess whether the interpretation of national security in the light of the actions carried out under mass surveillance does not infringe rights to privacy.

1.3. Finding balance between interests under mass surveillance and one's right to privacy

⁶⁷ European Union Agency for Fundamental Rights. "Surveillance by Intelligence Services: Fundamental Rights Safeguards and Remedies in the European Union – Volume II – Summary," May 9, 2018. Available on: <http://fra.europa.eu/en/publication/2018/surveillance-intelligence-services-fundamental-rights-safeguards-and-remedies>. Accessed April 10, 2023.

⁶⁸ Burden shall be necessary and directly related to the achievement of the legitimate objective, thus establishing a narrative of the legitimacy of the government's action taken. Rupert Dunbar, "The Application of International Law in the Court of Justice of the European Union: Proportionality Rising," *German Law Journal* 22, no. 4 (2021): 557–92, <https://doi.org/10.1017/glj.2021.25>; Reinhard Gebhard v. Consiglio dell'Ordine degli Avvocati e Procuratori di Milano, No. Case C-55/94 (CJEU November 30, 1995), § 37; Commission of the European Communities v. Italian Republic, No. Case C-110/05 (CJEU February 10, 2009), § 59; Eugen Schmidberger, Internationale Transporte und Planzüge v. Republik Österreich, No. Case C-112/00 (CJEU June 12, 2003), §79.

⁶⁹ Internationale Handelsgesellschaft mbH v Einfuhr- und Vorratsstelle für Getreide und Futtermittel, No. Case 11-70 (CJEU December 17, 1970), §24; Liselotte Hauer v. Land Rheinland-Pfalz, No. Case 44/79 (CJEU December 13, 1979), §23.

⁷⁰ Article 7, Article 8 and Article 52(1) of the EUCFR. See Annex 2.

⁷¹ Article 52(1) of the EUCFR. See Annex 2.

Before outlining the judicial spectrum's approach on the balancing interest of constituted under mass surveillance and one's right to privacy, the author explores both interests' proponents arguments and the narrative of a need for such balancing act – establishment of fair interest tradeoff.

1.3.1. Pro-surveillance camp

Those who advocate in favor of the necessity of mass surveillance are driven by growing threats of cyber-attacks, terrorism and a rise of extremist groups.⁷² For example, Charlie Hebdo attack in Paris in 2015 sparked calls for greater surveillance.⁷³ As a result, national security concerns often become a key item on the political agenda. The proponents of mass surveillance are frequently criticized for their alleged disregard for constitutional principles or democratic values.⁷⁴ Nevertheless, pro-surveillance proponents aiming to meet the objectives of a privacy are in search for engineering tools that would make mass surveillance less encroaching.⁷⁵ For example, introducing less directly linked data sets to the individual and anonymizing those that are unnecessary to detect for safety and surveillance precautions.⁷⁶

The pro-surveillance camp has been also criticized for its lack of transparency in security policies, which has been seen as an attack on one of the core values of democracy, hence, losing the trust in the public sector.⁷⁷ However, it should be noted that democratic societies recognize the need for legitimate secrecy within the context of security policies that are implemented to achieve the objectives of national security.⁷⁸ In author's opinion in a matters of national security completely lifting the veil of secrecy⁷⁹ would do more harm than good as it would establish never-ending spiral of policy establishment and consequent breaches by those who are the subject to such policies. Nevertheless, the compromise shall lay within the balancing act of interest, namely, keeping one safe whilst not intruding with one's rights to privacy explained further. According to political

⁷² Ünver, "Politics of Digital Surveillance, National Security and Privacy," 1.

⁷³ Kevin D. Haggerty and Amber Gazso, "Seeing beyond the Ruins: Surveillance as a Response to Terrorist Threats," *The Canadian Journal of Sociology / Cahiers Canadiens de Sociologie* 30, no. 2 (2005): 169–87, <https://doi.org/10.2307/4146129>. For more statistics on terrorist attacks in the EU See Annex 6.

⁷⁴ For instance, the USA Fourth Amendment⁷⁴ protection lays within the notion of respect towards privacy by government agencies, such as law enforcement, to protect against arbitrary interventions which would let democracy slide into totalitarian apparatus.⁷⁴ The act of respect, thus, shall be *Seen* in a "reasonable expectation of privacy,"⁷⁴ where the reasonableness entails the probable cause and need to be carried out in accordance with a warrant, namely, possessing legitimate aim and legal grounds. However, as the core of mass surveillance (that distinguishes it from targeted surveillance) is to intercept the lack of evidence of wrongdoing, it rather possesses superficial and intrusive nature. Ünver, "Politics of Digital Surveillance, National Security and Privacy," 1; *Katz v. United States*, 389 U.S. 347 (1967) (United States Supreme Court December 18, 1967); David Alan Sklansky, "Too Much Information: How Not to Think About Privacy and the Fourth Amendment," *California Law Review* 102, no. 5 (2014): 1070, <http://www.jstor.org/stable/24758163>.

⁷⁵ Inez Miyamoto, "Mass Surveillance and Individual Privacy" (Daniel K. Inouye Asia-Pacific Center for Security Studies, 2020), JSTOR, <http://www.jstor.org/stable/resrep24871>.

⁷⁶ George Danezis and Bettina Wittneben, "The Economics of Mass Surveillance," n.d.; Feldstein, "Distinguishing Between Legitimate and Unlawful Surveillance."

⁷⁷ Albert Meijer, "Understanding the Complex Dynamics of Transparency," *Public Administration Review* 73, no. 3 (2013): 429–39, <http://www.jstor.org/stable/42002946>.

⁷⁸ Ünver, "Politics of Digital Surveillance, National Security and Privacy," 4.

⁷⁹ Transparency these days shall also be understood with an indirect mediation regime, namely, some of the institutional characteristics are described via action shown, for example, via social media, etc., not directly stating what are the direct procedures at hand. Meijer, "Understanding the Complex Dynamics of Transparency."

scientist Michael Desch, the transparency cost in democracies differ from such regimes as authoritarian or totalitarian due to that in democracies the transparency secrecy is established throughout many institutional layers and possess whistleblowing instruments that are made available to society in a case of a doubt or concern of exercised security policies.⁸⁰

Proponents of mass surveillance also argue that the likelihood of the variety of individual's data interception lays within the hands of the individual, namely, one is responsible for its own digital exposure and needs to be self-aware of the risks of surveillance.⁸¹ Hence, arguing that there is an artificial bubble of privacy seeking individuals, who themselves put their lives on digital display.⁸²

1.3.2. Pro-privacy camp

The human rights protection camp on the other hand advocates that the invasive character of mass surveillance, which often replaces less intrusive measures that could be implemented by governments to ensure societal safety,⁸³ is a source of considerable concern for the right to privacy.⁸⁴ Such systematic monitoring practices represent a significant intrusion into an individual's daily life, as almost every action and movement is meticulously documented in a digital format.⁸⁵ As the surveillance opportunities increase alongside of technological advancement and digitalization, so does the resistance to surveillance. Sociological anti-surveillance movement can be also seen expressed in an art form, a vivid example of such is a graffiti artist Banksy from the United Kingdom, who in his London mural⁸⁶ outlines how one individual is fighting the system of mass surveillance or employed oppressing system (outlining such idea via using Soviet font).⁸⁷

If pro-surveillance camp fosters its impetus on advancing security via growing threats in various fields, then privacy proponents find their resistance *inter alia* in a fear of misuse of

⁸⁰ Michael C. Desch, "Democracy and Victory: Why Regime Type Hardly Matters," *International Security* 27, no. 2 (2002): 5–47, <http://www.jstor.org/stable/3092142>.

⁸¹ Dennis Kingsley, "Keeping a Close Watch – The Rise of Self-Surveillance and the Threat of Digital Exposure," *The Sociological Review* 56 (August 1, 2008): 347–57, <https://doi.org/10.1111/j.1467-954X.2008.00793.x>.

⁸² Kingsley, "Keeping a Close Watch – The Rise of Self-Surveillance and the Threat of Digital Exposure."

⁸³ For example, using targeted surveillance, which monitors specific individuals or groups who are suspected of engaging in criminal or terrorist activity. See, Pieter Omtzigt, "Mass Surveillance Report | Doc. 13734 |" (Council of Europe, March 18, 2015), <https://pace.coe.int/en/files/21583/html>.

⁸⁴ Alongside threats to such fundamental right as privacy, mass surveillance, also endangers such human rights and freedoms as freedom of information and expression, right to a fair trial and freedom of religion. Joanna Kulesza and Roy Balleste, *Cybersecurity and Human Rights in the Age of Cybertechnology*, 2015; Abhik Chaudhuri, "Internet of Things Data Protection and Privacy in the Era of the General Data Protection Regulation," *Journal of Data Protection and Privacy* Vol-1 (December 1, 2016): 64–75; Omtzigt, "Mass Surveillance Report | Doc. 13734 |."

⁸⁵ A. Michael Froomkin, "The Death of Privacy?," *Stanford Law Review* 52, no. 5 (2000): 1461–1543, <https://doi.org/10.2307/1229519>.

⁸⁶ Banksy mural "One Nation Under CCTV". See Annex 7.

⁸⁷ Aaron K. Martin, Rosamunde E. van Brakel, and Daniel J. Bernhard, "Understanding Resistance to Digital Surveillance: Towards a Multi-Disciplinary, Multi-Actor Framework," *Surveillance & Society* 6, no. 3 (April 26, 2009): 213–32, <https://doi.org/10.24908/ss.v6i3.3282>.

collected information; intervention with one's freedom;⁸⁸ perceptions molded by public debate.⁸⁹ Additionally, supervising parties, such as Council of Europe has expressed its concern over creation of "back doors" for additional terrorist or cyberterrorist attack due to weak security standards and practices employed by the intelligence agencies.⁹⁰

One of the core principles to safeguard privacy is transparency, which is one of the pillar values of pro-privacy proponents, who criticize pro-surveillance camp of lacking such. Consequently, criticizing the pro-surveillance camp's argument about the self-awareness of the risks being intercepted outlining that the inherent nature of the mass surveillance where individuals do not even in some instances possess an awareness of their personal data interception.⁹¹ As bulk interception cannot be justified with the invitation for the society to not to use technological advancement, putting oneself in a pit of technical or digital illiteracy or leaving oneself in digital black box.⁹²

1.3.3. Tradeoffs – balancing interests

The middlemen of both camps seek to establish balance between two needs. For instance, the pro-surveillance camp should step forward in advancing less intrusive engineering methods, the pro-privacy camp should acknowledge the need of legitimate transparency secrecy's veil, nevertheless, resists of the intrusive nature of the mass surveillance. Thus, for such dispute to be fair it needs to be adequately balanced employing the proportionality principle.

Some theorists, as David Pozen perceives such relationship of balance as a tradeoff, namely, trading the interests of, for instance, national security with such of an individual's privacy.⁹³ Moreover, privacy scholar Daniel Solove establishes privacy taxonomy and views such notion from a pluralistic approach, where one of the pillars of such privacy taxonomy is an information collection, which includes the action of mass surveillance.⁹⁴ Thus in the balancing game of fair tradeoff, the personal data shall be understood as an individual's privacy interest whereas the act

⁸⁸ Privacy is also perceived as in the form of freedom not only a right, mainly, in the form of an individual being free from unreasonable search (that would be mass surveillance). Ari Waldman, "Privacy as Trust: Sharing Personal Information in a Networked World," *Articles & Chapters*, January 1, 2015, 567, https://digitalcommons.nyls.edu/fac_articles_chapters/445.

⁸⁹ Dumitrina Galantou, "The Big Brother Fear," *American Intelligence Journal* 33, no. 1 (2016): 59, <https://www.jstor.org/stable/26202166>.

⁹⁰ Omtzigt, "Mass Surveillance Report | Doc. 13734 |."

⁹¹ Charles D. Raab, "Security, Privacy and Oversight," in *Security in a Small Nation*, ed. Andrew W. Neal, 1st ed., vol. 4, Scotland, Democracy, Politics (Open Book Publishers, 2017), 77–102, <http://www.jstor.org/stable/j.ctt1sq5v42.8>.

⁹² For analogy See Cathy O'Neil's "Weapons of Math Destruction", which argues about leaving individuals with technical illiteracy via enabling one to understand the sophisticated nature of algorithms that discriminate against one's human rights. Cathy O'Neil, *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy*, First edition (New York: Crown, 2016).

⁹³ David E. Pozen, "Privacy-Privacy Tradeoffs," *The University of Chicago Law Review* 83, no. 1 (2016): 221–47, <http://www.jstor.org/stable/43741598>. See also SÍOFRA O'LEARY, "BALANCING RIGHTS IN A DIGITAL AGE," *Irish Jurist* 59 (2018): 59–92, <https://www.jstor.org/stable/26431267>.

⁹⁴ Daniel J. Solove, "Understanding Privacy," SSRN Scholarly Paper (Rochester, NY, May 5, 2008), <https://papers.ssrn.com/abstract=1127888>.

of mass surveillance as an act which aim is to safeguard interest, for example, of national security.⁹⁵ Such tradeoff narrative is fostered upon interest shift,⁹⁶ constituting a dimensional tradeoff.⁹⁷

One of the common loopholes' illuminated by both camps are the need of transparency where on the one hand here is a need of a legitimate transparency's secrecy veil to meet the objectives of national security in regards to mass surveillance activities,⁹⁸ whilst on the other hand secrecy might lead to public distrust and foster technical illiteracy, where the society is left in a black box and does not share common knowledge of the threats associated with mass surveillance.⁹⁹ To illustrate one side effect of improperly balanced privacy needs causing the

⁹⁵ The author invites one to look at quite a similar analogy by a right to a fair trial, namely, the ECtHR has noted in its case law that as long as some restrictions possess lawful grounds, legitimate aim, and necessity in society, consequently fulfilling the test of proportionality, some procedural missteps taken by domestic authorities can be overlooked, as one needs to *See* rather the whole picture of a dispute at hand to establish whether there was a breach of the right to a fair trial (*See*, for example, *López Ribalda and Others v. Spain*). In the author's view, the same goes with the right to private life, one needs to sacrifice something to get in return some benefit which possesses a greater gravity than safeguarding a particular aspect of privacy. Of course, in many instances, there can be an individual subjective point of a particular breach of privacy. *López Ribalda and Others v. Spain*, No. 1874/13, 8567/13 (ECtHR [GC] October 17, 2019).

⁹⁶ In the light of the *Schrems II* case analyzed below, examining the National Security Agency's surveillance mechanisms should be such a framework that would serve as a mitigating factor in the contradicting privacy setoffs, which in its core shall be based on an axis of distributional tradeoff, namely, its end goal shall be the people's gain. Hence, one comes to the question of when tradeoffs are to be considered fair and proportionate. For instance, one can view the above-described loophole of transparency, namely, in a democratic apparatus where mass surveillance regulations possess a non-disclosure policy decreasing transparency, thus, undermining some democracy's fundamental values, are to be considered acceptable? Here the balancing act of proportionality comes into play to meet so-called lawful illegality in order to serve society. Pozen, "Privacy-Privacy Tradeoffs," 229–31. Consequently, privacy within the realm of constitutionalism could be constitutionally legitimate in the interests of the suppression of, for example, crime and national security only when accompanied by appropriate safeguards. Lisa M. Austin, "Lawful Illegality: What Snowden Has Taught Us About the Legal Infrastructure of the Surveillance State," SSRN Scholarly Paper (Rochester, NY, April 1, 2014), <https://doi.org/10.2139/ssrn.2524653>.

⁹⁷ An example of such type - a police officer's body camera that depending on the nature of the dispute serves both parties, namely, safeguards the officer vis-à-vis the person concerned. It may *Seem* from one perspective that state intervention via policies applied tends to go against and deter people's rights to privacy, nonetheless, mostly, such actions counterbalance other private interests. Pozen, "Privacy-Privacy Tradeoffs," 230.

⁹⁸ According to political scientist Michael Desch, the transparency cost in democracies differ from such regimes as authoritarian or totalitarian due to that in democracies the transparency secrecy is established throughout many institutional layers and possess whistleblowing instruments that are made available to society in a case of a doubt or concern of exercised security policies. Desch, "Democracy and Victory: Why Regime Type Hardly Matters."

⁹⁹ Not only individuals are equipped with the lack of common understanding, it also can be observed in the judicial proceedings - where dispute resolution is left in the hands of a good will and knowledge of witness experts, because judges do not possess even the basic knowledge of digital data gathering, moreover, the witness experts themselves have a hard time explaining algorithms, especially, AI decision making processes, thus leaving everyone in a black box. Namely, the High-Tech companies under the Competition Law possess a right not to disclose proprietary information, as the algorithms are considered as the main property of a company which are crucial for their activities, such algorithms are not fully described also for expert witnesses to examine, hence, leaving the judicial system in complete technical pit. For example, in the case of *State v. Loomis* (originating in the US) which concerned a judge using an algorithm Correctional Offender Management Profiling for Alternative Sanctions (COMPAS) for the categorizing defendant as a "high risk of recidivism," the Wisconsin Supreme Court concurring Justice Shirley Abrahamson stated: "this court's lack of understanding of COMPAS was a significant problem in the instant case." Hence, outlining, loopholes fostering algorithmic discrimination due to the lack of technical knowledge. *State of Wisconsin, Plaintiff Respondent, v. Eric L. Loomis, Defendant-Appellant.*, No. 2015AP157-CR (Supreme Court of Wisconsin 2016); O'Neil, *Weapons of Math Destruction*; Ashley Deeks, "The Judicial Demand for Explainable Artificial Intelligence," *Columbia Law Review* 119, no. 7 (2019): 1829–50, <https://www.jstor.org/stable/26810851>; Sargur N. Srihari, "Explainable Artificial Intelligence," *Journal of the Washington Academy of Sciences* 106, no. 4

Streisand effect, namely, with more restrictions fostering more evil,¹⁰⁰ for example, one may recall emergence of the bubble of the right to be forgotten, where Internet censorship websites quickly formed to keep such information alive throughout a deep web,¹⁰¹ namely, fostering an evil axis.¹⁰² Thus, the synergetic and mitigating interplay of privacy-national security needs and interests is of key importance to escape functional and regulatory risks.

Such tradeoff oftentimes involves commercial interest, both private and public, where for States competing in a technological race data sets are of a key importance for technological advancement and economic gain.¹⁰³ Hence, in the balance act of privacy and national security, oftentimes commercial interests are present, where a multiparty relationship thus is constituted by an individual, state and an entity. Such multilevel interplay may set the interests of an economic gains of a priority, thus the individual is in the most vulnerable position.¹⁰⁴

Moreover, diversity of such habitat fosters debate over the privacy and trust. One of the grassroots elements for seeking privacy is individual's feeling of the misuse of collected personal data.¹⁰⁵ The trust narrative is also of a great importance in a field of international relations, especially concerning cross border data transfers. The loss of a trust on a political level could be observed after Edward Snowden's revelations where the EU media and politicians expressed their distrust in the US government over the outrageous mass surveillance activities.¹⁰⁶

The never-ending tradeoff and debate over privacy via narrative of interest shift, in author's opinion, thus greatly demonstrates a swinging pendulum concept, namely, illustrating how policy

(2020): 9–38, <https://www.jstor.org/stable/27130153>; FRANK PASQUALE, *The Black Box Society* (Harvard University Press, 2015), <http://www.jstor.org/stable/j.ctt13x0hch>.

¹⁰⁰ Pozen, "Privacy-Privacy Tradeoffs," 238.

¹⁰¹ Deep web is an Internet content that is not searchable by your standard search engines. Britannica "What is the Difference Between the Deep Web and the Dark Web?" Available on: <https://www.britannica.com/story/whats-the-difference-between-the-deep-web-and-the-dark-web>. Accessed April 10, 2023.

¹⁰² Pozen, "Privacy-Privacy Tradeoffs."

¹⁰³ Thus, states are rather reluctant to share their data policy with the public and their citizens. Ünver, "Politics of Digital Surveillance, National Security and Privacy."

¹⁰⁴ Margaret Byrne Sedgewick, "Transborder Data Privacy as Trade," *California Law Review* 105, no. 5 (2017): 1513–42, <https://www.jstor.org/stable/26577713>. See Chapter "Facts of the Schrems I case."

¹⁰⁵ Ari Ezra Waldman, ed., "What Does Trust Mean for Privacy?," in *Privacy as Trust: Information Privacy for an Information Age* (Cambridge: Cambridge University Press, 2018), 61–76, <https://doi.org/10.1017/9781316888667.007>.

¹⁰⁶ Also exercised upon the key political figures such as Angela Merkel, who stated: "Actions in which the ends justify the means, in which everything that is technically possible is done, violate trust, they sow distrust." Thus, the EU Commission issued a communication with the aim to rebuild trust between the EU-US data flows. The US in the case of *Am. Civil Liberties Union v. Clapper*, 804 F.3d 617 after Snowden's revelations saw public trust and governmental credibility relationship downgrade due to the mass surveillance program's being "expansive concept of 'relevance'" was "unprecedented and unwarranted." In short, the loophole to public trust was that the scale of the collection was far beyond anything the public could have imagined. Alison Smale, "German Leader Criticizes U.S. Over Pervasive Surveillance," *The New York Times*, January 29, 2014, sec. World. Available on: <https://www.nytimes.com/2014/01/30/world/europe/german-leader-criticizes-united-states-over-surveillance.html>.

Accessed April 10, 2023; Adam Klein, Michèle Flournoy, and Richard Fontaine, "Defining the Problem," *Surveillance Policy* (Center for a New American Security, 2016), 18, JSTOR, <http://www.jstor.org/stable/resrep06418.5>; *Am. Civil Liberties Union v. Clapper*, 804 F.3d 617 (United States Court of Appeals for the Second Circuit May 7, 2015); European Data Protection Supervisor. "Rebuilding Trust in EU-US Data." Available on: https://edps.europa.eu/data-protection/our-work/publications/opinions/rebuilding-trust-eu-us-data-flows_en. Accessed April 10, 2023.

governing is shaped over time via impact of various factors.¹⁰⁷ For example, above mentioned Charlie Haddo attack portrayed right to privacy as an public concern, hence swinging the pendulum towards the pro-surveillance camp,¹⁰⁸ nevertheless, the Snowden's revelations and consequent cases of Schrems I, Schrems II and Big Brother Watch took individualistic turn and swung pendulum towards pro-privacy camp with an rather personal outlook – an individual's right to not to have an arbitrary interference with a personal data. Thus, underlining the main challenge of all democracies - to simultaneously serve political culture of a state that would safeguard security and technological advancement whilst ensuring universal and fundamental human right – right to privacy.

¹⁰⁷ Carly Nyst, "Secrets and Lies: The Proliferation of State Surveillance Capabilities and the Legislative Secrecy Which Fortifies Them – An Activist's Account," *State Crime Journal* 7, no. 1 (2018): 8–23, <https://doi.org/10.13169/statecrime.7.1.0008>.

¹⁰⁸ Same applies, for instance, of 9/11 attacks, where public security was demanded at the highest level, establishing, for example, internationally airport security checks. Christopher Slobogin, "Privacy at Risk: The New Government Surveillance and the Fourth Amendment," *Bibliovault OAI Repository, the University of Chicago Press*, January 1, 2007, <https://doi.org/10.7208/chicago/9780226762944.001.0001>.

2. ANALYSIS OF THE CJEU JUDGEMENT IN SCHREMS I AND SCHREMS II CASES

Following case analysis aims to establish the prerequisites of a balanced tradeoff of interests, consequently observing whether the judicial spectrum also guides the oscillation of the pendulum toward right to privacy. It is of a great importance to note the Snowden's revelations¹⁰⁹ and their subsequent key findings as they are regarded as the grassroots event of 21st century that sparked an international attention and consequent resistance on pro-privacy camp for prohibition on one's personal data infringement stemming from mass surveillance.¹¹⁰

2.1. Facts of the Schrems I case

Edward Snowden upon his findings emphasized the vastness of the surveillance activities conducted on personal data by the NSA, stating:

The NSA specifically targets the communications of everyone. It ingests them by default. It collects (...) filters (...) analyzes (...) measures (...) and it stores them.¹¹¹

Thus, revealing two major surveillance programs – PRISM program (collecting information from technology companies)¹¹² and “Upstream collection” programs (intercepting communications).¹¹³

¹⁰⁹ Edward Snowden was a former NSA intelligence contractor (IT system administrator of a company Booz Allen Hamilton) and CIA employee acknowledged that he leaked (was the whistleblower) great amount of NSA documents describing surveillance programs used by the US to be published in The Guardian for series of investigating articles. Latter also published in the Washington Post and in the new York Times Tom McCarthy, Edward Snowden identifies himself as source of NSA leaks - as it happened, 9 June 2013 (The Guardian). His revelations are also known as the NSA revelations of 2013. Oliver Stone and Gary Crowdus, “Edward Snowden Is Not Your Average Hero: An Interview with Oliver Stone,” *Cinéaste* 42, no. 1 (2016): 22–30, <http://www.jstor.org/stable/26356872>; Barton Gellman, Aaron Blake, and Greg Miller, “Edward Snowden Comes Forward as Source of NSA Leaks,” *Washington Post*, June 9, 2013, sec. Politics, Available on: https://www.washingtonpost.com/politics/intelligence-leaders-push-back-on-leakers-media/2013/06/09/fff80160-d122-11e2-a73e-826d299ff459_story.html. Accessed April 10, 2023; Ewen MacAskill et al., “NSA Files Decoded: Edward Snowden’s Surveillance Revelations Explained,” the Guardian, November 1, 2013. Available on: <http://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded>. Accessed April 10, 2023.

¹¹⁰ Richard Kilroy, “No Place to Hide: Edward Snowden, the NSA, and the U.S. Surveillance State. By Glenn Greenwald, New York, NY: Metropolitan Books, 2014.” *Journal of Strategic Security* 9, no. 3 (October 1, 2016), <http://dx.doi.org/10.5038/1944-0472.9.3.1552>. Commission of the European Communities v. Italian Republic, No. Case C-110/05 (CJEU February 10, 2009), §59.

¹¹¹ Amy Davidson Sorkin, “Edward Snowden, The N.S.A. Leaker, Comes Forward,” *The New Yorker*, June 9, 2013. Available on: <https://www.newyorker.com/news/amy-davidson/edward-snowden-the-n-s-a-leaker-comes-forward>. Accessed April 10, 2023.

¹¹² From the Washington Post publication of 6 June 2013, the FBI:” are tapping directly into the central servers of nine leading US internet companies, extracting audio and video chats, photographs, e-mails, documents and connection logs that enable analysts to track foreign targets (...),” hence the PRISM program enables NSA to “collect personal data such as emails, photographs and videos from major internet providers such Microsoft, Google and Facebook. This is done on a mass scale in accordance with orders made by the US Federal Intelligence Court sanctioning such activities.” Schrems v. Data Protection Commissioner, No. 765JR (High Court of Ireland June 18, 2014), §§10-11. See PRISM/US-984XN Overview. See Annex 8.

¹¹³ Such programs included codenames as BLARNEY, FAIRVIEW, OAKSTAR, and STORMBREW. Andrew Chadwick and Simon Collister, “Boundary-Drawing Power and the Renewal of Professional News Organizations: The Case of The Guardian and the Edward Snowden NSA Leak,” *International Journal of Communication* 8, no. 0 (September 1, 2014): 2421, <https://ijoc.org/index.php/ijoc/article/view/2883>.

Additionally alleging that the GCHQ via TEMPORA program reportedly intercepted fiber-optic cables carrying personal data via internet traffic, both in the UK and outside its borders.¹¹⁴ Moreover, the Guardian publications alleged that the GCHQ took part in the PRISM project with an aim to enable the US access for surveillance of British citizens.¹¹⁵ Additionally, mentioning that the NSA intercepted the communications of foreign citizens.¹¹⁶

The loophole of the US initiated response to the allegations of its infringement of foreigners personal data, was closed by Austrian Law student Maximillian Schrems, who initiated Court proceedings, primarily seen as between an individual and entity (Schrems I and Schrems II), but from a broader perspective constituting a dispute between the US and the EU values and outlook upon privacy regulations.¹¹⁷ The revelations swung privacy pendulum over to the individualistic perspective – namely, in the center of attention is an individual and consequent personal data. Hence, the landmark case of Schrems I and Schrems II were initiated at the CJEU and in parallel a Big Brother Watch case was submitted before the ECtHR.

Upon the impetus received from Snowden’s revelations Maximillian Schrems begun his fight for privacy – advocating for stronger safeguards of personal data. Schrems has been a user of Facebook since 2008, consequently his personal data provided to the social media platform was

¹¹⁴ Parliament of the United Kingdom. “The Intelligence Services.” Available on: <https://www.parliament.uk/business/publications/research/key-issues-parliament-2015/defence-and-security/intelligence-services/>. Accessed April 10, 2023. See also Ewen MacAskill et al., “GCHQ Taps Fibre-Optic Cables for Secret Access to World’s Communications,” *The Guardian*, June 21, 2013, sec. UK news. Available on: <https://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa>. Accessed April 10, 2023; *Big Brother Watch and Others v. the United Kingdom*, §15.

¹¹⁵ Chadwick and Collister, “Boundary-Drawing Power and the Renewal of Professional News Organizations,” 2422.

¹¹⁶ The US responded in a rather politically hostile approach to such revelations (for the UK’s response See *Big Brother Watch* case). In the immediate response the US Intelligence chiefs outlined the upcoming great downfall regarding the US security mechanism by such disclosure. Moreover, keeping such stance after five years, where in 2018 the U.S. National Counterintelligence and Security Center spokesperson Joel Melstad stated:” [Snowden’s revelations] have put U.S. personnel or facilities at risk around the world, damaged intelligence collection efforts, exposed tools to amass intelligence, destabilized U.S. partnerships abroad and exposed U.S. intelligence operations, capabilities and priorities.” Nevertheless, the US also initiated on a national level judicial proceedings examining whether such NSA bulk interception was legitimate, only emphasizing infringement of citizens’ privacy, not of those being foreign. The United States Court of Appeals for the Second Circuit held that Section 215 of the Patriot Act (established after 9/11 with an aim to vastly expand government’s authority to conduct surveillance on the US citizens) could not constitute basis for legitimate grounds of mass surveillance of domestic correspondences. This aspect, namely, the US interception of foreigners’ personal data, is particularly crucial to note, as both of the Schrems’s cases (also for the *Big Brother Watch* case regarding a transfer of personal data) regard specifically trans-Atlantic data transfers and consequent privacy infringement within such. The US political hostilities continued with a filing of a civil lawsuit against Snowden over publishing a memoir “Permanent Record”, thus violating his contractual and fiduciary obligations of non-disclosure under the agreement with NSA and CIA. Leading to establish the US Freedom Act (establishing limits on the interception of communications of US citizens by the US intelligence agencies, for example, NSA) upon which Patriot Act Section 215 expired. Chadwick and Collister, “Boundary-Drawing Power and the Renewal of Professional News Organizations”; “US Expects Fallout From Snowden Leaks for Years to Come,” *US News & World Report*, accessed May 9, 2023. Available on: <http://www.usnews.com/news/world/articles/2018-06-03/5-years-on-us-government-still-counting-snowden-leak-costs>. Accessed April 10, 2023; Peter Bergen et al., “Do NSA’s Bulk Surveillance Programs Stop Terrorists?” (*New America*, 2014), JSTOR, <http://www.jstor.org/stable/resrep10476>.

¹¹⁷ Such concept of international perspective was also upheld by the High Court of Ireland in context of Schrems cases, which held that:” question of transnational data protection and state surveillance is admittedly difficult and sensitive and (...) can in many respects be resolved only at the level of international diplomacy and realpolitik.” *Schrems v. Data Protection Commissioner*, §4.

transferred from Facebook's Irish subsidiary (Facebook Ireland Limited) to the Facebook's servers in the US (Facebook, Inc),¹¹⁸ namely, the Facebook Ireland was a data controller within the scope of the Data Protection Act 1988.¹¹⁹

Schrems on 25 June 2013 brought a complaint before the Irish Data Protection Commissioner (DPC),¹²⁰ claiming that based on the Snowden's revelations concerning the NSA mass surveillance activities, the US legal framework and consequent practices did not adequately safeguard data transferred to the US by the EU Member State.¹²¹ The DPC rejected such application on the basis of ill-founded claim, stating that Schrems did not possess evidence illustrating that his personal data was being surveillance by the NSA, stating that complaint was "frivolous and vexatious".¹²² Moreover, the DPC held that matter of the adequacy of the data protection mechanism in the US had to be determined within the framework of Decision 2000/520/EC of 26 July 2000 – known as the Safe Harbor decision, allowing data transfer from the EU to the US¹²³ – where the Commission¹²⁴ established that the US ensured adequate level of protection.¹²⁵ Namely, the DPC hold that the US possessed needed safeguard mechanism to escape infringement of one's privacy, as *imprimatur* based on the Safe Harbor decision, thus did not conduct an independent analysis.¹²⁶

Claim further was brought before the High Court of Ireland for appeal, stating that DPC decision was unlawful.¹²⁷ The High Court of Ireland held that the DPC had taken a correct stance regarding the Safe Harbor decision, outlining that it includes a "Community finding" which requires determination of the adequacy of protection in the light of the Safe Harbor decision.¹²⁸ Consequently, concluding that the DPC could not pose a different view, which would, thus be inconsistent with the Community finding.¹²⁹ Regarding the issue of insufficient evidence of interception, the High Court noted that in any event, Schrems was entitled to bring such claim,

¹¹⁸ Maximillian Schrems v. Data Protection Commissioner, No. Case C-362/14 (CJEU October 6, 2015), §§26-27.

¹¹⁹ Schrems v. Data Protection Commissioner, §17. Data Protection Act 1988. Available on: <https://www.irishstatutebook.ie/eli/1988/act/25/enacted/en/print.html>. Accessed February 23, 2023.

¹²⁰ The DPC was established in accordance of Data Protection Act 1988.

¹²¹ Namely, M.Schrems claimed that the US did not possess an adequate legal safeguard mechanism to protect personal data from surveillance of the US public authorities of the data transferred to the US – foreigners data. In a particular instance, M.Schrems personal data faced a great risk of being infringed by the US intelligence agencies as his data was transferred from the confines of the EU to the US. Maximillian Schrems v. Data Protection Commissioner (Schrems I), §28.

¹²² Schrems v. Data Protection Commissioner, §32.

¹²³ 2000/520/EC: 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 and related frequently asked questions issued by the US Department of Commerce (notified under document number C(2000) 2441) (Text with EEA relevance.), 215 OJ L § (2000). Available on: <https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A32000D0520>. Accessed February 23, 2023. (Safe Harbor decision).

¹²⁴ European Commission.

¹²⁵ Directive 95/46/EC.

¹²⁶ Schrems v. Data Protection Commissioner.

¹²⁷ *Ibid.*

¹²⁸ Schrems v. Data Protection Commissioner, §64.

¹²⁹ Schrems v. Data Protection Commissioner, §66.

especially, due to the lack of limits imposed on mass surveillance by the US that illuminated upon the Snowden's revelations.¹³⁰

Thus, stating that the right to private life also guaranteed by the Irish Constitution requires that any interference with such shall be proportionate and in accordance with law, especially, in the case of such mass surveillance.¹³¹ The High Court also proposed that the Snowden revelations have illuminated loopholes on the US data protection laws and practices, hence the re-evaluation of the Safe Harbor decision should be seen as necessary.¹³²

On the basis of such practical importance not only in Ireland, but also in the whole of the EU, concluding that the Safe Harbor decision was contrary to the Article 7 and Article 8 of the EUCFR.¹³³ Nevertheless, noting that the Safe Harbor decision came into force before the EUCFR and reflects an “innocent age” of data protection in the advent of advancement of social media and national security threats in form of widespread terrorism.¹³⁴ In order to appropriately assess and safeguard right to private life under the Safe Harbor decision, the High Court of Ireland referred case to the CJEU in accordance with Article 267 of the TFEU¹³⁵ requesting preliminary ruling in regards of the duties of the DPC to be absolutely bound by the Community finding or should the DPC conduct independent investigation.¹³⁶ Thus, opening the Schrems I case.

2.2. CJEU approach in Schrems I – finding proportionality

¹³⁰ The High Court Particularly noted:” even if this [the US particular interference with M.Schrems personal data – emphasis added] were considered to be unlikely, he is nonetheless certainly entitled to object to a state of affairs where his data are transferred to a jurisdiction which, to all intents and purposes, appears to provide only a limited protection against any interference with that private data by the US security authorities.” Schrems v. Data Protection Commissioner, §45. Relying on the CJEU judgement in Case C-293/12 Digital Rights Ireland which regarded invalidation of Data Retention Directive (Directive 2006/24/EC) on the basis of serious infringements on privacy regarding allowances to access personal data.

¹³¹ Schrems v. Data Protection Commissioner, §50. Article 40(5) of the Constitution of Ireland states:” The dwelling of every citizen is inviolable and shall not be forcibly entered save in accordance with law.” Constitution of Ireland (last amended June 2004) July 1, 1937. Available on: <https://www.irishstatutebook.ie/eli/cons/en/html>. Accessed April 1, 2023. The High Court of Ireland had particularly negative outlook on mass surveillance, concluding that mass surveillance inherently is contrary to the right to private life, hence it should be targeted, justifying that also such interception is in the interest of national security, additionally, possessing needed safeguards. Moreover, stating that:” In this regard, it is very difficult to See how the mass and undifferentiated accessing by State authorities of personal data (...) would pass any proportionality test or could survive constitutional scrutiny.” Hence pointing out that to escape the totalitarian approach of mass surveillance, the DPC would have been obliged to investigate. Nevertheless, from the perspective of the High Court as the EU Law prevails, the Community finding surpassed such a view. Schrems v. Data Protection Commissioner, §§52-57.

¹³² Notwithstanding the fact, that the case concerned did not bring a dispute over such validity. High Court of Ireland Consequently outlined:” the Snowden revelations demonstrate a massive overreach on the part of the security authorities, with an almost studied indifference to the privacy interests of ordinary citizens. Their data protection rights have been seriously compromised by mass and largely unsupervised surveillance programmes ” Schrems v. Data Protection Commissioner, §8;§69.

¹³³ Schrems v. Data Protection Commissioner, §62.

¹³⁴ Schrems v. Data Protection Commissioner, §63.

¹³⁵ Article 267 of the TFEU. See Annex 9.

¹³⁶ Schrems v. Data Protection Commissioner, §71.

Upon the request from a High Court of Ireland of a preliminary ruling, the CJEU (Grand Chamber) on 6 October 2015 gave a judgment in the Schrems I case.¹³⁷ The main issues to examine within such request were:

- 1) interpretation of Article 7 and Article 8 (also Article 47)¹³⁸ of the EUCFR; Article 25(6) and Article 28 of the Directive 95/46/EC¹³⁹ in the context of dispute;
- 2) validity of Safe Harbor decision.¹⁴⁰

Hence, the aim of such analysis was to establish whether the Safe Harbor decision was valid and what the DPC as supervisory authority was obliged to do in such dispute. The author further examines the CJEU approach on the proportionality and consequent legitimacy of the mass surveillance interception with one's privacy. Before outlining the approach of the CJEU, author provides an overview of the examined regulatory framework.

The Directive 95/46/EC – personal data protection and movement of such data.¹⁴¹ Directive 95/46/EC starting from 2016 was substituted with the GDPR.¹⁴² However, at the time in force an Article 25(6) of Directive 95/46/EC established a principle of an adequate level of protection when data is transferred to a third country with a specific aim to safeguard one's privacy.¹⁴³ Article 28 of Directive 95/46/EC established rights and obligations of the supervisory authority of Member States (for the safeguard of personal data).¹⁴⁴ In the respect of Schrems I, such provisions concerned analysis of the DPC's rights and obligation when Schrems requested analysis of the Safe Harbor decision.

Safe Harbor decision – showcased principles of the governance of personal data exchange between the EU (including Switzerland) and the US.¹⁴⁵ Article 1 outlined the conditions that shall be met for each transfer: (1) agency that is recipient of data had unambiguously and publicly disclosed its commitment to comply with Safe Harbor decision (principled laid down);¹⁴⁶ (2) agency was a subject to investigative complaints and redress for individuals against unfair practice, namely, misuse and/or abuse of personal data.¹⁴⁷ Article 3 gave powers to Member States to suspend data flow to the particular agency, if such fails to abide by Safe Harbor decisions.¹⁴⁸ Article

¹³⁷ Maximillian Schrems v. Data Protection Commissioner (Schrems I).

¹³⁸ Article 47 of the EUCFR lays down the rights of an effective remedy, which will not be further analyzed, as it is not in the scope of this Thesis. *See* Annex 2.

¹³⁹ Article 25(6) and Article 28 of Directive 95/46/EC. *See* Annex 10.

¹⁴⁰ Based on the examination of the adequacy of the protection. Maximillian Schrems v. Data Protection Commissioner (Schrems I), §1.

¹⁴¹ It must be noted that Directive are not directly binding upon Member States, namely, they shall be transposed into national laws as opposed to the nature of Regulation. The Directive 95/46/EC in Ireland was transposed into the Data protection Act. Directive 95/46/EC.

¹⁴² Directive 95/46/EC.

¹⁴³ Article 25(6) of Directive 95/46/EC. *See* Annex 10.

¹⁴⁴ Article 25(6) of Directive 95/46/EC. *See* Annex 10. The obligations included monitoring of the application of Directive; draw reports; granted *inter alia* investigating powers; effective powers of intervention; the power to engage in legal proceedings; power to hear claims lodged by individuals. Directive 95/46/EC.

¹⁴⁵ Safe Harbor decision.

¹⁴⁶ Safe Harbor decision.

¹⁴⁷ Safe Harbor decision.

¹⁴⁸ Mainly, in two cases: (1) the US government body has determined violation of principles; (2) there is a substantial likelihood of violation of principles. Article 3 of Safe Harbor Decision. *See* Annex 11.

4 established that the Safe Harbor decision could be overtaken by the requirements of the US legislation.¹⁴⁹ Such decision contains a crucial part for the balance of interest scheme. For a privacy and national security tradeoff to constitute a balanced exchange within the spectrum of proportionality, the notion of adequate level of protection establishes the mitigating effect.¹⁵⁰ The US public authorities were not bound by the Safe Harbor decision, only self-certified US organizations receiving personal data from the EU, consequently, putting EU citizens' personal data even at greater risk.¹⁵¹

Upon such regulatory landscape the CJEU made consequent considerations of the questions requested by the High Court of Ireland. Regarding the powers of national supervisory authority¹⁵² specifically in the respect of such cross-border transfers, the CJEU noted importance of the monitoring of compliance with the Directive 95/46/EC with a complete independence when fundamental rights of an individual are in the risk of breach.¹⁵³ The CJEU mentioned that the requirement of such independent investigation (and thus authority) derives from the primary law, namely, Article 8(3) of the EUCFR,¹⁵⁴ which aim is to foster effective and reliable monitoring of compliance.¹⁵⁵ Consequently, strengthening individual's protection against such breaches of personal data.¹⁵⁶ Outlining that the DPC's Community Law approach not to investigate further was incorrect.

Thus, the CJEU introduced necessity of an application of a proportionality principle.¹⁵⁷ From the triad of players, the CJEU draw importance of insurance fair balance between movement

¹⁴⁹ Safe Harbor decision.

¹⁵⁰ Namely, one could agree on the interception of personal data if such activities possess needed safeguarding mechanisms, for example, possessing access to specific personal information that the data controller is holding. Moreover, the principle of proportionality was supported via additional principles established within the Safe Harbor decision including: notice – notifying an individual of the purpose of collecting data. this principle would adhere to the transparency principle described above (*See* chapter on privacy); choice – offering individual a choice to disclose such information to third party; onward transfer – the transferring agency shall assert whether the third party abides by the Safe Harbor decision; security – agency transferring data shall make reasonable precaution measures in order to secure data; data integrity – personal data transferred must be relevant to the aim; access – individual shall have access to the personal data that is being used by the agency; enforcement – effective privacy protection mechanism. Article 3 of Safe Harbor Decision. *See* Annex 11.

¹⁵¹ Thus, it is crucial to note the triad relationship that emerge within the Safe Harbor decision, namely, the privacy and national security dialog is interrupted by the commercial needs of the US and the EU, where Annex I of Safe Harbor decision notes: “The Principles were developed in consultation with industry and the general public to facilitate trade and commerce between the United States and European Union.” Hence, the balancing act becomes more diverse. The CJEU in its inherent nature, has always sought to foster the initial main goal of the EU – a single market, where the interest of commerce play a crucial role. Moreover, noting that personal data is one of the 21st century's financial instruments. However, via its case law on fundamental rights, the CJEU has also strongly stepped into the field of protection of human rights. Safe Harbor decision.

¹⁵² That of the EU Member States.

¹⁵³ Especially, in the instances where the complaint is lodged. Maximillian Schrems v. Data Protection Commissioner (Schrems I), §40;§53.

¹⁵⁴ *See* cases European Commission v. Republic of Austria, No. Case C- 614/10 (CJEU October 16, 2012), §36; European Commission v. Hungary, No. Case C- 288/12 (CJEU April 8, 2014), §47.

¹⁵⁵ Maximillian Schrems v. Data Protection Commissioner (Schrems I), §41.

¹⁵⁶ *Ibid.* *See* by analogy, judgment in Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others, No. Joined Cases C- 293/12 and C- 594/12 (CJEU April 8, 2014), §68.

¹⁵⁷ Maximillian Schrems v. Data Protection Commissioner (Schrems I), §42.

of personal data and observance of one's privacy.¹⁵⁸ To struck such fair balance, the CJEU noted wide range of powers granted to the national authority, where one of the tasks of such was to intervene with an aim to impose temporary or definite ban of data processing (if in breach).¹⁵⁹ However, if the authority after examining the claim with all due diligence,¹⁶⁰ found it to be ill-founded, the individual must be able for further judicial remedies.¹⁶¹

Whilst examining the validity of the Safe Harbor decision, the CJEU noted that such is wasted in the adequacy of the level of protection,¹⁶² which definition was not contained in any of the regulative documents.¹⁶³ Moreover, the CJEU acknowledged that the US is not bound by the definitions of the EU legal order, however, the protection level must be adequate in the light of the US domestic law or its international commitments, that would be equivalent to those in the EU.¹⁶⁴ Thus, the examination of such domestic rules shall be assessed by the Commission.¹⁶⁵

In the assessment of the principles laid by the Safe Harbor decision,¹⁶⁶ the CJEU noted that national security measures within such framework from the perspective of the US takes primacy, namely, constituting a derogation.¹⁶⁷ Nevertheless, such derogation shall be clearly regulated.¹⁶⁸ The CJEU also noted upon the establishment of interference with one's privacy, stating the interference shall not necessarily bear adverse consequences.¹⁶⁹ Therefore, it was not justifiable for the DPC to dismiss Schrems's claim solely on the grounds of insufficient evidence.

The CJEU observed that the Safe Harbor decision did not include any references to the US legislation that would intend to limit any interference with one's privacy, also not referring to the existence of an effective legal framework available in the US.¹⁷⁰ Contrary, the Safe Harbor decision solely addressed commercial nature disputes which could not be applied to such referring to the infringement of fundamental rights.¹⁷¹ Moreover, the CJEU noted that the Commission in its own assessment in 2013 found that US access to personal data was beyond the necessity and disproportionate to the protection of national security.¹⁷²

¹⁵⁸ *Ibid.*

¹⁵⁹ Maximillian Schrems v. Data Protection Commissioner (Schrems I), §43.

¹⁶⁰ Maximillian Schrems v. Data Protection Commissioner (Schrems I), §63.

¹⁶¹ In current case, where the DPC failed to exercise its investigative and protection obligations under the Directive 95/46/EC, Schrems correctly, thus, referred issues to the High Court of Ireland. However, it must be noted that when interpreting Article 3 of the Safe Harbor decision, the CJEU found that it actually denies national authorities to ensure the compliance with Article 25 of the Directive 95/46/EC namely, to assess adequate level of protection, thus exceeding its power shall be *Seen* as invalid. Maximillian Schrems v. Data Protection Commissioner (Schrems I), §64.

¹⁶² Maximillian Schrems v. Data Protection Commissioner (Schrems I), §68.

¹⁶³ Maximillian Schrems v. Data Protection Commissioner (Schrems I), §70.

¹⁶⁴ The CJEU acknowledged that the resources, connections and purpose of ensuring such level may differ, nevertheless, in practice must be an effective and the protection must be equivalently guaranteed). Maximillian Schrems v. Data Protection Commissioner (Schrems I), §§73-74.

¹⁶⁵ Maximillian Schrems v. Data Protection Commissioner (Schrems I), §75.

¹⁶⁶ Safe Harbor decision implied seven main principles: notice; choice; onwards transfer; access; security; data integrity; enforcement.

¹⁶⁷ Maximillian Schrems v. Data Protection Commissioner (Schrems I), §86.

¹⁶⁸ *Ibid.*

¹⁶⁹ Maximillian Schrems v. Data Protection Commissioner (Schrems I), §87.

¹⁷⁰ Maximillian Schrems v. Data Protection Commissioner (Schrems I), §88.

¹⁷¹ Maximillian Schrems v. Data Protection Commissioner (Schrems I), §89.

¹⁷² Maximillian Schrems v. Data Protection Commissioner (Schrems I), §90.

Thus, regarding the protection of individual's privacy within the context of Article 7 and Article 8 of the EUCFR,¹⁷³ the CJEU observed that especially in circumstances where personal data faces automated processing, its threshold of safeguard increases.¹⁷⁴ Consequently, the derogations or limitations of protection of such rights shall be strictly necessary.¹⁷⁵ Regarding the nature of a mass surveillance, the CJEU noted that regulatory framework allowing mass surveillance is in essence contrary to the right to privacy.¹⁷⁶ The CJEU concluded, as the Safe Harbor decision did not establish whether the US ensures an adequate level of protection, including remedies available to the individual, thus, its Article 1,¹⁷⁷ shall be seen as invalid, namely, not ensuring adequate level of protection.¹⁷⁸ Hence, concluding that Safe Harbor decision was invalid.¹⁷⁹

From the judgement and analysis of the CJEU, there were no direct references to the proportionality test explained above¹⁸⁰ rather a broad application of the proportionality principle. One of the factors not employing strict proportionality's test is the essence of the preliminary questions, where the CJEU lays grounds for its interpretation of the EU regulations at dispute. Nevertheless, the assessment of the US insurance of an adequate level of protection in broader perspective addresses proportionality principle. The CJEU concluded that the lack of strictly regulated derogations and limitations (for example, national security safeguard) of the right to privacy was contrary to Article 7 and Article 8 of the EUCFR, hence, noting that the aim of such mass surveillance activities were not recognized by the EU Law.¹⁸¹ Consequently, other steps of a proportionality test fall behind, moreover, mentioning that the compromising nature of the mass surveillance in connection of not possessing the adequate means of protection cannot be seen appropriate.¹⁸² Overall concluding that the major loophole of the invalidity of Safe Harbor decision, was inadequate regulatory framework and consequent ill-practice exercised by the US.¹⁸³ The lack of legitimate ground of derogations or limitations, thus fostered disproportionate measures taken by the US intelligence agencies (that could be taken only if strictly necessary) and infringing one's

¹⁷³ Article 7 and Article 8 of the EUCFR. *See* Annex 2.

¹⁷⁴ Maximillian Schrems v. Data Protection Commissioner (Schrems I), §91.

¹⁷⁵ Maximillian Schrems v. Data Protection Commissioner (Schrems I), §92.

¹⁷⁶ CJEU noted: "legislation permitting the public authorities to have access on a generalised basis to the content of electronic communications must be regarded as compromising the essence of the fundamental right to respect for private life." Maximillian Schrems v. Data Protection Commissioner (Schrems I), §94. The author agrees with a conclusion that it truly compromises fundamental right of privacy, nevertheless, believes in a compromise, where the mitigating factors shall be placed to constitute a fair trade, such as an effective safeguarding mechanism, employing principles described above. *See* Chapter "Concept of private life in realm of mass surveillance."

¹⁷⁷ Article 1 of the Safe Harbor decision. *See* Annex 11.

¹⁷⁸ Maximillian Schrems v. Data Protection Commissioner (Schrems I), §98.

¹⁷⁹ Maximillian Schrems v. Data Protection Commissioner (Schrems I), §106.

¹⁸⁰ *See* Chapter "Governing mass surveillance and privacy."

¹⁸¹ Maximillian Schrems v. Data Protection Commissioner (Schrems I), §91.

¹⁸² Maximillian Schrems v. Data Protection Commissioner (Schrems I), §94.

¹⁸³ Even though the Safe Harbor decision regards a commercial practice between the US and the EU, the organizations possessing such information within the US faced internal surveillance (*See* above facts of the case), where the EU citizens' data was exposed to the risk of being breached. As the public authorities of the US were not required to comply with Safe Harbor decision, personal data was exposed to the interception of the US intelligence agencies, especially, through the PRISM and Upstream surveillance programs. As follows from the background of the Schrems I case, Facebook Ireland was the controller and the processor of the personal data of the EU citizens', which was consequently outsourced by Facebook, Inc (the US company).

privacy. The matter of the legitimacy of such actions, consequently, was established as being invalid.¹⁸⁴

2.3. Implications of the Schrems I

The CJEU decision in Schrems I constituted a ground for a greater protection for the right to private life and personal data of the EU citizen's via ruling in favor in the balance game of the right to privacy (not the commercial interests).¹⁸⁵ After the Safe Harbor decision was found to be invalid, new debates on applicable framework begun. The European Article 29 Working Party – working party that dealt with protection of privacy and personal data until establishment of the GDPR – noted that the new framework should include following (based on the CJEU judgment): clear, precise and accessible rules; proof of necessity and employed proportionality; independent supervision; effective remedies.¹⁸⁶ Additionally, expressing the importance of reforming the US domestic legislation in order to ensure a ground for effective remedies in case of a breach of privacy.¹⁸⁷

Notwithstanding judicial spectrum debates on way forward, a great amount of a confusion amongst all of the parties involved in trans-Atlantic data transfers after the invalidation of Safe Harbor decision rose, as such spectrum for some time was left without a unified governing mechanism and practical uncertainty.¹⁸⁸ More than 4 000 US companies in meantime of new data

¹⁸⁴ Maximillian Schrems v. Data Protection Commissioner (Schrems I).

¹⁸⁵ From the judicial spectrum of precedence significance, the Schrems I case has been perceived as the landmark decision for the EU data protection law, moreover, having a worldwide influence. For example, cited in the ECtHR case *Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland* concerning the prohibition of companies to process personal tax data, where the ECtHR found no violation on the freedom of expression. In respective case, the ECtHR noted the CJEU's balancing approach, noting that a fair balance between the interest of commerce and right to privacy shall be ensured by national supervisory authorities. This example also outlines the author's observation about the interlinkage between both judicial bodies, namely, the ECtHR and the CJEU (*See* privacy chapter). *Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland*, No. 931/13 (ECtHR [GC] June 27, 2017). *Joined Cases Tele2 Sverige AB v. Post- och telestyrelsen and Secretary of State for the Home Department v. Watson* – concerning a mass surveillance of electronic communications with an objective to public security by fighting a crime (preliminary ruling at the CJEU). The CJEU also found a violation to right to privacy and data protection. When citing Schrems I, specifically, outlining the independent control of national authorities, which constitutes an essential element of protection. *Tele2 Sverige AB v. Post- och telestyrelsen and Secretary of State for the Home Department v Tom Watson and Others*, No. *Joined Cases C-203/15 and C-698/15* (CJEU December 21, 2016). *See also* *Puttaswamy v. Union of India (II)* – concerning a natural persons' identification number (personal data) use in a welfare scheme, which was challenged as being intrusive in one's privacy. The Supreme Court of India held that such scheme was constitutional, as it possessed a legitimate aim, necessity and proportionality. In its decision, it outlined that the CJEU interpretation of proportionality principle, where the derogations or limitations on the right to privacy shall only apply if strictly necessary. *Justice K.S.Puttaswamy v. Union of India*, No. 494 (Supreme Court of India).

¹⁸⁶ Article 29 Working Party. "Opinion 03/2015 on the Draft Directive on the Protection of Individuals with Regard to the Processing of Personal Data by Competent Authorities for the Purposes of Prevention, Investigation, Detection or Prosecution of Criminal Offences or the Execution of Criminal Penalties, and the Free Movement of Such Data." December 1, 2015. Available on: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2015/wp233_en.pdf. Accessed April 10, 2023.

¹⁸⁷ *Ibid.*

¹⁸⁸ *Ibid.*

protection agreement, relied on such mechanisms as Binding Corporate Rules or Standard Contractual Clauses.¹⁸⁹

The EU-US possess close economic ties. At the time of Safe Harbor the trade flow values were estimated to be over 1 trillion US dollars¹⁹⁰ annual and for each economy stock investment were estimated to be close to 4 trillion US dollars,¹⁹¹ Notably, data flows, particularly personal data, were one of the key drivers of such economic progress.¹⁹² Hence, the decision imposed some economic burdens for cross-data flows, nonetheless, urged companies to comply with upcoming regulations in order to continue their commercial activities using data.¹⁹³

Even though this case directly concerned a dispute between an individual and a state, it had major geopolitical influence.¹⁹⁴ From the perspective of international relations, self-evidently – impacting relationships among the US and the EU. The US Secretary of Commerce Penny Pritzker after the Schrems I decision stated:

We are deeply disappointed in today’s decision (...) which creates significant uncertainty for both U.S. and EU companies and consumers, and puts at risk the thriving transatlantic digital economy.¹⁹⁵

Rather showcasing negative attitudes towards the CJEU decision, and putting in forefront the commercial interest of both parties then the actual advancement of the fundamental rights of the EU citizens’. Such two different perspectives are explainable by the nature of the parties, where the US internally create a liberal market economy for data flows and does not establish a robust privacy protection mechanisms, additionally, not caring a lot about the foreigners’ well-being, whilst the EU cherishes the advancement of human right also in digital age establishing coordinate market economy.

The CJEU in its decision clearly noted that when personal data is transferred, rules governing such activity shall be clear and precise, imposing adequate safeguards, especially, in

¹⁸⁹ Shara Monteleone and Laura Puccio, “From Safe Harbour to Privacy Shield. Advances and Shortcomings of the New EU-US Data Transfer Rules,” January 2017, Available on: [https://www.europarl.europa.eu/RegData/etudes/IDAN/2017/595892/EPRS_IDA\(2017\)595892_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/IDAN/2017/595892/EPRS_IDA(2017)595892_EN.pdf). Accessed April 10, 2023.

¹⁹⁰ Think Tank, European Parliament. “US: Economic Indicators and Trade with the EU.” Available on: [https://www.europarl.europa.eu/thinktank/en/document/EPRS_ATA\(2016\)583777](https://www.europarl.europa.eu/thinktank/en/document/EPRS_ATA(2016)583777). Accessed April 10, 2023.

¹⁹¹ Marc Rotenberg, “Examining the EU Safe Harbor Decision and Impacts for Transatlantic Data Flows,” SSRN Scholarly Paper (Rochester, NY, November 3, 2015), <https://papers.ssrn.com/abstract=3651256>.

¹⁹² *Ibid.*

¹⁹³ Monteleone and Puccio, “From Safe Harbour to Privacy Shield. Advances and Shortcomings of the New EU-US Data Transfer Rules.”

¹⁹⁴ Renata Mieñkowska-Norkiene, “The Political Impact of the Case Law of the Court of Justice of the European Union,” *European Constitutional Law Review* 17, no. 1 (2021): 1–25, <https://doi.org/10.1017/S1574019621000080>.

¹⁹⁵ Further stating:” [T]he decision does not credit the benefits to privacy and growth that have been afforded by this Framework over the last 15 years. (...). [T]housands of U.S. and EU businesses that have complied in good faith with the Safe Harbor and provided robust protection of EU citizens’ privacy in accordance with the Framework’s principles (...).” Department of Commerce. “Statement From U.S. Secretary of Commerce Penny Pritzker on EU-U.S. Privacy Shield,” February 2, 2016. Available on: <https://2014-2017.commerce.gov/news/press-releases/2016/02/statement-us-secretary-commerce-penny-pritzker-eu-us-privacy-shield.html>. Accessed April 10, 2023. See also John Milko and Mieke Eoyang, “Congress Should Lay Out the Welcome Mat for Whistleblowers” (Third Way, 2018), JSTOR, <http://www.jstor.org/stable/resrep20151>.

cases of ADM processes to be considered as proportionate and legitimate.¹⁹⁶ Hence a new data transfer agreement between the US and the EU was established, known as Privacy Shield, however, not without loopholes.

2.4. Facts of the Schrems II case

After the Scherms I decision, negotiations among the US and the EU begun with an aim to establish new framework, that would advance the safeguards of the protection of privacy and personal data and close the gap highlighted by the Safe Harbor decision invalidation.

Amongst the political debates, Schrems continued his fight for even more robust privacy safeguards. Upon the Scherms I decision the High Court of Ireland annulled rejection of Schrems's complaint, consequently, referring it back to the DPC.¹⁹⁷ In the investigation stage the Facebook Ireland noted that the transfer of personal data to the Facebook, Inc was based on the SCC decision.¹⁹⁸ Thus, the DPC requested Schrems to reformulate his complaint,¹⁹⁹ where he consequently claimed that the US law required the transferred personal data to be available to public authorities (including NSA and FBI).²⁰⁰ Schrems on 1 December 2015 claimed that his personal data was used, thus, in various surveillance programs that went against Article 7 and Article 8 of the EUCFR (and Article 47 of the EUCFR) as the SCC decision could not justify such transfers,²⁰¹ hence, requesting the DPC to ban transfer of his personal data to Facebook Inc.²⁰²

Upon the investigation the DPC concluded that EU citizens personal data most likely were processed by the US public authorities in a manner incompatible with fundamental rights referred above as the US legislation did not provide the EU citizens with legal remedies under Article 47 of the EUCFR.²⁰³ The US public authorities were allowed to access personal data transferred to the US based on, *inter alia*, Section 702 of the FISA²⁰⁴ (which provides basis for PRISM²⁰⁵ and

¹⁹⁶ Maximillian Schrems v. Data Protection Commissioner (Schrems I).

¹⁹⁷ Data Protection Commissioner v. Facebook Ireland Limited and Maximillian Schrems, No. Case C-311/18 (CJEU July 16, 2020), §54. (Schrems II).

¹⁹⁸ Data Protection Commissioner v. Facebook Ireland Limited and Maximillian Schrems (Schrems II), §54. 2010/87/: 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 (notified under document C(2010) 593) (Text with EEA relevance), 039 OJ L § (2010). Available on: <http://data.europa.eu/eli/dec/2010/87/oj/eng>. Accessed February 23, 2023. (SCC decision).

¹⁹⁹ Data Protection Commissioner v. Facebook Ireland Limited and Maximillian Schrems (Schrems II), §54.

²⁰⁰ Data Protection Commissioner v. Facebook Ireland Limited and Maximillian Schrems (Schrems II), §55.

²⁰¹ *Ibid.*

²⁰² *Ibid.*

²⁰³ Data Protection Commissioner v. Facebook Ireland Limited and Maximillian Schrems (Schrems II), §56 Especially, regarding the Fourth Amendment of the Constitution of the US, which allows to challenge unlawful surveillance, however, only applying to nationals. Thus, putting on locus standi burden upon the EU citizens. Data Protection Commissioner v. Facebook Ireland Limited and Maximillian Schrems (Schrems II), §65.

²⁰⁴ Section 702 of FISA. *See* Annex 12.

²⁰⁵ Which required internet service providers to supplement NSA; FBI and CIA with collected personal data. *See* Annex 8. Data Protection Commissioner v. Facebook Ireland Limited and Maximillian Schrems (Schrems II), §61.

Upstream²⁰⁶ surveillance programs) and on E.O. 12333.²⁰⁷ Moreover, noting that SCC decision regulating standard protection clauses were not able to remedy such defect as they only regarded commercial activities, not activities conducted by the US public authorities.²⁰⁸ Thus, the DPC banned trans-Atlantic data transfers to the US under Article 4 of the SCC Decision.²⁰⁹ Moreover, upon its findings and reformulated Schrems's claim, the DPC on 31 May 2016 referred matter to the High Court of Ireland in order to request a preliminary ruling of the CJEU,²¹⁰ which contained various matters (together 11 preliminary questions),²¹¹ where two key issues were raised:

- 1) whether the SCC used by the Facebook Inc were violating Articles 7, 8 and 47 of the EUCFR (specifically, mentioning, whether the limitations imposed by the US law on the available remedies are proportionate within the meaning of Article 52 of the EUCFR,²¹² thus constituting adequate level of protection)²¹³ and;
- 2) if not, whether the Privacy Shield decision provided adequate level of safeguards for the protection of data transferred.²¹⁴

When examining both principal issues, the author concentrates on the second issue where the CJEU expressly employs the proportionality principle. Notwithstanding the preliminary rulings referred to the CJEU, on 3 October 2017 the High Court of Ireland in its judgement in essence hold that the US domestic surveillance laws allowed mass surveillance²¹⁵ of the EU citizens' personal data.²¹⁶

2.5. CJEU approach in Schrems II – finding proportionality

²⁰⁶ Establishing telecommunication surveillance, where the NSA was allowed to *See* the personal data flows and acquire information about foreigners' personal data (accessing metadata and content of the communications). Data Protection Commissioner v. Facebook Ireland Limited and Maximillian Schrems (Schrems II), §62.

²⁰⁷ Data Protection Commissioner v. Facebook Ireland Limited and Maximillian Schrems (Schrems II), §60-61. E.O. 12333 allowed NSA to access data in transit, namely, collecting any data before entering in the US. Data Protection Commissioner v. Facebook Ireland Limited and Maximillian Schrems (Schrems II), §63.

²⁰⁸ Data Protection Commissioner v. Facebook Ireland Limited and Maximillian Schrems (Schrems II), §56.

²⁰⁹ Article 4 of SCC decision. *See* Annex 13. Data Protection Commissioner v. Facebook Ireland Limited and Maximillian Schrems (Schrems II), §56.

²¹⁰ Data Protection Commissioner v. Facebook Ireland Limited and Maximillian Schrems (Schrems II), §57.

²¹¹ *See* Annex 14.

²¹² Article 7, Article 8 and Article 47 of the EUCFR. *See* Annex 2.

²¹³ The SCC decision was the primary concern of the High Court of Ireland outlining that: "Article 4 of the SCC decisions does not provide the answer (...) in relation to the remedial regime in the United States." Hence, concluding that the SCC Decision should be pronounced by the competent authority as invalid. Thus, preliminary rulings were requested. Data Protection Commissioner v. Facebook Ireland Ltd and Maximillian Schrems, No. 4809 (High Court of Ireland October 3, 2017), §340.

²¹⁴ Data Protection Commissioner v. Facebook Ireland Limited and Maximillian Schrems (Schrems II), §68.

²¹⁵ One of the disputing matters within a case was whether the US exercises mass surveillance. Schrems argued that all actions taken were to be characterized as mass surveillance (pursuant to the PRISM and Upstream programs), whilst the US and Facebook Inc claimed that the practice of surveillance was very targeted and was not indiscriminate, thus not constituting mass surveillance. *See* Data Protection Commissioner v. Facebook Ireland Ltd and Maximillian Schrems, §184.

²¹⁶ Data Protection Commissioner v. Facebook Ireland Ltd and Maximillian Schrems, §339.

Before delving into the analysis of the CJEU approach used in Schrems II, the author outlines applicable regulatory framework (it must be noted that the Schrems II concerned the same provision of the Directive 95/46/EC as in Schrems I, thus see above analysis).

The GDPR – Regulation of protection of natural persons’ data (enforce from 25 May 2018).²¹⁷ Article 23 of the GDPR specifically requests proportionate measures when a legislative restrictions on privacy are put in place, also referencing aim of national security.²¹⁸ Consequent respective Articles of the GDPR (Articles 44 to 50) regards transfer of personal data to third countries, here the main requirement is an adequate level of protection.²¹⁹ The High Court of Ireland in its request for preliminary ruling expressed clarification upon Article 46(1) and 46(2)(c) of the GDPR,²²⁰ former establishes need of appropriate safeguards; enforceable rights and effective legal remedies in a third countries, latter references SCC decision as appropriate safeguards.²²¹

The SCC decision – regulates standard contractual clauses covering a personal data transfer from the EU to third countries.²²² Article 1 of the SCC decision outlines that it is applicable to such data processors in a third country that are the established recipients.²²³ Consequently, highlighting obligations of data exporters and importers, mainly emphasizing that every action shall be done in accordance with law.²²⁴ The SCC decision allowed EUDPA to assess the protection level in the receiving state and ensure that the receiving state does not impose surveillance laws that go beyond what is necessary to safeguard national security.²²⁵ Even though the US is not a subject to EU Law, the EUDPA under the SCC decision allowed to suspend data transfer to the US, if the necessary safeguards were not met.²²⁶ Article 4 of the SCC decision referenced the EUDPA power to ban data flows in specified instances.²²⁷

The Privacy Shield decision – post Safe Harbor agreement between the US and the EU on an adequate safeguards of protection of protection of personal data in trans-Atlantic data transfers.²²⁸ The Privacy Shield decision’s aim was to close the loopholes of the Safe Harbor

²¹⁷ Is directly applicable to all EU Member States and replaces Directive 95/46/EC. GDPR.

²¹⁸ Article 23 of the GDPR. *See* Annex 1. Consequently noting that such derogating legislative measures shall contain specific provisions relating to:” (1) the purposes of the processing or categories of processing; (2) the categories of personal data; (3) the scope of the restrictions introduced; (4) the safeguards to prevent abuse or unlawful access or transfer; (5) the specification of the controller or categories of controllers; (6) the storage periods and the applicable safeguards taking into account the nature, scope and purposes of the processing or categories of processing; (7) the risks to the rights and freedoms of data subjects; and (8) the right of data subjects to be informed about the restriction, unless that may be prejudicial to the purpose of the restriction.” *Data Protection Commissioner v. Facebook Ireland Limited and Maximilian Schrems (Schrems II)*.

²¹⁹ GDPR.

²²⁰ Article 46(1) and Article 46(2)(c) of the GDPR. *See* Annex 1.

²²¹ GDPR.

²²² SCC decision.

²²³ Namely, commercial activity holders. *See* Annex 13.

²²⁴ *See* Annex 13.

²²⁵ Lawfare. “Geopolitical Implications of the European Court’s Schrems II Decision,” July 17, 2020. Available on: <https://www.lawfareblog.com/geopolitical-implications-european-courts-schrems-ii-decision>. Accessed April 10, 2023.

²²⁶ *See* Annex 13.

²²⁷ SCC decision.

²²⁸ It must be noted that the DPC or Ireland brought a case before the High Court of Ireland prior establishment of the Privacy Shield Decision. Nevertheless, the CJEU, noted that it shall take into account the consequences of the adoption of the Privacy Shield Decision (the same consideration was also used by the CJEU when referring to the GDPR and

decision – limit access for the US national security agencies of personal data of the EU citizens, possess safeguarding and supervisory mechanism.²²⁹ The Privacy Shield decision, establishing mutually agreed principles of personal data protection, thus was also a subject to the investigatory and enforcement powers of the US Federal Trade Commission, the Department of Transportation and other state bodies in order to ensure compliance.²³⁰ Consequently, the PPD-28 came into force – the US legislative act limiting signals intelligence operations (binding upon the US intelligence agencies).²³¹ Specifically, in Annex VI noting that the PPD-28 allowed for bulk interception, where such derogation is based on national security and public interest requirements.²³²

Upon established regulatory landscape the CJEU gave its judgement. Regarding the SCC decision's applicability to data transfers and compatibility with Articles 7, 8 and 47 of the EUCFR, the CJEU, firstly, noted that GDPR provision referenced are of the aim to maintain highly quality of personal data protection outside the EU confines.²³³ Thus, concluding that to the assessment of the level of protection afforded must be based on the bilateral arrangements, whether based on contractual clauses or relevant legal systems, and must be compatible of equivalent protection of personal data that is afforded by the EUCFR.²³⁴

Consequently, the CJEU directly addressed the issue of the SCC decision's compatibility of ensuring an adequate level of protection.²³⁵ The CJEU noted that it is a shared ground, that such contractual clauses are not binding upon public authorities as they are not a part of such agreements.²³⁶ Nevertheless, noting that there might be instances, where content of SCC would not constitute effective protection of personal data, for example, in instances where a third country allows public authorities to interfere with the transferred personal data, thus, establishing the question of the validity of SCC decision.²³⁷ Namely, the CJEU referred to the US, which under its

Data Protection Directives expiration). Such an approach was also taken by the High Court of Ireland which expressed that it shall take into account any amendment of a law in the interval of proceedings. Data Protection Commissioner v. Facebook Ireland Limited and Maximillian Schrems (Schrems II), §§ 151-153. 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 (notified under document C(2016) 4176) (Text with EEA relevance), 207 OJ L § (2016). Available on: http://data.europa.eu/eli/dec_impl/2016/1250/oj/eng. Accessed February 23, 2023. (Privacy Shield decision).

²²⁹ See analysis above. Article 1 of the Privacy Shield embedded the aim – to adequately safeguard personal data. See Annex 15.

Moreover, the Commissioner for Justice, Consumers and Gender Equality, Vera Jourová upon the draft of Privacy Shield decision expressed that the US in negotiations assured not to engage in indiscriminate mass surveillance and to provide adequate judicial remedies if breaches occurred. Monteleone and Puccio, "From Safe Harbour to Privacy Shield. Advances and Shortcomings of the New EU-US Data Transfer Rules," 16.

²³⁰ SCC decision.

²³¹ Presidential Policy Directive 28 (PPD-28) (2014). Available on: <https://www.dhs.gov/publication/presidential-policy-directive-28-ppd-28-signals-intelligence-activities>. Accessed April 1, 2023.

²³² Annex VI of the Privacy Shield decision. See Annex 15. Data Protection Commissioner v. Facebook Ireland Limited and Maximillian Schrems (Schrems II).

²³³ Data Protection Commissioner v. Facebook Ireland Limited and Maximillian Schrems (Schrems II), §93.

²³⁴ Also regarding the public authorities use of personal data. Data Protection Commissioner v. Facebook Ireland Limited and Maximillian Schrems (Schrems II), §§104-105.

²³⁵ The main loophole of such was its inapplicability to the public authorities. Data Protection Commissioner v. Facebook Ireland Limited and Maximillian Schrems (Schrems II), §123.

²³⁶ Data Protection Commissioner v. Facebook Ireland Limited and Maximillian Schrems (Schrems II), §125.

²³⁷ Data Protection Commissioner v. Facebook Ireland Limited and Maximillian Schrems (Schrems II), §126.

domestic provisions allowed mass surveillance.²³⁸ Thus, to ensure protection, the supplementary guarantees should be established.²³⁹ The CJEU noted Advocate General's Opinion in such matter, outlining that in such cases the responsibility of establishment of such supplementary measures lays within the controller or alternatively within the component EUDPA, hence, supplementing action shall be conducted on case-by-case basis.²⁴⁰ Such conclusion outlined that the mere fact that SCC decision does not bind the US public authorities does not necessarily invalidate the SCC decision.²⁴¹

Nevertheless, the CJEU expressed that the validity of such agreement in the light of Articles 46(1) and 46(2)(c) of the GDPR²⁴² depend on the possibility of such SCC decision to effectively in practice establishes mechanism to ensure the compliance with level of protection required by the EU Law and to monitor whether data flow is stopped in the event of a breach.²⁴³ Such responsibility falls within the data controller, recipient and processor, which mutually undertake to ensure such protection in accordance with regulations, specifically, the GDPR and the EUCFR,²⁴⁴ however, the controller (namely, the EUDPA) is responsible of verification of whether level of protection afforded is compatible with EU Law prior the transfer of personal data.²⁴⁵

Upon such considerations, the CJEU concluded that the SCC decision shall be seen as valid as it provides an effective mechanism to safeguard one's personal data, especially, as it possess control mechanism and for mitigating factors invites to establish needed supplementary safeguarding measures.²⁴⁶

With regard to the efficacy of the Privacy Shield decision in safeguarding fundamental rights, the CJEU engaged in a thorough application of the principle of proportionality to assess whether the protection provided of fundamental rights in essence is equivalent to the guaranteed in the EU.²⁴⁷ Privacy Shield decision showcased that one of the derogations from right to privacy is a national security interest, where such interference can be based on PRISM and Upstream

²³⁸ See Annex 12.

²³⁹ With an main aim to close the loophole of availability of personal data to the public authorities of the US. Data Protection Commissioner v. Facebook Ireland Limited and Maximillian Schrems (Schrems II), §§132-133.

²⁴⁰ However, from the author's perspective, such approach seems bureaucratically burdensome, as each individual company found in the US could not automatically rely on the SCC Decision, namely, on a bilateral agreement (not efficient). Data Protection Commissioner v. Facebook Ireland Limited and Maximillian Schrems (Schrems II), §134.

²⁴¹ Data Protection Commissioner v. Facebook Ireland Limited and Maximillian Schrems (Schrems II), §136.

²⁴² Article 46(1) and Article 46(2)(c) of the GDPR. See Annex 1.

²⁴³ Data Protection Commissioner v. Facebook Ireland Limited and Maximillian Schrems (Schrems II), §137.

²⁴⁴ Data Protection Commissioner v. Facebook Ireland Limited and Maximillian Schrems (Schrems II), §138.

²⁴⁵ Data Protection Commissioner v. Facebook Ireland Limited and Maximillian Schrems (Schrems II), §142.

²⁴⁶ Where the EUDPA is authorized to suspend or prohibit transfer of data in with it deems such to be incompatible with the EU Laws. Data Protection Commissioner v. Facebook Ireland Limited and Maximillian Schrems (Schrems II), §§148-149.

²⁴⁷ Prior to assessing the validity of the Privacy Shield Decision, the CJEU noted that it is binding upon the US and the EUDPA Similarly as regards the SCC Decision are the ones to find whether the US ensures an adequate level of protection, consequently, allowing or prohibiting data transfers. Such observation is wasted in the framework of conclusions made by the CJEU in the Schrems I case, namely, regarding the obligations of supervisory authorities (*inter alia*, to conduct an independent investigation). Nevertheless, concluding that whilst the CJEU examines the validity of the Privacy Shield Decision, the EUDPA are not entitled to suspend data flows on grounds of inadequate safeguards provided by the US legislation. Data Protection Commissioner v. Facebook Ireland Limited and Maximillian Schrems (Schrems II), §§154-157;§162.

surveillance programs under the US domestic law - Section 702 of the FISA and E.O. 12333.²⁴⁸ Such action could be conducted in the light of established principles and only exercised when strictly necessary and with effective legal remedies (drawing on the judgment of Schrems I).²⁴⁹

The CJEU noted that the transfer of personal data and its subsequent processing of a third party, *inter alia*, public authority is an interference with one's right to privacy and protection of personal data as constituted by Article 7 and 8 of the EUCFR, hence must meet the data protection requirements.²⁵⁰ Notably, the CJEU expressed that right to privacy and protection of personal data are not an absolute rights,²⁵¹ thus require examination of their function in society.²⁵² Regarding the personal data processing, the CJEU noted that it must be done for: "specified purposes (...) on the basis of the consent (...) or some other legitimate basis laid down by law."²⁵³ Thus, alongside principle of proportionality requiring to abide by principle of consent; principle of legality, lawfulness and legitimacy and principle of transparency.

The CJEU examined Article 7 and 8 of the EUCFR in the light of Article 52(1) of the EUCFR²⁵⁴ which governs derogations from fundamental rights,²⁵⁵ where it directly mentions application of principle of proportionality when assessing whether exercised derogations meets necessary and genuine objectives of the subjected interests.²⁵⁶ The CJEU further noted that a second key concept for the proportionality principle, is the lawfulness of such derogations.²⁵⁷ Lastly outlining that requirements of proportionality must meet the threshold of a strict necessity, consequently, the legislation governing such shall be clear and precise and shall showcase minimum safeguards (especially, concerning availability of judicial remedies), additionally, noting that such approach shall be taken especially in the cases of ADM processes.²⁵⁸

When assessing the Privacy Shield decision's compatibility with such proportionality requirements, the CJEU noted that Section 702 of the FISA and E.O. 12333 allowing mass

²⁴⁸ See Annex 12. "Executive Order 12333" (1981), <https://www.archives.gov/federal-register/codification/executive-order/12333.htm> Executive Order 12333 of December 4, 1981. Available on: <https://dpcl.d.defense.gov/Portals/49/Documents/Civil/eo-12333-2008.pdf>. Accessed February 23, 2023.1. (E.O. 12333).

²⁴⁹ Data Protection Commissioner v. Facebook Ireland Limited and Maximillian Schrems (Schrems II), §§165-167. This Privacy Shield Decision perspective was objected by the High Court of Ireland rising its doubts over the established domestic legislation for limiting such derogations, outlining that such does not ensure effective judicial protection, adding that the establishment of Privacy Shield Ombudsperson cannot close the existing gap of available judicial remedies. Data Protection Commissioner v. Facebook Ireland Limited and Maximillian Schrems (Schrems II), §168.

²⁵⁰ Data Protection Commissioner v. Facebook Ireland Limited and Maximillian Schrems (Schrems II), §§170-171. The CJEU drew such stance on a case-law, such as judgments Volker und Markus Schecke GbR (C-92/09) and Hartmut Eifert (C-93/09) v. Land Hessen, No. Joined cases C-92/09 and C-93/09 (CJEU November 9, 2010), §§49-52; Rechnungshof (C-465/00) v. Österreichischer Rundfunk and Others and Christa Neukomm (C-138/01) and Joseph Lauerermann (C-139/01) v. Österreichischer Rundfunk, No. Joined cases C-465/00, C-138/01, C-139/01 (CJEU May 20, 2003), §29.

²⁵¹ Namely, are not such rights from which any form of derogation is prohibited.

²⁵² Data Protection Commissioner v. Facebook Ireland Limited and Maximillian Schrems (Schrems II), §172.

²⁵³ Data Protection Commissioner v. Facebook Ireland Limited and Maximillian Schrems (Schrems II), §173.

²⁵⁴ Article 52(1) of the EUCFR. See Annex 2.

²⁵⁵ Data Protection Commissioner v. Facebook Ireland Limited and Maximillian Schrems (Schrems II), §174.

²⁵⁶ *Ibid.*

²⁵⁷ Data Protection Commissioner v. Facebook Ireland Limited and Maximillian Schrems (Schrems II), §175.

²⁵⁸ Data Protection Commissioner v. Facebook Ireland Limited and Maximillian Schrems (Schrems II), §176.

surveillance²⁵⁹ rises doubts over the US compatibility to ensure the same level of personal data and privacy protection equivalent to such in the EU.²⁶⁰

The CJEU noted that the Privacy Shield established that the US public authorities authorizes mass surveillance programs, such as PRISM or Upstream rather than individual targeted surveillance measures, thus not covering assessment of whether the individual in the mass surveillance programs are properly being intercepted to acquire foreign intelligence information.²⁶¹ Therefore, concluding that Section 702 of the FISA does not indicate any limitations on the power of derogation, such as limitations on the implementations of surveillance programs.²⁶² Thus not being able to ensure equivalent protection to the EUCFR as it falls short on satisfying one of the components of the proportionality principle – strict necessity – which requires to possess such regulation that imposes limitations on derogations, are clear and precise and provide minimum safeguards.²⁶³

It was established that the PPD-28 does not grant EU citizens a possibility to bring a claim before the US courts, if the rights of privacy are infringed (also not available under E.O. 12333),²⁶⁴ thus outlining that the protection granted is incompatible with one provided in the EU in the context of effective and enforceable rights.²⁶⁵ Moreover, adding that the findings upon the E.O. 12333 permitting mass surveillance program without any judicial review makes it burdensome to determine the amount of personal data being collected and the aim of such collection, hence showcasing ambiguity and potential risk of breach of privacy.²⁶⁶ Overall concluding that neither of the US domestic regulatory provisions provides minimum safeguards, hence not meeting the principle of proportionality principle, namely, the legal grounds are not limited to strict necessity.²⁶⁷ Thus, the Privacy Shield decision was announced to be invalid in its entirety.²⁶⁸

2.6. Implications of the Schrems II

The CJEU truly via both decisions, Schrems I and Schrems II – invalidating such trans-Atlantic data transfers that are not up to the standards of the EU fundamental rights safeguarding mechanism, outlined the EU priority – protection of privacy and personal data. Such consistent approach, also showcases the EU's international influence and power of possessing strong framework of digital sovereignty, which was embraced by the President of the European Commission, Ursula von der Leyen, who has emphasized the importance of digital sovereignty for

²⁵⁹ See Annex 12. E.O. 12333.

²⁶⁰ Data Protection Commissioner v. Facebook Ireland Limited and Maximilian Schrems (Schrems II), §178.

²⁶¹ Data Protection Commissioner v. Facebook Ireland Limited and Maximilian Schrems (Schrems II), §179.

²⁶² *Ibid.*

²⁶³ Data Protection Commissioner v. Facebook Ireland Limited and Maximilian Schrems (Schrems II), §180.

²⁶⁴ Data Protection Commissioner v. Facebook Ireland Limited and Maximilian Schrems (Schrems II), §182.

²⁶⁵ Data Protection Commissioner v. Facebook Ireland Limited and Maximilian Schrems (Schrems II), §181.

²⁶⁶ Data Protection Commissioner v. Facebook Ireland Limited and Maximilian Schrems (Schrems II), §183.

²⁶⁷ The CJEU further concluded that there is also a lack of judicial redress, namely, a lack of an effective remedy in case of breach of the right to privacy. Data Protection Commissioner v. Facebook Ireland Limited and Maximilian Schrems (Schrems II), §184.

²⁶⁸ Data Protection Commissioner v. Facebook Ireland Limited and Maximilian Schrems (Schrems II), §200.

Europe's perspective.²⁶⁹ Both cases have illuminated pro-privacy camp, swinging the pendulum in favor of the fundamental rights. Via the CJEU approach mass surveillance as a concept has undergone a major scrutiny, firstly, by the Schrems I decision regarding such as “inherently evil”, namely, in its nature jeopardizing right to privacy, secondly, by the Schrems II decision outlining harsh path of establishing a mutually benefiting agreement.²⁷⁰ The author holds view that there must be a middle ground found, which would not jeopardize neither of the thoughts (neither pro-surveillance nor pro-privacy camps) and rather uphold both needs and interest.²⁷¹

Similarly to the Schrems I also the Schrems II had practical implications for companies engaged in transatlantic data transfers, as they no longer were able to conduct their activities based on the Privacy Shield decision. Those still practicing such transfer, according to Article 83(5)(c) of the GDPR faced penalty of 20 million EUR or 4% of their global turnover.²⁷² The judgment also led to a demand for higher levels of corporate transparency reports in the US, further complicating the determination of what constitutes adequate supplementary measures for SCCs.²⁷³ As such, the Schrems II ruling caused considerable uncertainty for businesses and highlighted the need for clearer and more consistent regulations governing cross-border data transfers.²⁷⁴

²⁶⁹ Frances G. Burwell and Kenneth Propp, “The Search for Digital Sovereignty,” *Digital Sovereignty in Practice*: (Atlantic Council, 2022), JSTOR, <http://www.jstor.org/stable/resrep44035.4>; Andrea Ratiu, “The European Union and the Search for Digital Sovereignty: Building ‘Fortress Europe’ or Preparing for a New World?,” *Atlantic Council* (blog), June 22, 2020. Available on: <https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/the-european-union-and-the-search-for-digital-sovereignty/>. Accessed April 10, 2023.

²⁷⁰ Claes Gustav Granmar, “A Reality Check of the Schrems Saga,” SSRN Scholarly Paper (Rochester, NY, January 3, 2022), <https://papers.ssrn.com/abstract=4000713>.

²⁷¹ Such author’s view is also based on a fast technological advancement track, which needs to possess freedom for development, nevertheless, author strongly agrees that within such progress human rights shall be adequately safeguarded, therefore, there is a need of certain level of transparency and societal knowledge within such technical spectrum to close above expressed technical illiteracy’s black box.

²⁷² GDPR. Data controllers also were affected, as they have to conduct additional tests and bureaucratic procedures to ensure compliance with the GDPR's requirements for adequate protection of personal data, mostly via the SCC decision. Kenneth Propp, “Transatlantic Data Transfers” (Council on Foreign Relations, 2021), JSTOR, <http://www.jstor.org/stable/resrep29990>.

²⁷³ As the CJEU noted: “The assessment of the level of protection afforded by a third country or a territory or a processing sector within a third country must be based on all the relevant aspects of the legal system and the practice in place in the third country or the processing sector in that country.” *Data Protection Commissioner v. Facebook Ireland Limited and Maximilian Schrems (Schrems II)*, §202.

²⁷⁴ Hence, guidelines of further approach were drafted. In the author’s communication with the EDPS, it emphasized in more detail a practical implications on Schrems II, outlining that after Schrems II findings it started an investigation on the EU institution which processes personal data (namely, are the controllers of such process, thus are bound by the Schrems II) use of Microsoft Office 365 and found number of concerning areas of non-compliance with data protection, such as, lack of control, use of sub-processors (to which data is exposed); lack of proper safeguards. Hence, the EDPS has been advising EU institutions on renegotiation of their license agreements, outlining an increased activity also in a domestic realm, to safeguard data. Another action taken by the EDPS was a coordinated enforcement action of 2022 with an aim to focus on EU institution compliance with cloud-based services (one of the risk areas for mass surveillance). See European Data Protection Supervisor. “Data Protection and Use of Cloud by Public Sector: The EDPS Initiates and Participates in the 2022 Coordinated Enforcement Action of the EDPB,” May 23, 2023. Available on: <https://edps.europa.eu/press-publications/press-news/press-releases/2022/data-protection-and-use-cloud-public-sector-edps>. Accessed April 10, 2023; European Data Protection Board. “Frequently Asked Questions on the Judgment of the Court of Justice of the European Union in Case C-311/18 - Data Protection Commissioner v Facebook Ireland Ltd and Maximilian Schrems.” Available on: https://edpb.europa.eu/our-work-tools/our-documents/other/frequently-asked-questions-judgment-court-justice-european-union_en. Accessed April 10, 2023; European Data Protection Supervisor. “Outcome of Own-Initiative Investigation into EU Institutions’ Use of Microsoft Products and Services.”

The CJEU strong supranational influence, also extends outside its confines. The CJEU's strong geopolitical standing also grants it a power to be influential on an international level, mostly through the concept known as the Brussels Effect. Namely, fostering its regulative perspectives outside its confines and influencing other regions. For example, China – in technological and consequent regulatory approach – quite robust and sealed from international practices due to Chinese firewall framework was influenced also by the EU on GDPR, establishing Personal Information Protection Law. In words of Tim Wu, the EU has become an effective sovereign in the field of privacy, with an power to influence.²⁷⁵ Nevertheless, some also argue that the CJEU via Schrems II decision has also outlined the “exalting illusion” of imagining that the EU can expand its protection of personal data on global basis, due to the difficulty of such implementation in practice.²⁷⁶ However, regarding trans-Atlantic data transfer it awaits new era under the draft of a Trans-Atlantic Data Privacy Framework.²⁷⁷

Schrems II decision also had its implications for the international relations. The Privacy Shield Decision invalidation once again from the US perspective was seen as a deep disappointment which was expressed by the US Secretary of Commerce Wilbur Ross and US Secretary of State Mike Pompeo suggesting that the estimated loss would amount to 7.1 million US dollar loss within EU-US economic relationship.²⁷⁸ Consequently, expressing the need of further corporation to ensure smooth data flows for the economic growth, hence rather putting in fore front economic interests.²⁷⁹ European Parliament in its brief relating to the impact of Schrems II for international relations expressed that the ruling would have major impact to other third countries that exercise extensive mass surveillance, particularly emphasizing the UK's aspect of being treated as a third country after Brexit.²⁸⁰

Available on: <https://edps.europa.eu/data-protection/our-work/publications/investigations/outcome-own-initiative-investigation-eu>. Accessed April 10, 2023.

²⁷⁵ Jack Goldsmith and Tim Wu, “Who Controls the Internet?: Illusions of a Borderless World,” *Faculty Books*, January 1, 2006, 176, <https://scholarship.law.columbia.edu/books/175>.

²⁷⁶ Christopher Kuner, “Reality and Illusion in EU Data Transfer Regulation Post Schrems,” *German Law Journal* 18, no. 4 (2017): 910, <https://doi.org/10.1017/S2071832200022197>.

²⁷⁷ European Commission. “EU-U.S. Data Privacy Framework, Draft Adequacy Decision.” Text. Available on: https://ec.europa.eu/commission/presscorner/detail/en/qanda_22_7632. Accessed April 10, 2023; European Data Protection Supervisor. “EDPB Welcomes Improvements under the EU-U.S. Data Privacy Framework, but Concerns Remain.” Available on: https://edpb.europa.eu/news/news/2023/edpb-welcomes-improvements-under-eu-us-data-privacy-framework-concerns-remain_en. Accessed April 10, 2023.

²⁷⁸ Luxembourg, U. S. Mission. “U.S. Secretary of Commerce Wilbur Ross Statement on Schrems II Ruling and the Importance of EU-U.S. Data Flows.” U.S. Embassy in Luxembourg, July 16, 2020. Available on: <https://lu.usembassy.gov/u-s-secretary-of-commerce-wilbur-ross-statement-on-schrems-ii-ruling-and-the-importance-of-eu-u-s-data-flows/>. Accessed April 10, 2023.

²⁷⁹ *Ibid.*

²⁸⁰ “The CJEU Judgment in the Schrems II Case | Think Tank | European Parliament,” accessed May 9, 2023, [https://www.europarl.europa.eu/thinktank/en/document/EPRS_ATA\(2020\)652073](https://www.europarl.europa.eu/thinktank/en/document/EPRS_ATA(2020)652073).

3. ANALYSIS OF THE ECtHR JUDGMENT BIG BROTHER WATCH AND OTHERS V. THE UK

Alongside disputes at the CJEU, the ECtHR conducted its examination of mass surveillance implications in one's privacy via examining the UK's national perspective. The ECtHR stands in a different spectrum than the CJEU, thus the consequent analysis illuminates some interesting differences on the application of the principle of proportionality.

3.1. Facts of the Big Brother Watch case

The Big Brother Watch case is constituted upon three applications that find their origins in the UK after the Snowden revelations.²⁸¹ The UK domestically via the IPT²⁸² on December 2014, February 2015 and June 2015 examined alleged activities by Snowden, namely, being involved in the PRISM project and using Upstream program (also the TEMPORA), which allegedly was done by its intelligence services.²⁸³ The IPT at large sought to establish whether such activities were in compliance with the ECHR's Article 8 and Article 10.²⁸⁴

The first judgment of the IPT saw PRISM program activities as compatible with ECHR as the government revealed information to the public during a litigation process over an existing safeguarding system.²⁸⁵ Nevertheless, sparking question whether such protection framework was compatible with ECHR prior being known to the public.²⁸⁶ As the IPT lacked jurisdiction to assess claims brought by persons situated outside the UK,²⁸⁷ the first judgement regarding the legitimacy of conducting such surveillance activities of foreigners, hence was forwarded to the regional level.²⁸⁸

The second judgement (on the matter of public knowledge) was given, which found such safeguarding mechanisms as incompatible with the ECHR, as it was not disclosed to the public prior litigation process.²⁸⁹ The third judgement regarded question of whether applicants' data obtained under surveillance programs (PRISM and Upstream) by the UK intelligence agencies were in compliance with Article 8 and 10 of the ECHR.²⁹⁰ The IPT did not find in favor of eight out of ten applicants and did not confirm whether they have been intercepted by the UK

²⁸¹ Big Brother Watch and Others v. the United Kingdom.

²⁸² Established under Section 65(1) of RIPA and has a jurisdiction to hear cases brought by citizens of wrongful interference with communications. *See* Annex 16. Expert Participation, "Regulation of Investigatory Powers Act 2000" (200AD), <https://www.legislation.gov.uk/ukpga/2000/23/contents>. (RIPA).

²⁸³ Liberty/Privacy No 2 (The Investigatory Powers Tribunal December 5, 2014); Human Rights Watch Inc & Ors - And - The Secretary Of State For The Foreign & Commonwealth Office & Ors (The Investigatory Powers Tribunal May 16, 2016).

²⁸⁴ In the judicial proceedings at the ECtHR, the ECtHR received an acknowledgement from the NSA about the existence two surveillance programs – PRISM and Upstream. Liberty/Privacy No 2; Human Rights Watch Inc & Ors - And - The Secretary Of State For The Foreign & Commonwealth Office & Ors.

²⁸⁵ Liberty/Privacy No 2, §161.

²⁸⁶ Liberty/Privacy No 2.

²⁸⁷ Human Rights Watch Inc & Ors - And - The Secretary Of State For The Foreign & Commonwealth Office & Ors, §60.

²⁸⁸ Liberty/Privacy No 2.

²⁸⁹ Human Rights Watch Inc & Ors - And - The Secretary Of State For The Foreign & Commonwealth Office & Ors.

²⁹⁰ Liberty & Others v. the Security Service, SIS, GCHQ (The Investigatory Powers Tribunal May 16, 2016).

government.²⁹¹ For instance, the IPT found in favor of Amnesty International, noting that its e-correspondence was lawfully and proportionately intercepted and accessed in accordance with Section 8(4) of RIPA,²⁹² however, the time limit of retention exceeded the permitted, thus the violation was found.²⁹³

All applicants to the ECtHR²⁹⁴ claimed infringement on their rights to privacy under Article 8 of the ECHR (and in one instance Article 10 of the ECHR) via the extensive use of the electronic surveillance programs possessed by the UK.²⁹⁵

3.2. ECtHR approach in Big Brother Watch – finding proportionality

The Chamber of the First Section on 13 September 2018 held cases admissible²⁹⁶ and found that there has been a violation of Article 8 and Article 10 of the ECHR in the respect of the intelligence sharing regime.²⁹⁷ Upon the request of the first and third applicants the case was referred to the Grand Chamber.²⁹⁸

The Grand Chamber (on 10 July 2019), assessing the background of the facts of the case, noted the impact of such Snowden's revelations, not only on the EU level, but also regionally, reaching the ECtHR.²⁹⁹ The applicants based on the nature of their activities (mostly civil liberties and privacy advocates), believed to be intercepted by the UK government and its subsequent intelligence and security services.³⁰⁰

²⁹¹ Notwithstanding the prudent owner's outlook immediately conducting judicial proceedings, the UK did not acknowledge to be responsible for all allegations, as the GCHQ mentioned that the IPT only found against the UK in a small respect and stressed that established safeguards for privacy in respect of surveillance activities were fully adequate. *Liberty & Others v. the Security Service, SIS, GCHQ*, §§8-17.

²⁹² Section 8(4) of the RIPA. *See* Annex 16.

²⁹³ *Liberty & Others v. the Security Service, SIS, GCHQ*, §14.

²⁹⁴ Not satisfied with such rulings and dismissals of IPT ten human rights organizations filed an application to the ECtHR claiming that the regulatory landscape governing the surveillance in the UK was incompatible with Article 8 of the ECtHR. Besides these ten applications, two other applications were lodge regarding the same matter. *Big Brother Watch and Others v. the United Kingdom* – which did not bring a claim before IPT, however, applicants were concerned of being subject to such surveillance, thus, claiming that such surveillance would not be in accordance with a law as it constituted a disproportionate interference with their privacy. The third - *Bureau of Investigative Journalism and Alice Ross v. the United Kingdom* - application concerned applicants who also did not bring a claim before domestic proceedings as deemed such to be ineffective, thus lodging the claim within the ECtHR. The applicants submitted that such surveillance of communications was not in accordance with law or prescribed by law, consequently, arguing that such interception inhibited their ability to carry out investigative journalism (for instance, when exploiting their communications) via disproportionately interfering with their right to privacy and freedom of expression under ECHR. *10 Human Rights Organisations and Others v. the United Kingdom* 24960/15; *Big Brother Watch and Others v. the United Kingdom* 58170/13; *Bureau of Investigative Journalism and Alice Ross v. the United Kingdom* 62322/14. *Big Brother Watch and Others v. the United Kingdom*, §1.

²⁹⁵ *Big Brother Watch and Others v. the United Kingdom*, §3.

²⁹⁶ Only the third application was viewed as inadmissible under Article 6, Article 10 and Article 14 of the ECHR. *Big Brother Watch and Others v. the United Kingdom*, §5.

²⁹⁷ *Ibid.*

²⁹⁸ *Big Brother Watch and Others v. the United Kingdom*, §6.

²⁹⁹ *Big Brother Watch and Others v. the United Kingdom*, §12.

³⁰⁰ The applicants mostly were NGOs or organizations advocating for civil liberties and protection of privacy, such as the Big Brother Watch or Privacy International, additionally, among them were individuals. *Big Brother Watch and Others v. the United Kingdom*, §13.

The main mass surveillance schemes at the dispute were the international sub-marine fiber optic cables possessed by the CSPs, where these cables carries persons' data via using several bearers and packets, namely, connection points that could be also located outside of one's jurisdiction.³⁰¹ Hence, the personal data vulnerability facing the surveillance and misuse faces greater risk.³⁰² However, according to the 2015 Report of the Intelligence and Security Committee of Parliament of the UK, the intelligence services were running two mass surveillance systems – both of which find their legal grounds in RIPA.³⁰³

Regarding the background of an regulatory landscape for such interception the ECtHR assessed the UK's national legal framework. Following provisions and legal documents were analyzed. A Section 8(4) of the RIPA³⁰⁴ constituting bases for issuance of the warrants for such interception, Section 16 of RIPA,³⁰⁵ allowing to investigate specific events, if there is a suspicion of a risk of threat.³⁰⁶ Additionally, Chapter II of RIPA was viewed in the scope of the access of such data of other public authorities.³⁰⁷ Regarding such intelligence sharing the Chapter 12 of the IC Code was assessed the inter-state intelligence sharing assistance.³⁰⁸ The IC Code specifically established that in order to exercise RIPA surveillance warrant on the basis of national security or to prevent crime or to safeguard economic wellbeing of the UK, it shall be deemed as necessary and proportionate in order to satisfy requirement under Article 8 of the ECHR.³⁰⁹ Notably, as of the case references, the ECtHR outlined both the Schrems I and Schrems II cases.³¹⁰

³⁰¹ It must be noted that the UK did not confirm or deny the existence of TEMPORA program. Big Brother Watch and Others v. the United Kingdom, §15.

³⁰² The ECtHR noted that PRISM was a program:” through which the United States’ Government obtained intelligence material (such as communications) from Internet Service Providers (“ISPs”). Access under PRISM was specific and targeted (as opposed to a broad “data mining” capability). The United States’ administration stated that the programme was regulated under the Foreign Intelligence Surveillance Act (“FISA”), and applications for access to material through PRISM had to be approved by the Foreign Intelligence Surveillance Court (“FISC”).” Whilst the Upstream was a program that:” allowed the collection of content and communications data from fibre optic cables and infrastructure owned by United States’ CSPs. This programme had broad access to global data, in particular that of non-US citizens, which could then be collected, stored and searched using keywords.” Big Brother Watch and Others v. the United Kingdom, §§22-25.

³⁰³ Big Brother Watch, §16. One of them targeted small portion of bearers which used specific identifiers, for instance, e-mail address, relating to the data subject. After the process of data collection the analysts initiated triage process with an aim to evaluate which possess a certain risk, thus, were needed to be investigated. The other system targeted even smaller portion of bearers, which were used letter for targeting also those possessing highest risks, thus carrying a need to be investigated. Big Brother Watch and Others v. the United Kingdom, §§17-18.

³⁰⁴ Section 8(4) of the RIPA. See Annex 16.

³⁰⁵ Section 16 of the RIPA. See Annex 16.

³⁰⁶ Big Brother Watch, §19.

³⁰⁷ RIPA.

³⁰⁸ Interception of Communications Code of Practice 2018. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/715480/Interception_of_Communications_Code_of_Practice.pdf. Accessed February 23, 2023. Big Brother Watch and Others v. the United Kingdom, §20.

³⁰⁹ The ECtHR *inter alia* also elaborate on following regulatory provisions. Convention for the Protection of Individuals with Regard to the Automatic Processing of Individual Data, 28 January 1981, ETS 108; The Counter-Terrorism Act 2008. Available on: <https://www.legislation.gov.uk/ukpga/2008/28/contents>. Accessed February 23, 2023; The Data Protection Act 1998. Available on: <https://www.legislation.gov.uk/ukpga/1998/29>. Accessed March 3, 2023. Big Brother Watch and Others v. the United Kingdom, §§96-116.

³¹⁰ Big Brother Watch and Others v. the United Kingdom, §§223-234.

Based on above expressed, the ECtHR addressed interference of privacy via three perspectives:

- 1) a mass surveillance of communication in the light of Article 8(4) of RIPA;
- 2) an intelligence sharing system;
- 3) an acquisition of communications under Chapter II of RIPA.³¹¹

Further, the author will analyze the ECtHR provided assessment on the proportionality principle when analyzing alleged infringement of Article 8 of the ECHR by the mass surveillance exercised in the light of Article 8(4) of RIPA.³¹² It shall be noted that the ECtHR takes a bit more settled approach on the gravity of mass surveillance than the CJEU, namely, noting that its impact on one's privacy shall be seen as gradual process, where the degree of interception matters (nevertheless, finding that for each degree Article 8 of the ECHR applies).³¹³

The ECtHR expressed that in order to reduce the risk of mass surveillance abusing right to privacy, the each stage of interception shall be end-to-end safeguarded, primarily by applying the principle of proportionality, which in the ECtHR's view, *inter alia*,³¹⁴ is: "fundamental safeguard which will be the cornerstone of any Article 8 compliant bulk interception regime."³¹⁵ Furthermore, the ECtHR indirectly implies necessity of transparency regarding the availability of information concerning both purpose and the used bearers or communication routes of interception for the competent authority, thus enabling such to assess the proportionality of exercised mass surveillance.³¹⁶

The ECtHR observed that enhanced safeguards shall be put in place, when a strong selector are chosen (thus linking information to individuals) conducting surveillance activities.³¹⁷ Such approach is similar to the CJEU approach in the Schrems I case, which noted that protection shall be enhanced especially in cases of ADM processes of mass surveillance. The use of such selectors shall be justified by the intelligence services upon the balancing act of interests.³¹⁸

For the proportionality of a mass surveillance, specifically examining the matter of such accordance with law and its necessity, the ECtHR outlined need of clearly defined domestic legal

³¹¹ Big Brother Watch and Others v. the United Kingdom.

³¹² Such an approach has been taken as the first matter encompasses the key matter of the case and can be compared also with the Schrems I and Schrems II cases. Nevertheless, the author will draw on the main conclusions of the ECtHR also regarding the second and third issues described.

³¹³ Big Brother Watch and Others v. the United Kingdom, §325;§330.

³¹⁴ Additionally noting the need of the assessment of necessity; authorization and supervision. Big Brother Watch and Others v. the United Kingdom, 350.

³¹⁵ *Ibid.*

³¹⁶ Big Brother Watch and Others v. the United Kingdom, §352.

³¹⁷ Big Brother Watch and Others v. the United Kingdom, §355.

³¹⁸ Moreover, the ECtHR expressed that each stage of mass surveillance process shall possess supervision in which the principle of proportionality is also applied. Big Brother Watch and Others v. the United Kingdom, §§355-56.

framework (also one of the Schrems I conclusions – clear and precise regulatory landscape),³¹⁹ that would include following eight prerequisites.³²⁰

Firstly, the grounds on which bulk interception may be authorized shall be defined and narrow in order to provide an effective guarantee of protection in order to ensure that the mass surveillance would be authorized only for such interest's purpose that meets principle of proportionality.³²¹

Secondly, the circumstances in which an individual's communications may be intercepted shall be accordingly assessed, especially regarding external communication interception, where other States³²² might possess less intrusive measures to obtain communication of a specific individual.³²³ This concept serves a novelty if compared to the CJEU approach, nevertheless, from the author's perspective requires application of more advanced technological tools and great interstate relations to establish mutual assistance in such requests for data information, which would therefore be more burdensome.

Thirdly (and fourthly), the procedure to be followed for granting authorization is also the key to meet the standard of proportionality, where such shall be conducted by an independent body (which the UK failed to do in this case).³²⁴ One of the parts of such procedure consists of a consideration of why mass surveillance would be proportionate to the necessary aim.³²⁵ Specifically, the obliged body had to consider whether less intrusive measures were available.³²⁶ Consequently examining the size and scope of such surveillance, giving he explanation on how and why used surveillance mechanism would cause less damage as all other alternatives and the evidence that would outline that such alternatives would fall short on meeting the objective.³²⁷ Such perspective was not brought in the Schrems cases.³²⁸ The ECtHR to this aim noted as the Section 8(4) of the RIPA did not indicate specific categories of selectors to be implemented, there was no possibility for their proportionality to be assessed at the stage of authorization,³²⁹ noting that although the analysts had to note and justify the use of selectors in the light of the principle of proportionality, a strong selectors identifying an individuals were not subject to prior internal

³¹⁹ As the ECtHR puts it: "In principle, the wider the grounds are, the greater the potential for abuse." *Big Brother Watch and Others v. the United Kingdom*, §370. The ECtHR applied the same narrative in *Dragojević v. Croatia* case which concerned secret surveillance of a suspect in a drug trafficking case. Even though *Dragojević v. Croatia* case concerned targeted trafficking, the ECtHR noted that any type of surveillance is to be *Seen* as seriously interfering with one's private life and correspondence, hence such an act must be based on a law that is precisely established. *Dragojević v. Croatia*, No. 68955/11 (ECtHR January 15, 2015), §§ 94-98.

³²⁰ Additionally, regarding related communications data in the context of mass surveillance, the ECtHR noted that it shall bear the same threshold of safeguards and obligations. *Big Brother Watch and Others v. the United Kingdom*, §361.

³²¹ *Big Brother Watch and Others v. the United Kingdom*, §370.

³²² Namely, referring to a situation when a data flows to a different country for a connection point, nevertheless, being collected by the UK.

³²³ *Big Brother Watch and Others v. the United Kingdom*, §375.

³²⁴ *Ibid.*

³²⁵ *Big Brother Watch and Others v. the United Kingdom*, §378.

³²⁶ *Big Brother Watch and Others v. the United Kingdom*, §379.

³²⁷ *Ibid.*

³²⁸ However, the author indicated such an approach when describing the notion of privacy within the scope of the principle of minimization (moreover, also being observed in the principle of a legitimate aim).

³²⁹ *Big Brother Watch and Others v. the United Kingdom*, §381.

authorization.³³⁰ Consequently outlining the fourth requirement - the procedures to be followed for selecting, examining and using intercept material were foreseeable and provided adequate safeguards.³³¹

Fifthly, regarding the precautions to be taken when communicating the material to other parties, namely, transferring data outside the UK, the ECtHR noted that such action only would intervene with Article 8 of the ECHR if the sending State did not ensure that the receiving State had adequate safeguards of preventing disproportionate interference, especially, could guarantee secure storage.³³² This approach also mirrors the CJEU perspective of ensuring that third party has adequate safeguards.

Sixthly, the limits on the time span of data collection, storage and deletion shall also correspond to the principle of proportionality, where such durations shall be clearly stated in the regulatory provisions.³³³ The CJEU in neither of the Schrems's cases examined in such detail practical implications that would rise doubts over a proportionality.

Seventhly (and eighthly) the ECtHR put emphasis on the supervision and *ex post facto* monitoring.³³⁴ Specifically expressing a need to supervisory authority being able to assess the proportionality of each warrant application and the choice of chosen surveillance method, additionally noting that such approach shall be also applied in the assessment of data retention, storage and deletion.³³⁵ Regarding the *ex post facto* review, the ECtHR references the need of an effective remedy. This was one of the major loopholes in Schrems II, namely, lack of an enforcement mechanism available in the US that gave one of the pillars of Privacy Shield invalidation. Interestingly, the ECtHR was satisfied with the IPT ability to provide an effective remedy, even though one of the major backlash of the IPT was its dismissal of a claimants that were situated outside the UK and claimed a violation of the.³³⁶ Whereas the CJEU (regarding this matter taking detailed approach) concluded that the US did not provide effective remedies also after the Safe Harbor Decision upgrades in the US domestic law, namely, put a great gravity to such issues then the ECtHR.

After an examination of the proportionality prerequisites, the ECtHR noted that in case of data transfers (that is of a legality of international intelligence sharing under the ECHR), the transferring State is the one which is obliged to ensure the receiving State has in place appropriate safeguards that are capable to prevent disproportionate interference.³³⁷ Such conclusion practically mirrors the Schrems I and Schrems II cases, where the CJEU noted that the data controllers

³³⁰ Big Brother Watch and Others v. the United Kingdom, §383.

³³¹ Big Brother Watch and Others v. the United Kingdom, §§384-391.

³³² Regarding this prerequisite the ECtHR noted that it was satisfied with the regulatory framework and practices put in place by the UK. Big Brother Watch and Others v. the United Kingdom, §395.

³³³ Big Brother Watch and Others v. the United Kingdom, §403.

³³⁴ Big Brother Watch and Others v. the United Kingdom, §§406-415.

³³⁵ Big Brother Watch and Others v. the United Kingdom, §§409-412.

³³⁶ With this regard it must be noted that IPT in its decision did note that non-UK residents could be considered for domestic claims, nonetheless only if such would submit additional information illustrating that they are at a potential risk to be surveillance, namely, establishing a higher level of burden of proof (where the access to justice is thus more limited). However, as expressed in the background of the case, one of the applicants also noted that the claim was not brought before the IPT due to the disbelief of it provided an effective remedy.

³³⁷ Big Brother Watch and Others v. the United Kingdom, §362.

(EUDPA) are the ones obliged to assess whether the third country possess an adequate protection mechanism.³³⁸ However, interesting difference follows from such statement made by the ECtHR:” does not necessarily mean that the receiving State must have comparable protection to that of the transferring State.”³³⁹ Such approach is completely different from that of the CJEU which firmly in both cases advocated for such safeguarding mechanism available in the third country that would essentially mirror the guarantees of protection laid down in Articles 7 and 8 of the EUCFR.³⁴⁰

The ECtHR noted that it was satisfied with the RIPA regime that constitutes legal grounds for the mass surveillance, including, legitimate aims – national security; prevention of crime; protection of right and freedoms of others.³⁴¹ Nevertheless, it was crucial to consider whether such framework contains adequate and effective safeguards that guarantee foreseeability and necessity in a democratic society.³⁴² Thus, outlining that the components of assessing proportionality are: lawful grounds; legitimate aim; foreseeability and necessity in a democratic society. Regarding the requirement of foreseeability (explained above in the proportionality prerequisites), in author’s opinion, it shall be viewed as an analogous for the principle of transparency. Consequently, the ECtHR noted that notwithstanding the complex regulatory structure of the UK’s mass surveillance governance, its implementation of IC Code (encompassed in many RIPA provisions) that is public document, shall be seen as adequately foreseeable or accessible.³⁴³

The ECtHR in its conclusions acknowledged the importance of mass surveillance in national security,³⁴⁴ hence drawing on a wide margin of appreciation that High Contracting Parties possess in such matters.³⁴⁵ Such approach is quite different then that taken by the CJEU in Schrems I case, which loudly pronounced mass surveillance as inherently juxtaposing right to privacy and through both of its decisions rather decreased mass surveillance’s importance, rather seeking for substitutes.³⁴⁶ Nevertheless, the ECtHR emphasized the major risk of a mass surveillance adversely impacting the right to private life.³⁴⁷ Thus, concluding that notwithstanding robust safeguards employed by the UK, they did not showcase sufficient end-to-end protection mechanism that would protect from an arbitrary intervention and possible abuse.³⁴⁸ The ECtHR highlighted following deficiencies observed in the actions of mass surveillance (and related data interception): the absence on an independent authorization body;³⁴⁹ failure to include the selector categories in the warrant application;³⁵⁰ failure to examine selector linked to an individual prior authorization.³⁵¹

³³⁸ See Chapter “Analysis of the CJEU judgement in Schrems I and Schrems II cases.”

³³⁹ Big Brother Watch and Others v. the United Kingdom, §362.

³⁴⁰ See Chapter “Analysis of the CJEU judgement in Schrems I and Schrems II cases.”

³⁴¹ However, the latter notes that the UK’s mass surveillance regime lacks clarity due to its complex structure. Big Brother Watch and Others v. the United Kingdom, §§365-366.

³⁴² Big Brother Watch and Others v. the United Kingdom, §365.

³⁴³ Big Brother Watch and Others v. the United Kingdom, §366.

³⁴⁴ Drawing on the submission of the UK other governments and experts, outlined that mass surveillance bears an essential capability, hence the importance for national security. Big Brother Watch and Others v. the United Kingdom, §424.

³⁴⁵ *Ibid.*

³⁴⁶ See Chapter “Analysis of the CJEU judgement in Schrems I and Schrems II cases.”

³⁴⁷ Big Brother Watch and Others v. the United Kingdom, §425.

³⁴⁸ *Ibid.*

³⁴⁹ As the authorization largely was given by the State Secretary – an executive, not designated independent body. *Ibid.*

³⁵⁰ *Ibid.*

³⁵¹ *Ibid.*

The ECtHR expressed that effective judicial oversight did not counterbalance such insufficiency.³⁵² Consequently finding that Section 8(4) of the RIPA did not meet quality of law prerequisite, hence was incapable of regulating mass surveillance activities as a necessity in a democratic society that would uphold the proportionality principle.³⁵³ Therefore, pronouncing a violation of Article 8 of the ECHR.³⁵⁴

3.3. Implications of the Big Brother Watch case

After the Big Brother Watch decision the ECtHR faced lesser scrutiny if compared to the CJEU.³⁵⁵ The Big Brother Watch decision was perceived as reinforcement of the ECtHR liberal approach on the matters regarding wide margin of appreciation, specifically referring to the national security aspect.³⁵⁶ Upon the ruling, the UK government was required to amend legal framework governing mass surveillance, which was done by replacing RIPA with an IPA which enhanced needed safeguards.³⁵⁷

Similarly to the effect of the both Schrems's decision, the ECtHR ruling advanced the data privacy law perspective not only in the national level, but also had its implications on a regional spectrum. Especially, the involved NGOs praised ruling as a landmark for exposure of how vulnerable privacy concept is in today's narrative. Kate Logan, Senior Legal Counsel at Amnesty International, expressed: "The unfettered harvesting and processing of millions of people's private communications must end."³⁵⁸

³⁵² *Ibid.*

³⁵³ Big Brother Watch and Others v. the United Kingdom, §426.

³⁵⁴ Big Brother Watch and Others v. the United Kingdom, §427.

³⁵⁵ Some spectators as the Massimo Frigo, ICJ Senior Legal Adviser, Europe and Central Asia Program shared the opinion that the ECtHR missed the mark in such landmark decision, namely, missing the threats associated with the concept of the era of Big Data. Frigo outlined that the judgement showcased the ECtHR's explicit trust in the intelligence services that constituted conceptual weakness as it asserted to make the mass surveillance work. The author does not share the same viewpoint, especially, as the ECtHR truly applied detailed assessment of an each action taken in the process of mass surveillance and in itself applied the proportionality principle. Rather, the author perceives this approach as an opportunity to create a compromise that reconciles the interests of both pro-surveillance and pro-privacy factions. International Commission of Jurists. "Big Brother Watch v. UK: A Landmark Judgment Missing the Mark," June 4, 2021. Available on: <https://www.icj.org/big-brother-watch-v-uk-a-landmark-judgment-missing-the-mark/>. Accessed April 10, 2023.

³⁵⁶ Such an approach by the ECtHR also was taken in the case of Weber and Saravia v. Germany (from which the ECtHR drew the proportionality requirements analyzed above). Weber and Saravia v. Germany (déc.), No. 54934/00 (ECtHR June 29, 2006); Monika Zalnieriute, "Big Brother Watch and Others v. the United Kingdom," *American Journal of International Law* 116, no. 3 (2022): 585–92, <https://doi.org/10.1017/ajil.2022.35>.

³⁵⁷ Government of the United Kingdom. "Responding to Human Rights Judgments: 2021 to 2022." Available on: <https://www.gov.uk/government/publications/responding-to-human-rights-judgments-2021-to-2022>. Accessed April 10, 2023; Paula Giliker, "The Influence of EU and European Human Rights Law on English Private Law," *The International and Comparative Law Quarterly* 64, no. 2 (2015): 237–65, <http://www.jstor.org/stable/24760680>.

³⁵⁸ Adding that: "Today's ruling marks a significant step forward in condemning surveillance at the whim of the government." Amnesty International. "UK: Europe's Top Court Rules UK Mass Surveillance Regime Violated Human Rights," May 25, 2021. Available on: <https://www.amnesty.org/en/latest/press-release/2021/05/uk-surveillance-gchq-ecthr-ruling/>. Accessed April 10, 2023.

Moreover, the other applicant – Privacy International – celebrated the importance of the UK’s governments acknowledgement of the abuse of mass surveillance and consequent payment of compensation to the victims.³⁵⁹

Nevertheless, the UK government’s response to the Big Brother Watch case was a bit delusional as the governmental spokesperson noted that:” The UK has one of the most robust and transparent oversight regimes for the protection of personal data and privacy anywhere in the world.”³⁶⁰ Whilst it bears a grain of truth also wasted in the ECtHR’s reasoning, such bold response does not necessarily suit the letter actions taken by the UK government in the improvement of the regulatory framework and consequent acknowledgement of the wrongdoing.

At large the ECtHR decision can be seen as praised by both side. The pro-privacy camp celebrates the victory over the acknowledgement of the infringement and advancement in the regulatory field, whilst pro-surveillance camp, namely the government of the UK welcomes the critique of the ECtHR which also did not overlook the importance of the mass surveillance, accordingly amending its legal landscape the suit the safeguards of the privacy.

3.4. Comparison of the CJEU and ECtHR approaches

Both courts ruled in favor of the protection of privacy, nevertheless, with some interesting differences that the author will indicate further.³⁶¹ It can be observed that the CJEU’s rulings in both Schrems cases carries a great political importance and in a some level power play. The CJEU really puts in forefront its values, despite inherently EU being an economic union, the CJEU with such robust approach leaving commercial benefits on a secondary level, truly outlines the EU’s policies power play.³⁶² Whilst the ECtHR took more relaxed approach than the CJEU, nevertheless, coming to same conclusions. The CJEU expressed a need of such safeguards that would mirror the EU regulatory landscape (would be equivalent). Whilst the ECtHR on contrary noted, that it does not necessarily need to have a comparable protection, what matters is a guarantee of security and such effective practice to safeguard privacy.

The ECtHR adopted a more practical and lenient approach in its assessment, particularly when scrutinizing the application of the proportionality principle. The ECtHR provided detailed guidelines outlining the steps that should be taken in order to achieve a balance, and subsequently evaluated whether such measures were indeed proportional. As an illustration, the ECtHR amongst

³⁵⁹ Privacy International. “UK Government Acknowledges Past Violations of Individuals’ Rights and the Fight Continues...” Available on: <http://privacyinternational.org/news-analysis/4818/uk-government-acknowledges-past-violations-individuals-rights-and-fight>. Accessed April 10, 2023.

³⁶⁰ Guy Faulconbridge and Guy Faulconbridge, “UK Spies Violated Human Rights with Bulk Intercepts, European Court Rules,” *Reuters*, May 25, 2021, sec. United Kingdom. Available on: <https://www.reuters.com/world/uk/uk-violated-human-rights-with-bulk-intercepts-european-rights-court-rules-2021-05-25/>. Accessed April 10, 2023.

³⁶¹ It must be noted that the author regarding specific procedural issues compared both court approaches in the Big Brother Watch case analysis.

³⁶² It must be noted that the CJEU works in the context of the EU Law which from its roots has been focused on constructing a single market area within the confines of the EU. Hence, also always keep in mind the impact of the decision on the area of the single market, specifically, regarding market integration. As the data is the new currency of the 21st century, the single market paradigm could also impact the CJEU’s stance on such matters. R. Daniel Kelemen, “THE COURT OF JUSTICE OF THE EUROPEAN UNION IN THE TWENTY-FIRST CENTURY,” *Law and Contemporary Problems* 79, no. 1 (2016): 117–19, <http://www.jstor.org/stable/43920647>.

other practicalities assessed the time span that would be adequate for the deletion or storage of the collected data, whilst the CJEU strongly through its decisions reiterated need of mirroring the EU regulatory framework, namely, did not provide such detailed analysis. Additionally, the ECtHR gave explicit direction on what should be upgraded regarding regulatory framework to reach needed proportionality whereas the CJEU only referred to desirable equivalence and in neither of the cases gave clear forward directions after the invalidation of the Safe Harbor and the Privacy Shield decisions.³⁶³

Nevertheless, it must be noted that the CJEU truly possesses the gatekeeper role of the safeguard of the EU values and interest.³⁶⁴ Of course, the ECHR is one of the major human rights defenders in the Europe, regarding cases where the High Contracting Parties possess wide margin of appreciation, as in the case of the Big Brother Watch, which main interest on the side of the respondent is national security – the ECtHR does not exercise such politically robust approach, rather via its though extermination on detail draws an emphasis on the existing loopholes and gives guidance of preferable outcome.³⁶⁵ Thus, taking itself off of a too much of a scrutiny and backlash, yet safeguarding the fundamental right to privacy.³⁶⁶

³⁶³ Whilst the CJEU put emphasis on the legality and effectiveness of the regulatory regime employed for the mass surveillance, the ECtHR via its approach rather emphasized the importance of a procedural safeguards (nevertheless, the CJEU conclusions also largely find their basis on the procedural missteps, nevertheless, great importance is put on the inherent illegitimacy of a mass surveillance and consequent great risks).

³⁶⁴ Elizabeth Defeïs, “Human Rights and the European Court of Justice: An Appraisal,” *Fordham International Law Journal* 31, no. 5 (January 1, 2007): 1104, <https://ir.lawnet.fordham.edu/ilj/vol31/iss5/2>.

³⁶⁵ Hutchinson, “The Margin of Appreciation Doctrine in the European Court of Human Rights.”

³⁶⁶ It is crucial to note the importance of the CJEU and ECtHR relationship with the applicable States and the nature of the disputes that impact the approach employed. From the perspective of the CJEU, it possess a great power, as the Member States with their succession to the EU, give supremacy to the EU Law over the national constitutional law, namely, the CJEU is hierarchically superior in the fields where it has a competence to intervene. As the Schrems’s cases concerned a preliminary ruling, the CJEU so robustly illuminated the EU Law, as its task was to set a precedent of a correct way of an interpretation of EU regulatory landscape. Whilst the ECHR saw disputes on all levels, namely, domestic parallel to, for example, EU Law, however, primarily thoroughly examining domestic practices of the UK, hence taking more lenient approach and rather stopping the swinging pendulum in the middle of concurring interests. Andreas Paulus, “Human Rights Protection in a European Network of Courts,” *Proceedings of the ASIL Annual Meeting* 107 (2013): 178, <https://doi.org/10.5305/procanmeetasil.107.0174>. See also Nico Krisch, “The Open Architecture of European Human Rights Law,” *The Modern Law Review* 71, no. 2 (2008): 183–216, <http://www.jstor.org/stable/25151192>.

CONCLUSION

Mass surveillance particularly in the digital age which foster wide spectrum of technologies allows public authorities advanced opportunities at the same time cultivating a greater risk of the infringement of one's privacy, particularly under the notion of the use of personal data. The proponents of mass surveillance mostly advocate for the enhancement of the protection of national security, especially, in times of troublesome events, such as terrorist attacks or geopolitically closely linked military hostilities that increase the risk of protentional breach of state security interest, hence, leaving the individual interest on the level of secondary importance.

The concept of privacy fosters an understanding of one being independent of needless interference in one's private life, which is constituted on the pillars of personal dignity, freedom, and identity and serves as an umbrella term, also encompassing personal data. The advocates for privacy argue that mass surveillance infringe individual's right to privacy. Hence claiming that such intrusion on many occasions can be substituted by less demanding means. Moreover, in such bilateral debates commercial interests are commonly present as personal data nowadays is perceived to serve as a great asset for financial gains.

The regulatory landscape in such diverse relationships consequently is complex and multilayer. It must be noted that mass surveillance activities are regulated on a national level, there is no international unified practice of governing mass surveillance policies. On the other hand, the right to privacy is extensively safeguarded on all levels – international, regional, and national. If viewed in Europe's context, it is enshrined in the ECHR Article 8 and in the EUCFR Articles 7 and 8. Alongside other international human rights and various guidelines, named provisions establish the following pillar requirements to ensure the protection of a right to privacy.

As mass surveillance is regarded as an interference with one's private life it invokes a breach of a state's negative obligation to refrain from such action. Upon interference the act shall be exercised in accordance with law; possess a legitimate aim and shall be necessary for a democratic society. As the right to private life is not absolute, there might be derogations, for example, in the interest of national security. Consequently, such interference invokes a balance of interest which inherently imposes to apply the principle of proportionality.

It must be noted that from the soft law instruments, additional principles emerge to safeguard privacy: consent, transparency, minimization, legality, legitimacy, and others. The leading loophole in such debate is the level of transparency employed. The pro-surveillance camp highlights that a complete openness would be contrary to the legitimate aim of increasing security, thus, advocates to employ a legitimate transparency secrecy veil that would possess a certain level of transparency and a possibility to rise doubts of exercised mass surveillance activities. Whilst the pro-privacy camp advocates for more transparent policies that would consequently foster shared knowledge and understanding of processes.

The author holds an opinion that transparency's secrecy in democratic societies shall not be perceived as a great burden as it is constituted upon institutional framework, where whistleblowing opportunities provide a way of lifting such a veil. In the author's opinion, too much openness might lead to greater risks, consequently, pushing for stricter regulations. Therefore, fostering rather a circularly spiral effect which with each demand for transparency would tighten,

consequently leading to more autocratic and desperate regulatory decisions or illegitimate practices. Moreover, the author believes as there is a lack of transparency within such a realm, the lack of concrete legitimate grounds should withhold the threshold for suspicion, thus allowing one to blow the whistle. One of the great examples of the availability to lift the veil is judicial proceedings or formal claims to competent authorities, which proved to be successful in the examined cases.

However, the author notes that such an approach is rather burdensome and lack of transparency leads to other drawbacks, such as technical illiteracy of society, hence, fostering the risk of societal manipulation which emerges from individuals' being left in such a black box. Clearly established rules, in the author's opinion, would, thus, sweep away some level of fear in public of the unknown – how exactly data is collected and used. The other problem emerging from such a great loophole is the lack of trust not only among the individual and state but also between the states themselves, as mass surveillance increases the risk of spying.

Hence, the author believes that to reach a mitigating effect on mutual trust the society needs to be educated on such matters so that technical illiteracy would not lead to hollow and unnecessary disputes. Moreover, States shall employ such engineering solutions that would minimize privacy intrusions and upgrade personal data governance policies.

Thus, the author invites to apply the principle of proportionality as it synergistically binds together above expressed principles and statutory norm requirements. Such an approach can also be characterized as a tradeoff of interests, where the middleman between two camps aspires to establish beneficial habitats for all concurring interests involved. The author chose to assess the judicial bodies' approach to such a matter.

When viewing the Schrems I case, the CJEU perceived mass surveillance at its core as contrary to the fundamental right of privacy, as the author notes it – inherently evil. Thus, to safeguard privacy such an act shall possess an adequate protection mechanism that would be clear and precise ensuring that there would be no unlawful access from any party to one's personal data. The CJEU concluded that derogations are possible only when strictly necessary and proportionate to reach the legitimate aim. Hence, establishing a high threshold on the national security interest side that should be reached in order to set a balanced tradeoff.

The CJEU employed a similar perspective in the Schrems II case. The CJEU in the analysis of the SCC decision's validity thoroughly exercised the principle of proportionality aiming to establish a mitigating factor from available governing instruments, concluding that case-by-case tailored supplementary measures for the transfer of personal data would meet the needed requirements for an adequate safeguard. However, in the author's opinion, it is quite burdensome upon the companies and controllers involved in such transfers, that potentially would lead to a room for missteps and would require a more excessive amount of resources as the component supervisory authority shall examine and approve every modality and consequent implication on data transfer activities. Thus, the author favors the establishment of a unified and effective safeguarding mechanism in order to continue to conduct trans-Atlantic data flows more freely, which is currently under the drafting process of the Trans-Atlantic Data Transfer Framework succeeding Safe Harbor and Privacy Shield decisions.

Regarding the prerequisite of strict necessity, also outlined in the Schrems II, the CJEU added specific requirements and expanded the scope, namely, calling for the need for clear and precise rules governing such derogations, a need for the imposition of minimum safeguards, especially concerning available judicial remedies and in the instances of the use of ADM processes. Furthermore highlighting the need for following reforms - a limitation on the bulk collection, precise application of the principles of necessity and proportionality, and advancement of standards regarding surveillance targeting, thus, enhancing transparency and providing disclosure policies.

If to compare Schrem I and Schrem II, in the former, the CJEU looked more at the commercial interest and the privacy, that comes from the nature of the data transfer decisions. Nevertheless, the inherent concern was the interception of personal data, hence it amended its approach to see whether there are adequate safeguards. Thus demonstratively swinging the pendulum towards the right to privacy emphasizing via both judgments the need for the US to possess such a framework that would be equivalent to safeguards provided under the EUCFR. Whereas in Schrems II case, the CJEU advanced its strict narrative focusing on and assessing more directly concerns of the public authority access to personal data.

The CJEU placed individual fundamental human rights at the forefront of the legal landscape, underlining the importance also of digital sovereignty. As a result, both the Safe Harbor and Privacy Shield decisions via the application of a principle of proportionality were struck down by the CJEU, reflecting a shift towards prioritizing the protection of personal data over the interests of transatlantic data transfer. According to the author's perspective, the Schrems II ruling (as well as Schrems I) provides a notable illustration of the Brussels Effect, whereby the far-reaching impact of the personal data protection regulation, particularly in the context of the GDPR, has resulted in its evolution from a supranational regulatory framework into a widely recognized global standard. Therefore, Schrems's cases highlight that the strength of a law such as the GDPR is contingent upon initiative, advocacy, and social pressure to apply it in a transatlantic context, which gathers such interest groups and individuals, states, and companies – all with their individual agendas. Moreover, both preliminary rulings broadened the disputed scope to the international cross-border level, hence playing a major role in EU and US political relations.

The ECtHR exercised a rather lenient approach if compared to the CJEU not finding mass surveillance as inherently evil, but rather portraying its necessity in the realm of national security, hence, aspiring to establish the golden pathway serving both interests. The ECtHR to reach such an aim more directly employed and stressed the importance of the principle of proportionality, establishing eight prerequisites: defined and narrow grounds for the authorization of mass surveillance; observance of less intrusive measures if data are transferred outside one's confines; the principle of proportionality shall be employed in every stage of mass surveillance authorization; the exercised procedures shall be foreseeable and shall provide adequate safeguards; when transferring data outside one's confines adequacy of receiving State's safeguarding mechanism shall be assessed; the data processing limits shall be proportionate; there shall be an *ex post facto* monitoring and availability of judicial remedies.

The ECtHR thus introduced two novelties in mass surveillance proportionality requirements if compared to the CJEU, namely, the need for the assessment of whether external communication interception concerns such jurisdiction that exercises less intrusive surveillance means and the establishment of proportionate limits of data processing steps.

The main prerequisites emerging from the analyzed cases for the act of mass surveillance to be proportionate, thus not infringing the right to privacy, are following: interference shall be exercised in accordance with law; possess a legitimate aim; shall be strictly necessary to achieve the legitimate aim; parties involved in data transfers shall ensure an adequate level of safeguard; such mechanism shall be clear and precise and provide effective judicial remedies; the process of mass surveillance shall be monitored and authorized invoking the principle of proportionality at every stage of usage of personal data; process shall be foreseeable; when possible less intrusive measures shall be placed and limits to the time span of the usage of such data shall be invoked in the light of the principle of proportionality. It must be noted that the list is not exhaustive. As the analysis proved, the assessment of a particular case might bring a novelty in the field of needed safeguards for proportionality.

For further research, the author noted that there are no unified mass surveillance policies internationally, hence, each state must be assessed on a case-by-case basis. There might be regional trends on such approaches, for example, amongst the Member States of the EU, thus such paradigm could also be analyzed in order to establish what are the trends of mass surveillance in a regional context and whether they meet the requirements established in such landmark cases. Moreover, this Thesis is conducted on the eve of the establishment of the new Trans-Atlantic Data Transfer Framework, thus further research could assess such landmark implications on the new data transfer framework, especially, one that is a successor to the Safe Harbor and Privacy Shield decisions. Other narratives to explore could be the infringement of mass surveillance on other human rights, such as the right not to be discriminated, the right to a fair trial, and others.

BIBLIOGRAPHY

PRIMARY SOURCES:

TREATIES

1. 2000/520/EC: 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 and related frequently asked questions issued by the US Department of Commerce (notified under document number C(2000) 2441) (Text with EEA relevance.), 215 OJ L § (2000). Available on: <https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A32000D0520>. Accessed February 23, 2023.
2. 2010/87/: 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 (notified under document C(2010) 593) (Text with EEA relevance), 039 OJ L § (2010). Available on: <http://data.europa.eu/eli/dec/2010/87/oj/eng>. Accessed February 23, 2023.
3. Charter of Fundamental Rights of the European Union, 326 OJ C § (2012). Available on: http://data.europa.eu/eli/treaty/char_2012/oj/eng. Accessed February 23, 2023.
4. 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 (notified under document C(2016) 4176) (Text with EEA relevance), 207 OJ L § (2016). Available on: http://data.europa.eu/eli/dec_impl/2016/1250/oj/eng. Accessed February 23, 2023.
5. Consolidated version of the Treaty on the Functioning of the European Union, 326 OJ C § (2012). Available on: http://data.europa.eu/eli/treaty/tfeu_2012/oj/eng. Accessed February 23, 2023.
6. European Convention for the Protection of Human Rights and Fundamental Freedoms, as amended by Protocols Nos. 11 and 14, 4 November 1950, ETS 5.
7. Convention for the Protection of Individuals with Regard to the Automatic Processing of Individual Data, 28 January 1981, ETS 108.
8. 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, 281 OJ L § (1995). Available on: <http://data.europa.eu/eli/dir/1995/46/oj/eng>. Accessed February 23, 2023.
9. UN General Assembly, International Covenant on Civil and Political Rights, 16 December 1966.
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) (Text with EEA Relevance).” Available on: <https://eur-lex.europa.eu/eli/reg/2016/679/oj>. Accessed February 23, 2023.

11. Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act) (Text with EEA relevance), 265 OJ L § (2022). Available on: <http://data.europa.eu/eli/reg/2022/1925/oj/eng>. Accessed February 23, 2023.
12. Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act) (Text with EEA relevance), 277 OJ L § (2022). Available on: <http://data.europa.eu/eli/reg/2022/2065/oj/eng>. Accessed February 23, 2023.

LEGISLATION

Legislation of the United States of America

1. Executive Order 12333 of December 4, 1981. Available on: <https://dpcl.d.defense.gov/Portals/49/Documents/Civil/eo-12333-2008.pdf>. Accessed February 23, 2023.
2. Health Insurance Portability and Accountability Act of 1996 (HIPAA) June 28, 2022. Available on: <https://www.cdc.gov/phlp/publications/topic/hipaa.html>. Accessed February 23, 2023.
3. Presidential Policy Directive 28 (PPD-28) (2014). Available on: <https://www.dhs.gov/publication/presidential-policy-directive-28-ppd-28-signals-intelligence-activities>. Accessed April 1, 2023.
4. The Foreign Intelligence Surveillance Act of 1978 (FISA). Available on: <https://bja.ojp.gov/program/it/privacy-civil-liberties/authorities/statutes/1286>. Accessed February 23, 2023.

Legislation of the Republic of Ireland

1. Constitution of Ireland (last amended June 2004) July 1, 1937. Available on: <https://www.irishstatutebook.ie/eli/cons/en/html>. Accessed April 1, 2023.
2. Data Protection Act 1988. Available on: <https://www.irishstatutebook.ie/eli/1988/act/25/enacted/en/print.html>. Accessed February 23, 2023.

Legislation of the United Kingdom

1. Interception of Communications Code of Practice 2018. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/715480/Interception_of_Communications_Code_of_Practice.pdf. Accessed February 23, 2023.

2. Investigatory Powers Act 2016 (King's Printer of Acts of Parliament). Available on: <https://www.legislation.gov.uk/ukpga/2016/25/part/1/enacted>. Accessed April 1, 2023.
3. The Counter-Terrorism Act 2008. Available on: <https://www.legislation.gov.uk/ukpga/2008/28/contents>. Accessed February 23, 2023.
4. The Data Protection Act 1998. Available on: <https://www.legislation.gov.uk/ukpga/1998/29>. Accessed March 3, 2023.
5. The Security Service Act 1989. Available on: <https://www.legislation.gov.uk/ukpga/1989/5/contents>. Accessed March 3, 2023.

Legislation of the People's Republic of China

1. Cybersecurity Law of the People's Republic of China, June 1, 2017.
2. Data Security Law of the People's Republic of China, September 1, 2021.
3. Personal Information Protection Law of the People's Republic of China, November 1, 2021.

CASE LAW

Case-law of the European Court of Human Rights

1. Abdi Ibrahim v. Norway (communiquée), No. 15379/16 (ECtHR September 20, 2016).
2. Axel Springer Ag v. Germany, No. 39954/08 (ECtHR [GC] February 7, 2012).
3. Bédat v. Switzerland, No. 56925/08 (ECtHR [GC] March 29, 2016).
4. Big Brother Watch and Others v. the United Kingdom, No. 58170/13, 62322/14, 24960/15 (ECtHR [GC] May 25, 2021).
5. Denisov v. Ukraine, No. 76639/11 (ECtHR [GC] September 25, 2018).
6. Dragojević v. Croatia, No. 68955/11 (ECtHR January 15, 2015).
7. Fedotova and Others v. Russia, No. 40792/10, 30538/14, 43439/14 (ECtHR [GC] January 17, 2023).
8. Folgerø and Others v. Norway, No. 15472/02 (ECtHR [GC] June 29, 2007).
9. Hatton and Others v. the United Kingdom, No. 36022/97 (ECtHR [GC] July 8, 2003).
10. Kroon and Others v. the Netherlands, No. 18535/91 (ECtHR October 27, 1994).
11. Liberty and Others v. the United Kingdom, No. 58243/00 (ECtHR July 1, 2008).
12. López Ribalda and Others v. Spain, No. 1874/13, 8567/13 (ECtHR [GC] October 17, 2019).
13. Lozovyye v. Russia, No. 4587/09 (ECtHR April 24, 2018).
14. Mozer v. the Republic of Moldova and Russia, No. 11138/10 (ECtHR [GC] February 23, 2016).
15. Mustafa Sezgin Tanrikulu v. Turkey, No. 27473/06 (ECtHR July 18, 2017).

16. Niemietz v. Germany, No. 13710/88 (ECtHR December 16, 1992).
17. Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland, No. 931/13 (ECtHR [GC] June 27, 2017).
18. Szabó and Vissy v. Hungary, No. 37138/14 (ECtHR January 12, 2016).
19. T.c. v. Italy, No. 54032/18 (ECtHR May 19, 2022).
20. Telegraaf Media Nederland Landelijke Media B.v. and Others v. the Netherlands, No. 39315/06 (ECtHR November 22, 2012).
21. Weber and Saravia v. Germany (déc.), No. 54934/00 (ECtHR June 29, 2006).

Case-law of the Court of Justice of the European Union

1. Commission of the European Communities v. Italian Republic, No. Case C-110/05 (CJEU February 10, 2009).
2. Data Protection Commissioner v. Facebook Ireland Limited and Maximilian Schrems, No. Case C-311/18 (CJEU July 16, 2020).
3. Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others, No. Joined Cases C- 293/12 and C- 594/12 (CJEU April 8, 2014).
4. Eugen Schmidberger, Internationale Transporte und Planzüge v. Republik Österreich, No. Case C-112/00 (CJEU June 12, 2003).
5. European Commission v. Hungary, No. Case C- 288/12 (CJEU April 8, 2014).
6. European Commission v. Republic of Austria, No. Case C- 614/10 (CJEU October 16, 2012).
7. Internationale Handelsgesellschaft mbH v. Einfuhr- und Vorratsstelle für Getreide und Futtermittel, No. Case 11-70 (CJEU December 17, 1970).
8. Liselotte Hauer v. Land Rheinland-Pfalz, No. Case 44/79 (CJEU December 13, 1979).
9. Maximilian Schrems v. Data Protection Commissioner, No. Case C-362/14 (CJEU October 6, 2015).
10. Rechnungshof (C-465/00) v. Österreichischer Rundfunk and Others and Christa Neukomm (C-138/01) and Joseph Lauermann (C-139/01) v. Österreichischer Rundfunk, No. Joined cases C-465/00, C-138/01, C-139/01 (CJEU May 20, 2003).
11. Reinhard Gebhard v. Consiglio dell'Ordine degli Avvocati e Procuratori di Milano, No. Case C-55/94 (CJEU November 30, 1995).
12. Tele2 Sverige AB v. Post- och telestyrelsen and Secretary of State for the Home Department v. Tom Watson and Others, No. Joined Cases C-203/15 and C-698/15 (CJEU December 21, 2016).
13. Volker und Markus Schecke GbR (C-92/09) and Hartmut Eifert (C-93/09) v. Land Hessen, No. Joined cases C-92/09 and C-93/09 (CJEU November 9, 2010).

Case-law of the High Court of Ireland

1. Data Protection Commissioner v. Facebook Ireland Ltd and Maximillian Schrems, No. 4809 (High Court of Ireland October 3, 2017).
2. Schrems v. Data Protection Commissioner (High Court of Ireland June 18, 2014).

Case-law of the United States of America courts

1. Am. Civil Liberties Union v. Clapper, 804 F.3d 617 (United States Court of Appeals for the Second Circuit May 7, 2015).
2. Katz v. United States, 389 U.S. 347 (1967) (United States Supreme Court December 18, 1967).
3. State of Wisconsin, Plaintiff Respondent, v. Eric L. Loomis, Defendant-Appellant., No. 2015AP157-CR (Supreme Court of Wisconsin 2016).

Case-law of the Investigatory Powers Tribunal of the United Kingdom

1. Human Rights Watch Inc & Ors - And - The Secretary Of State For The Foreign & Commonwealth Office & Ors (The Investigatory Powers Tribunal May 16, 2016).
2. Liberty & Others v. the Security Service, SIS, GCHQ (The Investigatory Powers Tribunal June 22, 2015).
3. Liberty/Privacy No 2 (The Investigatory Powers Tribunal December 5, 2014).

Case-law of the Supreme Court of India

1. Justice K.S.Puttaswamy v. Union of India, No. 494 (Supreme Court of India).

OFFICIAL DOCUMENTS

1. Article 29 Working Party. "Opinion 03/2015 on the Draft Directive on the Protection of Individuals with Regard to the Processing of Personal Data by Competent Authorities for the Purposes of Prevention, Investigation, Detection or Prosecution of Criminal Offences or the Execution of Criminal Penalties, and the Free Movement of Such Data." December 1, 2015. Available on: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2015/wp233_en.pdf. Accessed April 10, 2023.
2. Department of Commerce. "Statement From U.S. Secretary of Commerce Penny Pritzker on EU-U.S. Privacy Shield," February 2, 2016. Available on: <https://2014-2017.commerce.gov/news/press-releases/2016/02/statement-us-secretary-commerce-penny-pritzker-eu-us-privacy-shield.html>. Accessed April 10, 2023.
3. OHCHR. "A/77/196: Principles Underpinning Privacy and the Protection of Personal Data." Accessed May 9, 2023. Available on: <https://www.ohchr.org/en/documents/thematic-reports/a77196-principles-underpinning-privacy-and-protection-personal-data>. Accessed April 10, 2023.
4. OHCHR. "A/HRC/51/17: The Right to Privacy in the Digital Age." Accessed May 9, 2023. Available on: <https://www.ohchr.org/en/documents/thematic-reports/ahrc5117-right-privacy-digital-age>. Accessed April 10, 2023.

5. Organisation for Economic Cooperation and Development (OECD), Guidelines Governing the Protection of Privacy and Transborder Flow of Personal Data, 23 September 1980.
6. United Nations. “Universal Declaration of Human Rights.” United Nations. United Nations. Accessed May 9, 2023. Available on: <https://www.un.org/en/about-us/universal-declaration-of-human-rights>. Accessed April 10, 2023.

SECONDARY SOURCES:

BOOKS

1. Hildebrandt, Mireille. “Profiling and the Identity of the European Citizen.” In *Profiling the European Citizen: Cross-Disciplinary Perspectives*, edited by Mireille Hildebrandt and Serge Gutwirth, 303–43. Dordrecht: Springer Netherlands, 2008. https://doi.org/10.1007/978-1-4020-6914-7_15.
2. Kulesza, Joanna, and Roy Balleste. *Cybersecurity and Human Rights in the Age of Cyberveillance*, 2015.
3. Kulhari, Shraddha. “Data Protection, Privacy and Identity: A Complex Triad.” In *Building-Blocks of a Data Protection Revolution*, 1st ed., 23–37. The Uneasy Case for Blockchain Technology to Secure Privacy and Identity. Nomos Verlagsgesellschaft mbH, 2018. <https://www.jstor.org/stable/j.ctv941qz6.7>.
4. Nissenbaum, Helen. *Privacy in Context: Technology, Policy, and the Integrity of Social Life*. Stanford: Stanford University Press, 2009. <http://www.sup.org/books/title/?id=8862>.
5. O’Neil, Cathy. *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy*. First edition. New York: Crown, 2016.
6. Pasquale, Frank. *The Black Box Society*. Harvard University Press, 2015. <http://www.jstor.org/stable/j.ctt13x0hch>.
7. Raab, Charles D. “Security, Privacy and Oversight.” In *Security in a Small Nation*, edited by Andrew W. Neal, 1st ed., 4:77–102. Scotland, Democracy, Politics. Open Book Publishers, 2017. <http://www.jstor.org/stable/j.ctt1sq5v42.8>.
8. Soskice, David and Wetenschappelijke Raad Voor Het Regeringsbeleid. “Varieties of Capitalism; Varieties of Reform.” In *Aftershocks*, edited by Anton Hemerijck, Ben Knapen, and Ellen van Doorne, 133–42. Economic Crisis and Institutional Choice. Amsterdam University Press, 2009. <http://www.jstor.org/stable/j.ctt46mtqx.16>.
9. Waldman, Ari Ezra, ed. “What Does Trust Mean for Privacy?” In *Privacy as Trust: Information Privacy for an Information Age*, 61–76. Cambridge: Cambridge University Press, 2018. <https://doi.org/10.1017/9781316888667.007>.

ARTICLES

1. Anderson, Ross. "Surveillance or Privacy?" In *Security Engineering*, 909–63. John Wiley & Sons, Ltd, 2020. <https://doi.org/10.1002/9781119644682.ch26>.
2. Andrejevic, Mark. "Big Data, Big Questions| The Big Data Divide." *International Journal of Communication* 8, no. 0 (June 16, 2014): 17. <https://ijoc.org/index.php/ijoc/article/view/2161>.
3. Borgesius, Frederik Zuiderveen, Jonathan Gray, and Mireille van Eechoud. "Open Data, Privacy, and Fair Information Principles: Towards a Balancing Framework." *Berkeley Technology Law Journal* 30, no. 3 (2015): 2073–2131. <https://www.jstor.org/stable/26377585>.
4. Brinkhoff, S. "Big Data Data Mining by the Dutch Police: Criteria for a Future Method of Investigation." *European Journal for Security Research* 2, no. 1 (April 1, 2017): 57–69. <https://doi.org/10.1007/s41125-017-0012-x>.
5. Carly Nyst. "Secrets and Lies: The Proliferation of State Surveillance Capabilities and the Legislative Secrecy Which Fortifies Them – An Activist’s Account." *State Crime Journal* 7, no. 1 (2018): 8–23. <https://doi.org/10.13169/statecrime.7.1.0008>.
6. Chadwick, Andrew, and Simon Collister. "Boundary-Drawing Power and the Renewal of Professional News Organizations: The Case of The Guardian and the Edward Snowden NSA Leak." *International Journal of Communication* 8, no. 0 (September 1, 2014): 22. <https://ijoc.org/index.php/ijoc/article/view/2883>.
7. Chaudhuri, Abhik. "Internet of Things Data Protection and Privacy in the Era of the General Data Protection Regulation." *Journal of Data Protection and Privacy* Vol-1 (December 1, 2016): 64–75.
8. Danezis, George, and Bettina Wittneben. "The Economics of Mass Surveillance," n.d.
9. Deeks, Ashley. "The Judicial Demand For Explainable Artificial Intelligence." *Columbia Law Review* 119, no. 7 (2019): 1829–50. <https://www.jstor.org/stable/26810851>.
10. Defeis, Elizabeth. "Human Rights and the European Court of Justice: An Appraisal." *Fordham International Law Journal* 31, no. 5 (January 1, 2007): 1104. <https://ir.lawnet.fordham.edu/ilj/vol31/iss5/2>.
11. Dennis, Kingsley. "Keeping a Close Watch – The Rise of Self-Surveillance and the Threat of Digital Exposure." *The Sociological Review* 56 (August 1, 2008): 347–57. <https://doi.org/10.1111/j.1467-954X.2008.00793.x>.
12. Desch, Michael C. "Democracy and Victory: Why Regime Type Hardly Matters." *International Security* 27, no. 2 (2002): 5–47. <http://www.jstor.org/stable/3092142>.
13. Dunbar, Rupert. "The Application of International Law in the Court of Justice of the European Union: Proportionality Rising." *German Law Journal* 22, no. 4 (2021): 557–92. <https://doi.org/10.1017/glj.2021.25>.
14. Fromkin, A. Michael. "The Death of Privacy?" *Stanford Law Review* 52, no. 5 (2000): 1461–1543. <https://doi.org/10.2307/1229519>.

15. Gady, Franz-Stefan. "EU/U.S. Approaches to Data Privacy and the 'Brussels Effect': A Comparative Analysis." *Georgetown Journal of International Affairs*, 2014, 12–23. <http://www.jstor.org/stable/43773645>.
16. Galantou, Dumitrina. "The Big Brother Fear." *American Intelligence Journal* 33, no. 1 (2016): 59–64. <https://www.jstor.org/stable/26202166>.
17. Giliker, Paula. "The Influence of EU and European Human Rights Law on English Private Law." *The International and Comparative Law Quarterly* 64, no. 2 (2015): 237–65. <http://www.jstor.org/stable/24760680>.
18. Goldsmith, Jack, and Tim Wu. "Who Controls the Internet?: Illusions of a Borderless World." *Faculty Books*, January 1, 2006. <https://scholarship.law.columbia.edu/books/175>.
19. Graham, Stephen, and David Wood. "Digitizing Surveillance: Categorization, Space, Inequality." *Critical Social Policy* 23, no. 2 (May 1, 2003): 227–48. <https://doi.org/10.1177/0261018303023002006>.
20. Haggerty, Kevin D. and Amber Gazso. "Seeing beyond the Ruins: Surveillance as a Response to Terrorist Threats." *The Canadian Journal of Sociology / Cahiers Canadiens de Sociologie* 30, no. 2 (2005): 169–87. <https://doi.org/10.2307/4146129>.
21. Hutchinson, Michael R. "The Margin of Appreciation Doctrine in the European Court of Human Rights." *The International and Comparative Law Quarterly* 48, no. 3 (1999): 638–50. <http://www.jstor.org/stable/761320>.
22. Kelemen, R. Daniel. "The Court of Justice of the European Union in the Twenty-First Century." *Law and Contemporary Problems* 79, no. 1 (2016): 117–40. <http://www.jstor.org/stable/43920647>.
23. Kilroy, Richard. "No Place to Hide: Edward Snowden, the NSA, and the U.S. Surveillance State. By Glenn Greenwald, New York, NY: Metropolitan Books, 2014." *Journal of Strategic Security* 9, no. 3 (October 1, 2016). <http://dx.doi.org/10.5038/1944-0472.9.3.1552>.
24. Krisch, Nico. "The Open Architecture of European Human Rights Law." *The Modern Law Review* 71, no. 2 (2008): 183–216. <http://www.jstor.org/stable/25151192>.
25. Kuner, Christopher. "Reality and Illusion in EU Data Transfer Regulation Post Schrems." *German Law Journal* 18, no. 4 (2017): 881–918. <https://doi.org/10.1017/S2071832200022197>.
26. Lyon, David. "Surveillance Culture: Engagement, Exposure, and Ethics in Digital Modernity." *International Journal of Communication* 11(2017): 824-842.
27. Lyon, David. "Surveillance, Snowden, and Big Data: Capacities, Consequences, Critique." *Big Data and Society* 1, no. 2 (2014). <https://doi.org/10.1177/2053951714541861>.
28. Martin, Aaron K., Rosamunde E. van Brakel, and Daniel J. Bernhard. "Understanding Resistance to Digital Surveillance: Towards a Multi-Disciplinary, Multi-Actor Framework." *Surveillance & Society* 6, no. 3 (April 26, 2009): 213–32. <https://doi.org/10.24908/ss.v6i3.3282>.

29. Marx, Gary T. "Murky Conceptual Waters: The Public and the Private." *Ethics and Information Technology* 3, no. 3 (September 1, 2001): 157–69. <https://doi.org/10.1023/A:1012456832336>.
30. Meijer, Albert. "Understanding the Complex Dynamics of Transparency." *Public Administration Review* 73, no. 3 (2013): 429–39. <http://www.jstor.org/stable/42002946>.
31. Mieñkowska-Norkiene, Renata. "The Political Impact of the Case Law of the Court of Justice of the European Union." *European Constitutional Law Review* 17, no. 1 (2021): 1–25. <https://doi.org/10.1017/S1574019621000080>.
32. Nissim, Kobbi, and Alexandra Wood. "Is Privacy Privacy?" *Philosophical Transactions: Mathematical, Physical and Engineering Sciences* 376, no. 2128 (2018): 1–17. <https://www.jstor.org/stable/26601760>.
33. O'Connor, Nuala, Alethea Lange, and Ali Lange. "Privacy in the Digital Age." *Great Decisions*, 2015, 17–28. <https://www.jstor.org/stable/44214790>.
34. O'leary, Síofra. "Balancing Rights In a Digital Age." *Irish Jurist* 59 (2018): 59–92. <https://www.jstor.org/stable/26431267>.
35. Paulus, Andreas. "Human Rights Protection in a European Network of Courts." *Proceedings of the ASIL Annual Meeting* 107 (2013): 174–82. <https://doi.org/10.5305/procannmeetasil.107.0174>.
36. Pozen, David E. "Privacy-Privacy Tradeoffs." *The University of Chicago Law Review* 83, no. 1 (2016): 221–47. <http://www.jstor.org/stable/43741598>.
37. Roos, Anneliese. "Core Principles of Data Protection Law." *The Comparative and International Law Journal of Southern Africa* 39, no. 1 (2006): 102–30. <https://www.jstor.org/stable/23253014>.
38. Rubinfeld, Jed. "The Right of Privacy." *Harvard Law Review* 102, no. 4 (1989): 737–807. <https://doi.org/10.2307/1341305>.
39. Schwartz, Paul M., and Daniel J. Solove. "Reconciling Personal Information in the United States and European Union." *California Law Review* 102, no. 4 (2014): 877–916. <http://www.jstor.org/stable/23784355>.
40. Sedgewick, Margaret Byrne. "Transborder Data Privacy as Trade." *California Law Review* 105, no. 5 (2017): 1513–42. <https://www.jstor.org/stable/26577713>.
41. Sklansky, David Alan. "Too Much Information: How Not to Think About Privacy and the Fourth Amendment." *California Law Review* 102, no. 5 (2014): 1069–1121. <http://www.jstor.org/stable/24758163>.
42. Slobogin, Christopher. "Privacy at Risk: The New Government Surveillance and the Fourth Amendment." *Bibliovault OAI Repository, the University of Chicago Press*, January 1, 2007. <https://doi.org/10.7208/chicago/9780226762944.001.0001>.
43. Srihari, Sargur N. "Explainable Artificial Intelligence." *Journal of the Washington Academy of Sciences* 106, no. 4 (2020): 9–38. <https://www.jstor.org/stable/27130153>.

44. Stone, Oliver, and Gary Crowdus. "Edward Snowden Is Not Your Average Hero: An Interview with Oliver Stone." *Cinéaste* 42, no. 1 (2016): 22–30. <http://www.jstor.org/stable/26356872>.
45. Waldman, Ari. "Privacy as Trust: Sharing Personal Information in a Networked World." *Articles & Chapters*, January 1, 2015. https://digitalcommons.nyls.edu/fac_articles_chapters/445.

SCHOLARLY REPORTS

1. Austin, Lisa M. "Lawful Illegality: What Snowden Has Taught Us About the Legal Infrastructure of the Surveillance State." SSRN Scholarly Paper. Rochester, NY, April 1, 2014. <https://doi.org/10.2139/ssrn.2524653>.
2. Bergen, Peter, David Sterman, Emily Schneider, and Bailey Cahall. "Do NSA's Bulk Surveillance Programs Stop Terrorists?" *New America*, 2014. JSTOR. <http://www.jstor.org/stable/resrep10476>.
3. Burwell, Frances G., and Kenneth Propp. "The Search for Digital Sovereignty." *Digital Sovereignty in Practice: Atlantic Council*, 2022. JSTOR. <http://www.jstor.org/stable/resrep44035.4>.
4. Dworkin, Anthony. "Surveillance, Privacy, and Security: Europe's Confused Response to Snowden." *European Council on Foreign Relations*, 2015. <https://www.jstor.org/stable/resrep21543>.
5. Feldstein, Steven. "Distinguishing Between Legitimate and Unlawful Surveillance." *The Global Expansion of AI Surveillance*. Carnegie Endowment for International Peace, 2019. JSTOR. <http://www.jstor.org/stable/resrep20995.6>.
6. Granmar, Claes Gustav. "A Reality Check of the Schrems Saga." SSRN Scholarly Paper. Rochester, NY, January 3, 2022. <https://papers.ssrn.com/abstract=4000713>.
7. Klein, Adam, Michèle Flournoy, and Richard Fontaine. "Defining the Problem." *SURVEILLANCE POLICY*. Center for a New American Security, 2016. JSTOR. <http://www.jstor.org/stable/resrep06418.5>.
8. Mildebrath, Hendrik. "The CJEU Judgment in the Schrems II Case." *European Parliamentary Research Service*, September 2020. [https://www.europarl.europa.eu/thinktank/en/document/EPRS_ATA\(2020\)652073](https://www.europarl.europa.eu/thinktank/en/document/EPRS_ATA(2020)652073).
9. Milko, John, and Mieke Eoyang. "Congress Should Lay Out the Welcome Mat for Whistleblowers." *Third Way*, 2018. JSTOR. <http://www.jstor.org/stable/resrep20151>.
10. Miyamoto, Inez. "Mass Surveillance and Individual Privacy." Daniel K. Inouye Asia-Pacific Center for Security Studies, 2020. JSTOR. <http://www.jstor.org/stable/resrep24871>.
11. Omtzigt, Pieter. "Mass Surveillance Report | Doc. 13734 |." *Council of Europe*, March 18, 2015. <https://pace.coe.int/en/files/21583/html>.
12. Propp, Kenneth. "Transatlantic Data Transfers." *Council on Foreign Relations*, 2021. JSTOR. <http://www.jstor.org/stable/resrep29990>.

13. Rotenberg, Marc. "Examining the EU Safe Harbor Decision and Impacts for Transatlantic Data Flows." SSRN Scholarly Paper. Rochester, NY, November 3, 2015. <https://papers.ssrn.com/abstract=3651256>.
14. Solove, Daniel J. "Understanding Privacy." SSRN Scholarly Paper. Rochester, NY, May 5, 2008. <https://papers.ssrn.com/abstract=1127888>.
15. Ünver, H. Akin. "Politics of Digital Surveillance, National Security and Privacy." Centre for Economics and Foreign Policy Studies, 2018. <https://www.jstor.org/stable/resrep17009>.
16. Wright, David, Paul Hert, and Serge Gutwirth. "Are the OECD Guidelines at 30 Showing Their Age?" *Commun. ACM* 54 (February 1, 2011): 119–27. <https://doi.org/10.1145/1897816.1897848>.
17. Zalnieriute, Monika. "Big Brother Watch and Others v. the United Kingdom." *American Journal of International Law* 116, no. 3 (2022): 585–92. <https://doi.org/10.1017/ajil.2022.35>.

NEWS ARTICLES AND BLOG POSTS

1. Faulconbridge, Guy, and Guy Faulconbridge. "UK Spies Violated Human Rights with Bulk Intercepts, European Court Rules." *Reuters*, May 25, 2021, sec. United Kingdom. Available on: <https://www.reuters.com/world/uk/uk-violated-human-rights-with-bulk-intercepts-european-rights-court-rules-2021-05-25/>. Accessed April 10, 2023.
2. Gellman, Barton, Aaron Blake, and Greg Miller. "Edward Snowden Comes Forward as Source of NSA Leaks." *Washington Post*, June 9, 2013, sec. Politics. Available on: https://www.washingtonpost.com/politics/intelligence-leaders-push-back-on-leakers-media/2013/06/09/fff80160-d122-11e2-a73e-826d299ff459_story.html. Accessed April 10, 2023.
3. Gellman, Barton. "NSA Broke Privacy Rules Thousands of Times per Year, Audit Finds." *Washington Post*, August 15, 2013, sec. National Security. Available on: https://www.washingtonpost.com/world/national-security/nsa-broke-privacy-rules-thousands-of-times-per-year-audit-finds/2013/08/15/3310e554-05ca-11e3-a07f-49ddc7417125_story.html. Accessed April 10, 2023.
4. MacAskill, Ewen, Gabriel Dance, Feilding Cage, Greg Chen, and Nadja Popovich. "NSA Files Decoded: Edward Snowden's Surveillance Revelations Explained." *The Guardian*, November 1, 2013. Available on: <http://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded>. Accessed April 10, 2023.
5. MacAskill, Ewen, Julian Borger, Nick Hopkins, Nick Davies, and James Ball. "GCHQ Taps Fibre-Optic Cables for Secret Access to World's Communications." *The Guardian*, June 21, 2013, sec. UK news. Available on: <https://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa>. Accessed April 10, 2023.
6. Ratiu, Andrea. "The European Union and the Search for Digital Sovereignty: Building 'Fortress Europe' or Preparing for a New World?" *Atlantic Council* (blog), June 22, 2020. Available on: <https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/the-european-union-and-the-search-for-digital-sovereignty/>. Accessed April 10, 2023.

7. Smale, Alison. "German Leader Criticizes U.S. Over Pervasive Surveillance." *The New York Times*, January 29, 2014, sec. World. Available on: <https://www.nytimes.com/2014/01/30/world/europe/german-leader-criticizes-united-states-over-surveillance.html>. Accessed April 10, 2023.
8. Sorkin, Amy Davidson. "Edward Snowden, The N.S.A. Leaker, Comes Forward." *The New Yorker*, June 9, 2013. Available on: <https://www.newyorker.com/news/amy-davidson/edward-snowden-the-n-s-a-leaker-comes-forward>. Accessed April 10, 2023.
9. The Guardian. "NSA Prism Program Slides," November 1, 2013. Available on: <http://www.theguardian.com/world/interactive/2013/nov/01/prism-slides-nsa-document>. Accessed April 10, 2023.
10. US News & World Report. "US Expects Fallout From Snowden Leaks for Years to Come." Accessed May 9, 2023. Available on: [//www.usnews.com/news/world/articles/2018-06-03/5-years-on-us-government-still-counting-snowden-leak-costs](http://www.usnews.com/news/world/articles/2018-06-03/5-years-on-us-government-still-counting-snowden-leak-costs). Accessed April 10, 2023.

WEBSITES

1. Amnesty International. "Easy Guide to Mass Surveillance," March 18, 2015. Available on: <https://www.amnesty.org/en/latest/campaigns/2015/03/easy-guide-to-mass-surveillance/>. Accessed April 10, 2023.
2. Amnesty International. "UK: Europe's Top Court Rules UK Mass Surveillance Regime Violated Human Rights," May 25, 2021. Available on: <https://www.amnesty.org/en/latest/press-release/2021/05/uk-surveillance-gchq-ecthr-ruling/>. Accessed April 10, 2023.
3. Banksy Explained. "One Nation Under CCTV, 2007," May 7, 2021. Available on: <https://banksyexplained.com/one-nation-under-cctv-2007/>. Accessed April 10, 2023.
4. Britannica "What is the Difference Between the Deep Web and the Dark Web?" Available on: <https://www.britannica.com/story/whats-the-difference-between-the-deep-web-and-the-dark-web>. Accessed April 10, 2023.
5. European Commission. "EU-U.S. Data Privacy Framework, Draft Adequacy Decision." Text. Available on: https://ec.europa.eu/commission/presscorner/detail/en/qanda_22_7632. Accessed April 10, 2023.
6. European Data Protection Board. "Frequently Asked Questions on the Judgment of the Court of Justice of the European Union in Case C-311/18 - Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems." Available on: https://edpb.europa.eu/our-work-tools/our-documents/other/frequently-asked-questions-judgment-court-justice-european-union_en. Accessed April 10, 2023.
7. European Data Protection Supervisor. "Data Protection and Use of Cloud by Public Sector: The EDPS Initiates and Participates in the 2022 Coordinated Enforcement Action of the EDPB," May 23, 2023. Available on: <https://edps.europa.eu/press-publications/press-news/press-releases/2022/data-protection-and-use-cloud-public-sector-edps>. Accessed April 10, 2023.

8. European Data Protection Supervisor. “EDPB Welcomes Improvements under the EU-U.S. Data Privacy Framework, but Concerns Remain.” Available on: https://edpb.europa.eu/news/news/2023/edpb-welcomes-improvements-under-eu-us-data-privacy-framework-concerns-remain_en. Accessed April 10, 2023.
9. European Data Protection Supervisor. “Outcome of Own-Initiative Investigation into EU Institutions’ Use of Microsoft Products and Services.” Available on: <https://edps.europa.eu/data-protection/our-work/publications/investigations/outcome-own-initiative-investigation-eu>. Accessed April 10, 2023.
10. European Data Protection Supervisor. “Rebuilding Trust in EU-US Data.” Available on: https://edps.europa.eu/data-protection/our-work/publications/opinions/rebuilding-trust-eu-us-data-flows_en. Accessed April 10, 2023.
11. European Union Agency for Fundamental Rights. “Surveillance by Intelligence Services: Fundamental Rights Safeguards and Remedies in the European Union – Volume II – Summary,” May 9, 2018. Available on: <http://fra.europa.eu/en/publication/2018/surveillance-intelligence-services-fundamental-rights-safeguards-and-remedies>. Accessed April 10, 2023.
12. Europol. “European Union Terrorism Situation and Trend Report 2022 (TE-SAT).” Available on: <https://www.europol.europa.eu/publication-events/main-reports/european-union-terrorism-situation-and-trend-report-2022-te-sat>. Accessed April 10, 2023.
13. Government of the United Kingdom. “Responding to Human Rights Judgments: 2021 to 2022.” Available on: <https://www.gov.uk/government/publications/responding-to-human-rights-judgments-2021-to-2022>. Accessed April 10, 2023.
14. International Commission of Jurists. “Big Brother Watch v. UK: A Landmark Judgment Missing the Mark,” June 4, 2021. Available on: <https://www.icj.org/big-brother-watch-v-uk-a-landmark-judgment-missing-the-mark/>. Accessed April 10, 2023.
15. Lawfare. “Geopolitical Implications of the European Court’s Schrems II Decision,” July 17, 2020. Available on: <https://www.lawfareblog.com/geopolitical-implications-european-courts-schrems-ii-decision>. Accessed April 10, 2023.
16. Luxembourg, U. S. Mission. “U.S. Secretary of Commerce Wilbur Ross Statement on Schrems II Ruling and the Importance of EU-U.S. Data Flows.” U.S. Embassy in Luxembourg, July 16, 2020. Available on: <https://lu.usembassy.gov/u-s-secretary-of-commerce-wilbur-ross-statement-on-schrems-ii-ruling-and-the-importance-of-eu-u-s-data-flows/>. Accessed April 10, 2023.
17. Monteleone, Shara, and Laura Puccio. “From Safe Harbour to Privacy Shield. Advances and Shortcomings of the New EU-US Data Transfer Rules.,” January 2017. Available on: [https://www.europarl.europa.eu/RegData/etudes/IDAN/2017/595892/EPRS_IDA\(2017\)595892_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/IDAN/2017/595892/EPRS_IDA(2017)595892_EN.pdf). Accessed April 10, 2023.
18. Parliament of the United Kingdom. “The Intelligence Services.” Available on: <https://www.parliament.uk/business/publications/research/key-issues-parliament-2015/defence-and-security/intelligence-services/>. Accessed April 10, 2023.

19. Privacy International. "UK Government Acknowledges Past Violations of Individuals' Rights and the Fight Continues..." Available on: <http://privacyinternational.org/news-analysis/4818/uk-government-acknowledges-past-violations-individuals-rights-and-fight>. Accessed April 10, 2023.
20. Think Tank, European Parliament. "US: Economic Indicators and Trade with the EU." Available on: [https://www.europarl.europa.eu/thinktank/en/document/EPRS_ATA\(2016\)583777](https://www.europarl.europa.eu/thinktank/en/document/EPRS_ATA(2016)583777). Accessed April 10, 2023.

ANNEX 1. GENERAL DATA PROTECTION REGULATION

Relevant provisions of General Data Protection Regulation.³⁶⁷

Article 4(1)

(1) ‘personal data’ means any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Article 4(2)

(2) ‘processing’ means 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.

Article 4(4)

(4) ‘profiling’ means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.

Article 23 (in the context of Schrems II and applicable version)

‘1. Union or Member State law to which the data controller or processor is subject may restrict by way of a legislative measure the scope of the obligations and rights provided for in Articles 12 to 22 and Article 34, as well as Article 5 in so far as its provisions correspond to the rights and obligations provided for in Articles 12 to 22, when such a restriction respects the essence of the fundamental rights and freedoms and is a necessary and proportionate measure in a democratic society to safeguard:

- (a) national security;
- (b) defence;
- (c) public security;
- (d) the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security;
- (...)

³⁶⁷ 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) (Text with EEA Relevance).” Available on: <https://eur-lex.europa.eu/eli/reg/2016/679/oj>. Accessed February 23, 2023.

2. In particular, any legislative measure referred to in paragraph 1 shall contain specific provisions at least, where relevant, as to:

- (a) the purposes of the processing or categories of processing;
- (b) the categories of personal data;
- (c) the scope of the restrictions introduced;
- (d) the safeguards to prevent abuse or unlawful access or transfer;
- (e) the specification of the controller or categories of controllers;
- (f) the storage periods and the applicable safeguards taking into account the nature, scope and purposes of the processing or categories of processing;
- (g) the risks to the rights and freedoms of data subjects; and
- (h) the right of data subjects to be informed about the restriction, unless that may be prejudicial to the purpose of the restriction.’

Article 46(1) (in the context of Schrems II and applicable version)

‘1. In the absence of a decision pursuant to Article 45(3), a controller or processor may transfer personal data to a third country or an international organisation only if the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available.

Article 46(2)(c) (in the context of Schrems II and applicable version)

2. The appropriate safeguards referred to in paragraph 1 may be provided for, without requiring any specific authorisation from a supervisory authority, by:

(...)

- (c) standard data protection clauses adopted by the Commission in accordance with the examination procedure referred to in Article 93(2).

ANNEX 2. CHARTER OF FUNDAMENTAL RIGHTS OF THE EUROPEAN UNION

Relevant provisions of Charter of Fundamental Rights of the European Union.³⁶⁸

Article 7 - Respect for private and family life

Everyone has the right to respect for his or her private and family life, home and communications.

Article 8 - Protection of personal data

1. Everyone has the right to the protection of personal data concerning him or her.
2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.
3. Compliance with these rules shall be subject to control by an independent authority.

Article 47 - Right to an effective remedy and to a fair trial

Everyone whose rights and freedoms guaranteed by the law of the Union are violated has the right to an effective remedy before a tribunal in compliance with the conditions laid down in this Article.

Everyone is entitled to a fair and public hearing within a reasonable time by an independent and impartial tribunal previously established by law. Everyone shall have the possibility of being advised, defended and represented.

Legal aid shall be made available to those who lack sufficient resources in so far as such aid is necessary to ensure effective access to justice.

Article 52(1) - Scope and interpretation of rights and principles

1. Any limitation on the exercise of the rights and freedoms recognised by this Charter must be provided for by law and respect the essence of those rights and freedoms. Subject to the principle of proportionality, limitations may be made only if they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others.

³⁶⁸ Charter of Fundamental Rights of the European Union, 326 OJ C § (2012). Available on: http://data.europa.eu/eli/treaty/char_2012/oj/eng. Accessed February 23, 2023.

ANNEX 3. EUROPEAN CONVENTION ON HUMAN RIGHTS

Relevant provisions of European Convention on Human Rights.³⁶⁹

Preamble

The Governments signatory hereto, being members of the Council of Europe,

Considering the Universal Declaration of Human Rights proclaimed by the General Assembly of the United Nations on 10th December 1948; Considering that this Declaration aims at securing the universal and effective recognition and observance of the Rights therein declared;

Considering that the aim of the Council of Europe is the achievement of greater unity between its members and that one of the methods by which that aim is to be pursued is the maintenance and further realisation of Human Rights and Fundamental Freedoms;

Reaffirming their profound belief in those fundamental freedoms which are the foundation of justice and peace in the world and are best maintained on the one hand by an effective political democracy and on the other by a common understanding and observance of the Human Rights upon which they depend;

Being resolved, as the governments of European countries which are like-minded and have a common heritage of political traditions, ideals, freedom and the rule of law, to take the first steps for the collective enforcement of certain of the rights stated in the Universal Declaration,

Affirming that the High Contracting Parties, in accordance with the principle of subsidiarity, have the primary responsibility to secure the rights and freedoms defined in this Convention and the Protocols thereto, and that in doing so they enjoy a margin of appreciation, subject to the supervisory jurisdiction of the European Court of Human Rights established by this Convention,

Have agreed as follows, (...)

Article 8 - Right to respect for private and family life

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

³⁶⁹ European Convention for the Protection of Human Rights and Fundamental Freedoms, as amended by Protocols Nos. 11 and 14, 4 November 1950, ETS 5.

ANNEX 4. INTERNATIONAL COVENANT ON CIVIL AND POLITICAL RIGHTS

Relevant provision of International Covenant on Civil and Political Rights.³⁷⁰

Article 17

1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.
2. Everyone has the right to the protection of the law against such interference or attacks.

³⁷⁰ UN General Assembly, International Covenant on Civil and Political Rights, 16 December 1966.

ANNEX 5. UNIVERSAL DECLARATION OF HUMAN RIGHTS

Relevant provision of Universal Declaration of Human Rights.³⁷¹

Article 12

No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.

³⁷¹ United Nations. "Universal Declaration of Human Rights." United Nations. United Nations. Accessed May 9, 2023. Available on: <https://www.un.org/en/about-us/universal-declaration-of-human-rights>. Accessed April 10, 2023.

ANNEX 6. INFOGRAPHIC - TERRORISM IN THE EU

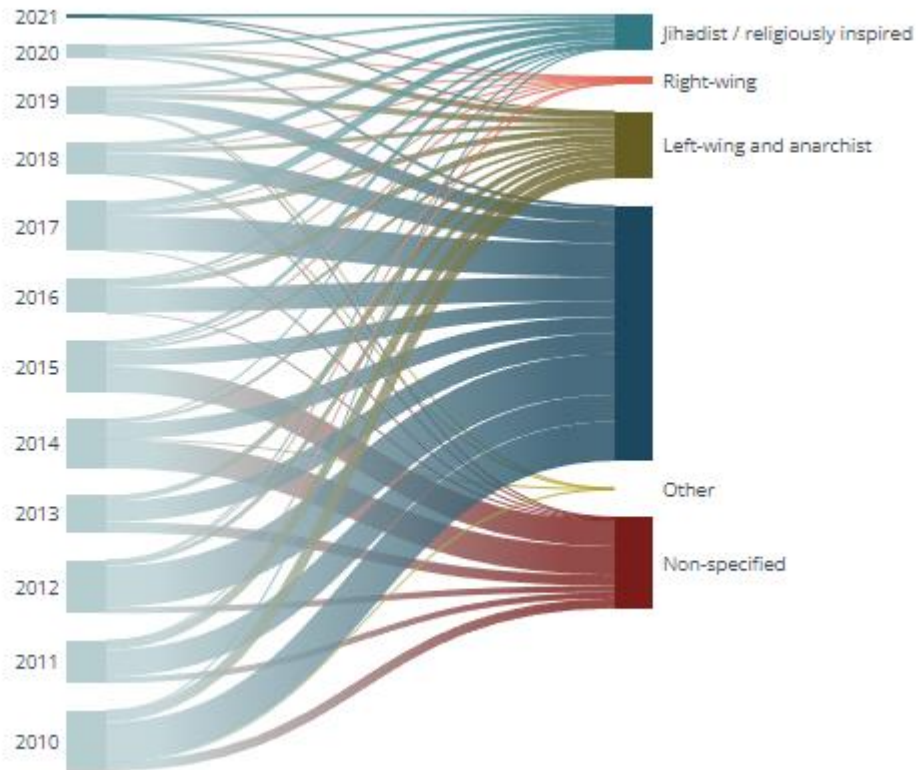


Figure 6.1. Terrorist attacks in the EU by type (2010-2021)³⁷²

³⁷² Europol. “European Union Terrorism Situation and Trend Report 2022 (TE-SAT).” Available on: <https://www.europol.europa.eu/publication-events/main-reports/european-union-terrorism-situation-and-trend-report-2022-te-sat>. Accessed April 10, 2023.

ANNEX 7. BANKSY MURAL “ONE NATION UNDER CCTV”

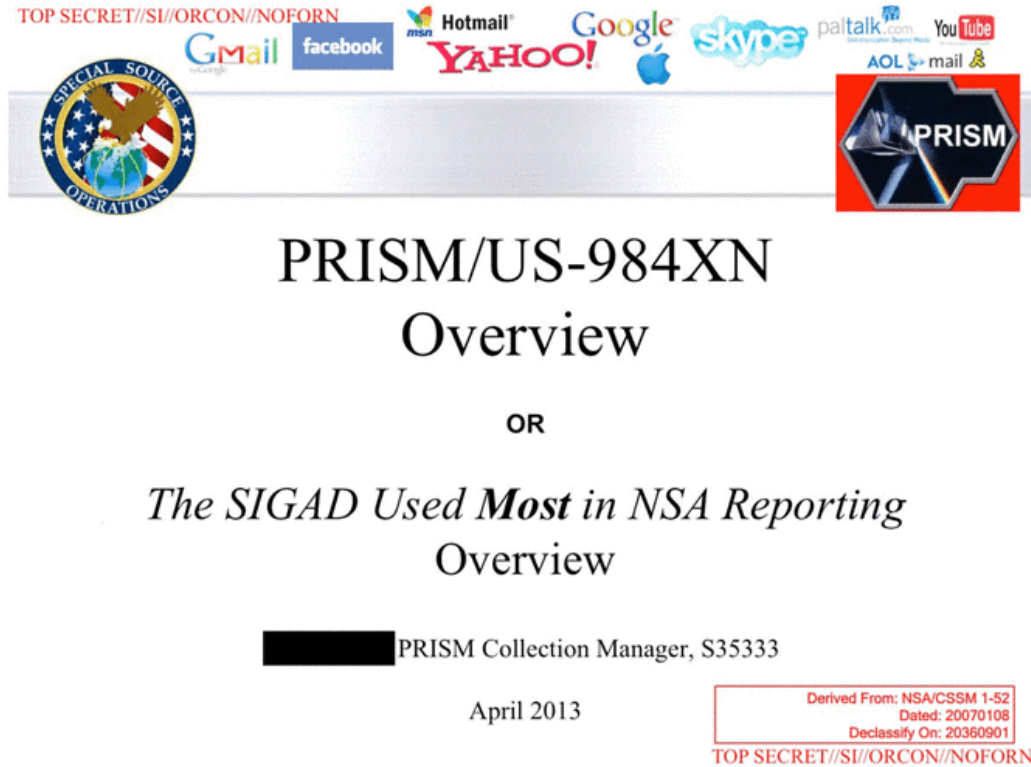


Figure 7.1. Banksy Mural “One Nation Under CCTV”³⁷³

³⁷³ Banksy Explained. “One Nation Under CCTV, 2007,” May 7, 2021. Available on: <https://banksyexplained.com/one-nation-under-cctv-2007/>. Accessed April 10, 2023.

ANNEX 8. PRISM/US-984XN OVERVIEW

Following information presented in the slide form reflects Snowden's revelations and are available to the public.³⁷⁴



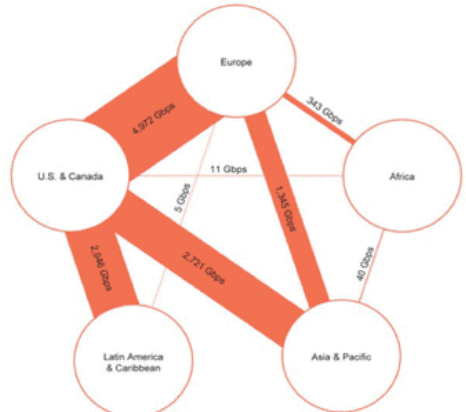
The slide features a header with the classification marking "TOP SECRET//SI//ORCON//NOFORN" in red. Below this, a row of logos includes Gmail, facebook, Hotmail, YAHOO!, Google, Apple, skype, paltalk.com, and YouTube. To the left is the "SPECIAL SOURCE OPERATIONS" logo, and to the right is the "PRISM" logo. The main title is "PRISM/US-984XN Overview" in large black font, followed by "OR" and "The SIGAD Used **Most** in NSA Reporting Overview" in a smaller, italicized font. Below the title is a redacted name followed by "PRISM Collection Manager, S35333" and the date "April 2013". A red box in the bottom right corner contains the text: "Derived From: NSA/CSSM 1-52", "Dated: 20070108", "Declassify On: 20360901", and "TOP SECRET//SI//ORCON//NOFORN" in red.

Figure 8.1. PRISM slide No. 1³⁷⁵

³⁷⁴ The Guardian. "NSA Prism Program Slides," November 1, 2013. Available on: <http://www.theguardian.com/world/interactive/2013/nov/01/prism-slides-nsa-document>. Accessed April 10, 2023.

³⁷⁵ *Ibid.*

- Much of the world's communications flow through the U.S.
- A target's phone call, e-mail or chat will take the **cheapest** path, **not the physically most direct** path – you can't always predict the path.
- Your target's communications could easily be flowing into and through the U.S.



International Internet Regional Bandwidth Capacity in 2011
 Source: Telegeography Research
 TOP SECRET//SI//ORCON//NOFORN

Figure 8.2. PRISM slide No. 2³⁷⁶

TOP SECRET//SI//ORCON//NOFORN

Special Source Operations (TS//SI//NF)

FAA702 Operations
 Two Types of Collection

PRISM

Upstream

- Collection of communications on fiber cables and infrastructure as data flows past. (FAIRVIEW, STORMBREW, BLARNEY, OAKSTAR)

PRISM

- Collection directly from the servers of these U.S. Service Providers: Microsoft, Yahoo, Google, Facebook, PalTalk, AOL, Skype, YouTube, Apple.

You Should Use Both

TOP SECRET//SI//ORCON//NOFORN

Figure 8.3. PRISM slide No. 3³⁷⁷

³⁷⁶ Ibid.
³⁷⁷ Ibid.

TOP SECRET//SI//ORCON//NOFORN

Gmail facebook msn Hotmail Google skype paltalk.com YouTube AOL mail

SPECIAL SOURCE OPERATIONS (TS//SI//NF) **FAA702 Operations** **PRISM**
Why Use Both: PRISM vs. Upstream

	PRISM	Upstream
DNI Selectors	9 U.S. based service providers ✓	Worldwide sources ✓
DNR Selectors	Coming soon ✗	Worldwide sources ✓
Access to Stored Communications (Search)	✓	✗
Real-Time Collection (Surveillance)	✓	✓
“Abouts” Collection	✗	✓
Voice Collection	✓ Voice over IP	✓
Direct Relationship with Comms Providers	✗ Only through FBI	✓

TOP SECRET//SI//ORCON//NOFORN

Figure 8.4. PRISM slide No. 4³⁷⁸

TOP SECRET//SI//ORCON//NOFORN

Gmail facebook msn Hotmail Google skype paltalk.com YouTube AOL mail

SPECIAL SOURCE OPERATIONS (TS//SI//NF) **PRISM Collection Details** **PRISM**

Current Providers

- Microsoft (Hotmail, etc.)
- Google
- Yahoo!
- Facebook
- PalTalk
- YouTube
- Skype
- AOL
- Apple

What Will You Receive in Collection (Surveillance and Stored Comms)?
 It varies by provider. In general:

- 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**

Complete list and details on PRISM web page:
 Go PRISMFAA

TOP SECRET//SI//ORCON//NOFORN

Figure 8.5. PRISM slide No. 5³⁷⁹

³⁷⁸ Ibid.

³⁷⁹ Ibid.

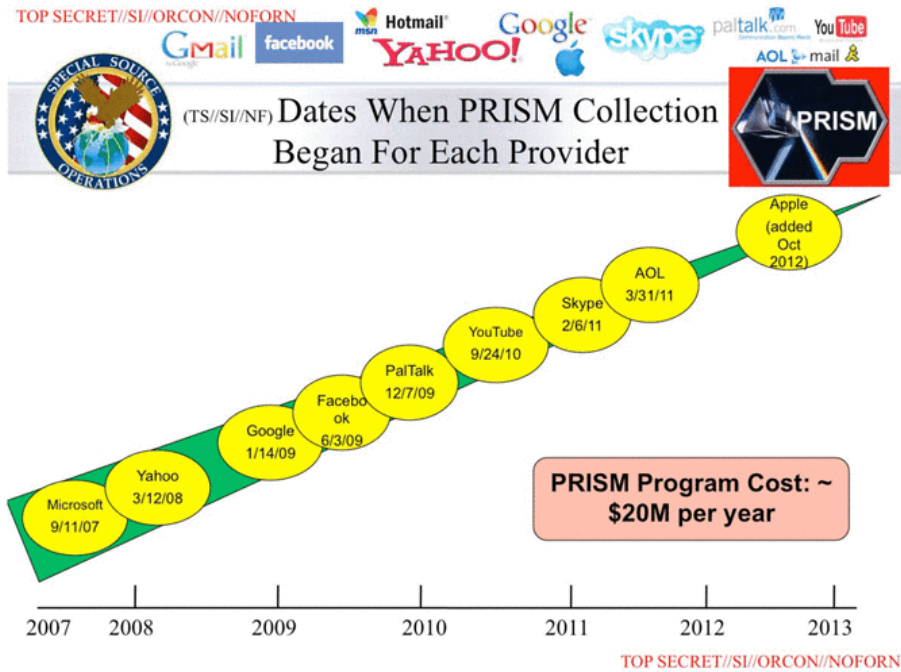


Figure 8.6. PRISM slide No. 6³⁸⁰



Figure 8.7. PRISM slide No. 7³⁸¹

³⁸⁰ Ibid.

³⁸¹ Ibid.

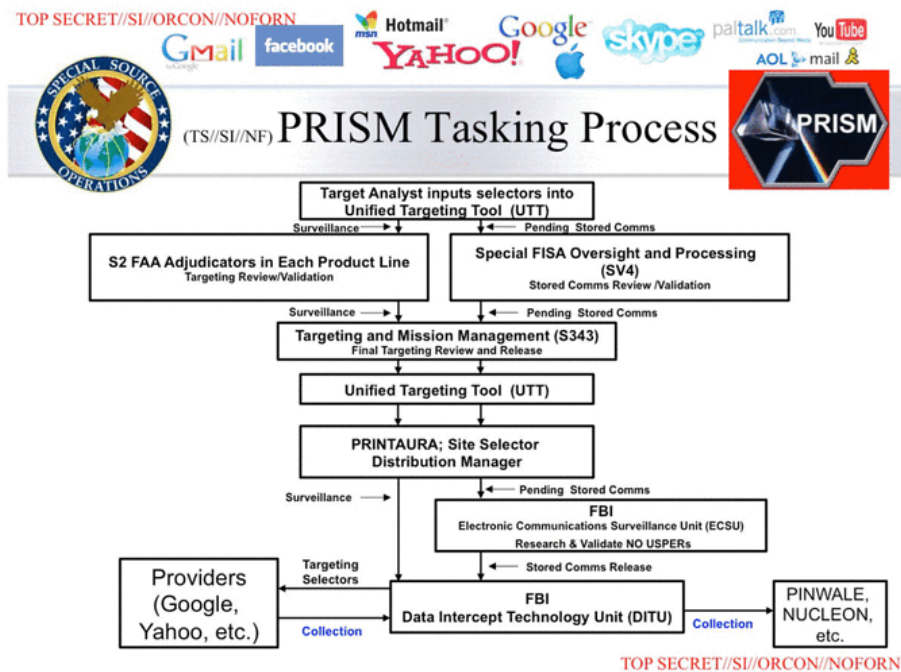


Figure 8.8. PRISM slide No. 8³⁸²

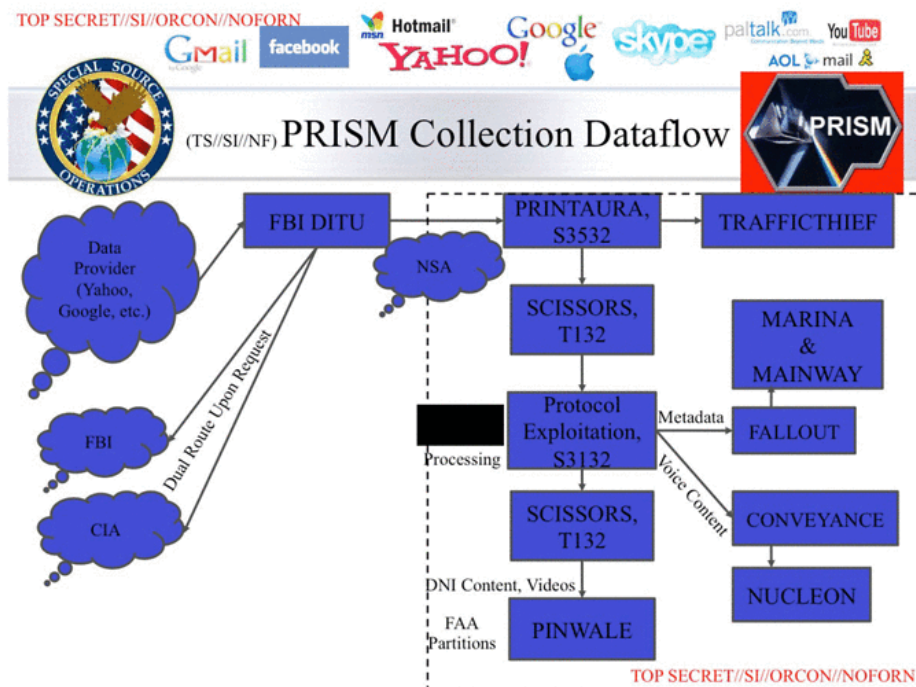


Figure 8.9. PRISM slide No. 9³⁸³

³⁸² Ibid.

³⁸³ Ibid.

TOP SECRET//SI//ORCON//NOFORN

Gmail facebook msn Hotmail® Google skype paltalk.com YouTube AOL mail

SPECIAL SOURCE OPERATIONS (TS//SI//NF) PRISM Case Notations PRISM

P2ESQC120001234

PRISM Provider
P1: Microsoft
P2: Yahoo
P3: Google
P4: Facebook
P5: PalTalk
P6: YouTube
P7: Skype
P8: AOL
PA: Apple

Fixed trigraph, denotes PRISM source collection

Year CASN established for selector

Serial #

Content Type
A: Stored Comms (Search)
B: IM (chat)
C: RTN-EDC (real-time notification of an e-mail event such as a login or sent message)
D: RTN-IM (real-time notification of a chat login or logout event)
E: E-Mail
F: VoIP
G: Full (WebForum)
H: OSN Messaging (photos, wallposts, activity, etc.)
I: OSN Basic Subscriber Info
J: Videos
. (dot): Indicates multiple types

TOP SECRET//SI//ORCON//NOFORN

Figure 8.10. PRISM slide No. 10³⁸⁴

TOP SECRET//SI//ORCON//NOFORN

Gmail facebook msn Hotmail® Google skype paltalk.com YouTube AOL mail

SPECIAL SOURCE OPERATIONS (TS//SI//NF) REPRISMFISA TIPS PRISM

DYNAMIC PAGE - HIGHEST POSSIBLE CLASSIFICATION IS TOP SECRET//SI//ORCON//NOFORN

REPRISMFISA COUNTERTERRORISM

2013-Apr-05 13:10:20

Click on the PRISM icon first (from the initial webpage)

PRISM ENTRIES
Last Load on Apr 05, 2013 at 12:22 PM GMT

Check the total record status, click on this link.

QUICK LINKS

- See Entire List (Current)
- See Entire List (Expired)
- See Entire List (Current and Expired)
- See NSA List
- See New Records
- Ownership Count

If the total count is much less than this, REPRISMFISA is having issues. E-MAIL THE REPRISMFISA HELP DESK AT [redacted]

AND INFORM THEM

Records 1 - 58 out of 117875 Page 1 of 2254 Records per page: 50

Clear Sort Order Click on column headers to sort, * in column is not sortable.

SEARCH
This search form below can be used as a filter to see a partial list of records.

Search For: [input]
AND OR
Expiration days (0-9999 days) [input]
Filter

Prism Current Entries

TOP SECRET//SI//ORCON//NOFORN

Figure 8.11. PRISM slide No. 11³⁸⁵

384 Ibid.

385 Ibid.

ANNEX 9. TREATY OF THE FUNCTIONING OF THE EUROPEAN UNION

Relevant provision of the Treaty on the Functioning of the European Union.³⁸⁶

Article 267

The Court of Justice of the European Union shall have jurisdiction to give preliminary rulings concerning:

- (a) the interpretation of the Treaties;
- (b) the validity and interpretation of acts of the institutions, bodies, offices or agencies of the Union;

Where such a question is raised before any court or tribunal of a Member State, that court or tribunal may, if it considers that a decision on the question is necessary to enable it to give judgment, request the Court to give a ruling thereon.

Where any such question is raised in a case pending before a court or tribunal of a Member State against whose decisions there is no judicial remedy under national law, that court or tribunal shall bring the matter before the Court.

If such a question is raised in a case pending before a court or tribunal of a Member State with regard to a person in custody, the Court of Justice of the European Union shall act with the minimum of delay.

³⁸⁶ Consolidated version of the Treaty on the Functioning of the European Union, 326 OJ C § (2012). Available on: http://data.europa.eu/eli/treaty/tfeu_2012/oj/eng. Accessed February 23, 2023.

ANNEX 10. DIRECTIVE 95/46/EC

Relevant provision of the Directive 95/46/EC.³⁸⁷

Article 25(6)

The Commission may find, in accordance with the procedure referred to in Article 31 (2), that a third country ensures an adequate level of protection within the meaning of paragraph 2 of this Article, by reason of its domestic law or of the international commitments it has entered into, particularly upon conclusion of the negotiations referred to in paragraph 5, for the protection of the private lives and basic freedoms and rights of individuals.

Article 28

Supervisory authority

1. Each Member State shall provide that one or more public authorities are responsible for monitoring the application within its territory of the provisions adopted by the Member States pursuant to this Directive.

These authorities shall act with complete independence in exercising the functions entrusted to them.

2. Each Member State shall provide that the supervisory authorities are consulted when drawing up administrative measures or regulations relating to the protection of individuals' rights and freedoms with regard to the processing of personal data.
3. Each authority shall in particular be endowed with:
 - investigative powers, such as powers of access to data forming the subject-matter of processing operations and powers to collect all the information necessary for the performance of its supervisory duties,
 - effective powers of intervention, such as, for example, that of delivering opinions before processing operations are carried out, in accordance with Article 20, and ensuring appropriate publication of such opinions, of ordering the blocking, erasure or destruction of data, of imposing a temporary or definitive ban on processing, of warning or admonishing the controller, or that of referring the matter to national parliaments or other political institutions,
 - the power to engage in legal proceedings where the national provisions adopted pursuant to this Directive have been violated or to bring these violations to the attention of the judicial authorities.
 - Decisions by the supervisory authority which give rise to complaints may be appealed against through the courts.
4. Each supervisory authority shall hear claims lodged by any person, or by an association representing that person, concerning the protection of his rights and freedoms in regard to the

³⁸⁷ 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, 281 OJ L § (1995). Available on: <http://data.europa.eu/eli/dir/1995/46/oj/eng>. Accessed February 23, 2023.

processing of personal data. The person concerned shall be informed of the outcome of the claim.

Each supervisory authority shall, in particular, hear claims for checks on the lawfulness of data processing lodged by any person when the national provisions adopted pursuant to Article 13 of this Directive apply. The person shall at any rate be informed that a check has taken place.

5. Each supervisory authority shall draw up a report on its activities at regular intervals. The report shall be made public.
6. Each supervisory authority is competent, whatever the national law applicable to the processing in question, to exercise, on the territory of its own Member State, the powers conferred on it in accordance with paragraph 3. Each authority may be requested to exercise its powers by an authority of another Member State.

The supervisory authorities shall cooperate with one another to the extent necessary for the performance of their duties, in particular by exchanging all useful information.

7. Member States shall provide that the members and staff of the supervisory authority, even after their employment has ended, are to be subject to a duty of professional secrecy with regard to confidential information to which they have access.

ANNEX 11. SAFE HARBOR DECISION

Relevant provision of the Safe Harbor decision.³⁸⁸

Article 1

Object of the Directive

1. In accordance with this Directive, Member States shall protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data.
2. Member States shall neither restrict nor prohibit the free flow of personal data between Member States for reasons connected with the protection afforded under paragraph 1.

Article 2

Definitions

For the purposes of this Directive:

- (a) 'personal data' shall mean any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity;
- (b) 'processing of personal data' ('processing') shall mean any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction;
- (c) 'personal data filing system' ('filing system') shall mean any structured set of personal data which are accessible according to specific criteria, whether centralized, decentralized or dispersed on a functional or geographical basis;
- (d) 'controller' shall mean the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data; where the purposes and means of processing are determined by national or Community laws or regulations, the controller or the specific criteria for his nomination may be designated by national or Community law;
- (e) 'processor' shall mean a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller;

³⁸⁸ 2000/520/EC: 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 and related frequently asked questions issued by the US Department of Commerce (notified under document number C(2000) 2441) (Text with EEA relevance.), 2000 OJ L 215 § (2000). Available on: <https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A32000D0520>. Accessed February 23, 2023.

(f) 'third party' shall mean any natural or legal person, public authority, agency or any other body other than the data subject, the controller, the processor and the persons who, under the direct authority of the controller or the processor, are authorized to process the data;

(g) 'recipient' shall mean a natural or legal person, public authority, agency or any other body to whom data are disclosed, whether a third party or not; however, authorities which may receive data in the framework of a particular inquiry shall not be regarded as recipients;

(h) 'the data subject's consent' shall mean any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed.

Article 3

Scope

1. This Directive shall apply to the processing of personal data wholly or partly by automatic means, and to the processing otherwise than by automatic means of personal data which form part of a filing system or are intended to form part of a filing system.
2. This Directive shall not apply to the processing of personal data:
 - in the course of an activity which falls outside the scope of Community law, such as those provided for by Titles V and VI of the Treaty on European Union and in any case to processing operations concerning public security, defence, State security (including the economic well-being of the State when the processing operation relates to State security matters) and the activities of the State in areas of criminal law,
 - by a natural person in the course of a purely personal or household activity.

Article 4

National law applicable

1. Each Member State shall apply the national provisions it adopts pursuant to this Directive to the processing of personal data where:
 - (a) the processing is carried out in the context of the activities of an establishment of the controller on the territory of the Member State; when the same controller is established on the territory of several Member States, he must take the necessary measures to ensure that each of these establishments complies with the obligations laid down by the national law applicable;
 - (b) the controller is not established on the Member State's territory, but in a place where its national law applies by virtue of international public law;
 - (c) the controller is not established on Community territory and, for purposes of processing personal data makes use of equipment, automated or otherwise, situated on the territory of the said Member State, unless such equipment is used only for purposes of transit through the territory of the Community.
2. In the circumstances referred to in paragraph 1 (c), the controller must designate a representative established in the territory of that Member State, without prejudice to legal actions which could be initiated against the controller himself.

ANNEX 12. THE FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978

Relevant provision of the Foreign Intelligence Surveillance Act of 1978.³⁸⁹

Section 702 - PROCEDURES FOR TARGETING CERTAIN PERSONS OUTSIDE THE UNITED STATES OTHER THAN UNITED STATES PERSONS.

“(a) AUTHORIZATION.—Notwithstanding any other provision of law, upon the issuance of an order in accordance with subsection (i)(3) or a determination under subsection (c)(2), the Attorney General and the Director of National Intelligence may authorize jointly, for a period of up to 1 year from the effective date of the authorization, the targeting of persons reasonably believed to be located outside the United States to acquire foreign intelligence information.

“(b) LIMITATIONS.—An acquisition authorized under subsection (a)— “(1) may not intentionally target any person known at the time of acquisition to be located in the United States; “(2) may not intentionally target a person reasonably believed to be located outside the United States if the purpose of such acquisition is to target a particular, known person reasonably believed to be in the United States; “(3) may not intentionally target a United States person reasonably believed to be located outside the United States; “(4) may not intentionally acquire any communication as to which the sender and all intended recipients are known at the time of the acquisition to be located in the United States; and “(5) shall be conducted in a manner consistent with the fourth amendment to the Constitution of the United States.

“(c) CONDUCT OF ACQUISITION.— “(1) IN GENERAL.—An acquisition authorized under subsection (a) shall be conducted only in accordance with— “(A) the targeting and minimization procedures adopted in accordance with subsections (d) and (e); and “(B) upon submission of a certification in accordance with subsection (g), such certification.

“(2) DETERMINATION.—A determination under this paragraph and for purposes of subsection (a) is a determination by the Attorney General and the Director of National Intelligence that exigent circumstances exist because, without immediate implementation of an authorization under subsection (a), intelligence important to the national security of the United States may be lost or not timely acquired and time does not permit the issuance of an order pursuant to subsection (i)(3) prior to the implementation of such authorization.

“(3) TIMING OF DETERMINATION.—The Attorney General and the Director of National Intelligence may make the determination under paragraph (2)— “(A) before the submission of a certification in accordance with subsection (g); or “(B) by amending a certification pursuant to subsection (i)(1)(C) at any time during which judicial review under subsection (i) of such certification is pending.

“(4) CONSTRUCTION.—Nothing in title I shall be construed to require an application for a court order under such title for an acquisition that is targeted in accordance with this section at a person reasonably believed to be located outside the United States.

“(d) TARGETING PROCEDURES.—

³⁸⁹ The Foreign Intelligence Surveillance Act of 1978 (FISA). Available on: <https://bja.ojp.gov/program/it/privacy-civil-liberties/authorities/statutes/1286>. Accessed February 23, 2023.

“(1) REQUIREMENT TO ADOPT.—The Attorney General, in consultation with the Director of National Intelligence, shall adopt targeting procedures that are reasonably designed to— “(A) ensure that any acquisition authorized under subsection (a) is limited to targeting persons reasonably believed to be located outside the United States; and “(B) prevent the intentional acquisition of any communication as to which the sender and all intended recipients are known at the time of the acquisition to be located in the United States.

“(2) JUDICIAL REVIEW.—The procedures adopted in accordance with paragraph (1) shall be subject to judicial review pursuant to subsection (i).

“(e) MINIMIZATION PROCEDURES.—

“(1) REQUIREMENT TO ADOPT.—The Attorney General, in consultation with the Director of National Intelligence, shall adopt minimization procedures that meet the definition of minimization procedures under section 101(h) or 301(4), as appropriate, for acquisitions authorized under subsection (a).

“(2) JUDICIAL REVIEW.—The minimization procedures adopted in accordance with paragraph (1) shall be subject to judicial review pursuant to subsection (i).

“(f) GUIDELINES FOR COMPLIANCE WITH LIMITATIONS.—

“(1) REQUIREMENT TO ADOPT.—The Attorney General, in consultation with the Director of National Intelligence, shall adopt guidelines to ensure— “(A) compliance with the limitations in subsection (b); and “(B) that an application for a court order is filed as required by this Act.

“(2) SUBMISSION OF GUIDELINES.—The Attorney General shall provide the guidelines adopted in accordance with paragraph (1) to— “(A) the congressional intelligence committees; “(B) the Committees on the Judiciary of the Senate and the House of Representatives; and “(C) the Foreign Intelligence Surveillance Court.

“(g) CERTIFICATION.— “(1) IN GENERAL.—

“(A) REQUIREMENT.—Subject to subparagraph (B), prior to the implementation of an authorization under subsection (a), the Attorney General and the Director of National Intelligence shall provide to the Foreign Intelligence Surveillance Court a written certification and any supporting affidavit, under oath and under seal, in accordance with this subsection.

“(B) EXCEPTION.—If the Attorney General and the Director of National Intelligence make a determination under subsection (c)(2) and time does not permit the submission of a certification under this subsection prior to the implementation of an authorization under subsection (a), the Attorney General and the Director of National Intelligence shall submit to the Court a certification for such authorization as soon as practicable but in no event later than 7 days after such determination is made.

“(2) REQUIREMENTS.—A certification made under this subsection shall— “(A) attest that— “(i) there are procedures in place that have been approved, have been submitted for approval, or will be submitted with the certification for approval by the Foreign Intelligence Surveillance Court that are reasonably designed to— “(I) ensure that an acquisition authorized under subsection (a) is limited to targeting persons reasonably believed to be located outside the United States; and “(II) prevent the intentional acquisition of any communication as to which the sender and all intended

recipients are known at the time of the acquisition to be located in the United States; “(ii) the minimization procedures to be used with respect to such acquisition— “(I) meet the definition of minimization procedures under section 101(h) or 301(4), as appropriate; and “(II) have been approved, have been submitted for approval, or will be submitted with the certification for approval by the Foreign Intelligence Surveillance Court; “(iii) guidelines have been adopted in accordance with subsection (f) to ensure compliance with the limitations in subsection (b) and to ensure that an application for a court order is filed as required by this Act; “(iv) the procedures and guidelines referred to in clauses (i), (ii), and (iii) are consistent with the requirements of the fourth amendment to the Constitution of the United States; “(v) a significant purpose of the acquisition is to obtain foreign intelligence information; “(vi) the acquisition involves obtaining foreign intelligence information from or with the assistance of an electronic communication service provider; and “(vii) the acquisition complies with the limitations in subsection (b); “(B) include the procedures adopted in accordance with subsections (d) and (e); “(C) be supported, as appropriate, by the affidavit of any appropriate official in the area of national security who is— “(i) appointed by the President, by and with the advice and consent of the Senate; or “(ii) the head of an element of the intelligence community; “(D) include— “(i) an effective date for the authorization that is at least 30 days after the submission of the written certification to the court; or “(ii) if the acquisition has begun or the effective date is less than 30 days after the submission of the written certification to the court, the date the acquisition began or the effective date for the acquisition; and “(E) if the Attorney General and the Director of National Intelligence make a determination under subsection (c)(2), include a statement that such determination has been made.

“(3) CHANGE IN EFFECTIVE DATE.—The Attorney General and the Director of National Intelligence may advance or delay the effective date referred to in paragraph (2)(D) by submitting an amended certification in accordance with subsection (i)(1)(C) to the Foreign Intelligence Surveillance Court for review pursuant to subsection (i).

“(4) LIMITATION.—A certification made under this subsection is not required to identify the specific facilities, places, premises, or property at which an acquisition authorized under subsection (a) will be directed or conducted.

“(5) MAINTENANCE OF CERTIFICATION.—The Attorney General or a designee of the Attorney General shall maintain a copy of a certification made under this subsection.

“(6) REVIEW.—A certification submitted in accordance with this subsection shall be subject to judicial review pursuant to subsection (i).

“(h) DIRECTIVES AND JUDICIAL REVIEW OF DIRECTIVES.—

“(1) AUTHORITY.—With respect to an acquisition authorized under subsection (a), the Attorney General and the Director of National Intelligence may direct, in writing, an electronic communication service provider to— “(A) immediately provide the Government with all information, facilities, or assistance necessary to accomplish the acquisition in a manner that will protect the secrecy of the acquisition and produce a minimum of interference with the services that such electronic communication service provider is providing to the target of the acquisition; and “(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.

“(2) COMPENSATION.—The Government shall compensate, at the prevailing rate, an electronic communication service provider for providing information, facilities, or assistance in accordance with a directive issued pursuant to paragraph (1).

“(3) RELEASE FROM LIABILITY.—No cause of action shall lie in any court against any electronic communication service provider for providing any information, facilities, or assistance in accordance with a directive issued pursuant to paragraph (1).

“(4) CHALLENGING OF DIRECTIVES.—

“(A) AUTHORITY TO CHALLENGE.—An electronic communication service provider receiving a directive issued pursuant to paragraph (1) may file a petition to modify or set aside such directive with the Foreign Intelligence Surveillance Court, which shall have jurisdiction to review such petition.

“(B) ASSIGNMENT.—The presiding judge of the Court shall assign a petition filed under subparagraph (A) to 1 of the judges serving in the pool established under section 103(e)(1) not later than 24 hours after the filing of such petition.

“(C) STANDARDS FOR REVIEW.—A judge considering a petition filed under subparagraph (A) may grant such petition only if the judge finds that the directive does not meet the requirements of this section, or is otherwise unlawful.

“(D) PROCEDURES FOR INITIAL REVIEW.—A judge shall conduct an initial review of a petition filed under subparagraph (A) not later than 5 days after being assigned such petition. If the judge determines that such petition does not consist of claims, defenses, or other legal contentions that are warranted by existing law or by a nonfrivolous argument for extending, modifying, or reversing existing law or for establishing new law, the judge shall immediately deny such petition and affirm the directive or any part of the directive that is the subject of such petition and order the recipient to comply with the directive or any part of it. Upon making a determination under this subparagraph or promptly thereafter, the judge shall provide a written statement for the record of the reasons for such determination.

“(E) PROCEDURES FOR PLENARY REVIEW.—If a judge determines that a petition filed under subparagraph (A) requires plenary review, the judge shall affirm, modify, or set aside the directive that is the subject of such petition not later than 30 days after being assigned such petition. If the judge does not set aside the directive, the judge shall immediately affirm or affirm with modifications the directive, and order the recipient to comply with the directive in its entirety or as modified. The judge shall provide a written statement for the record of the reasons for a determination under this subparagraph.

“(F) CONTINUED EFFECT.—Any directive not explicitly modified or set aside under this paragraph shall remain in full effect.

“(G) CONTEMPT OF COURT.—Failure to obey an order issued under this paragraph may be punished by the Court as contempt of court. “(5) ENFORCEMENT OF DIRECTIVES.— “(A) ORDER TO COMPEL.—If an electronic communication service provider fails to comply with a directive issued pursuant to paragraph (1), the Attorney General may file a petition for an order to compel the electronic communication service provider to comply with the directive with the Foreign Intelligence Surveillance Court, which shall have jurisdiction to review such petition. “(B)

ASSIGNMENT.—The presiding judge of the Court shall assign a petition filed under subparagraph (A) to 1 of the judges serving in the pool established under section 103(e)(1) not later than 24 hours after the filing of such petition.

“(C) PROCEDURES FOR REVIEW.—A judge considering a petition filed under subparagraph (A) shall, not later than 30 days after being assigned such petition, issue an order requiring the electronic communication service provider to comply with the directive or any part of it, as issued or as modified, if the judge finds that the directive meets the requirements of this section and is otherwise lawful. The judge shall provide a written statement for the record of the reasons for a determination under this paragraph.

“(D) CONTEMPT OF COURT.—Failure to obey an order issued under this paragraph may be punished by the Court as contempt of court.

“(E) PROCESS.—Any process under this paragraph may be served in any judicial district in which the electronic communication service provider may be found.

“(6) APPEAL.—

“(A) APPEAL TO THE COURT OF REVIEW.—The Government or an electronic communication service provider receiving a directive issued pursuant to paragraph (1) may file a petition with the Foreign Intelligence Surveillance Court of Review for review of a decision issued pursuant to paragraph (4) or (5). The Court of Review shall have jurisdiction to consider such petition and shall provide a written statement for the record of the reasons for a decision under this subparagraph.

“(B) CERTIORARI TO THE SUPREME COURT.—The Government or an electronic communication service provider receiving a directive issued pursuant to paragraph (1) may file a petition for a writ of certiorari for review of a decision of the Court of Review issued under subparagraph (A). The record for such review shall be transmitted under seal to the Supreme Court of the United States, which shall have jurisdiction to review such decision.

“(i) JUDICIAL REVIEW OF CERTIFICATIONS AND PROCEDURES.— “(1) IN GENERAL.—

“(A) REVIEW BY THE FOREIGN INTELLIGENCE SURVEILLANCE COURT.—The Foreign Intelligence Surveillance Court shall have jurisdiction to review a certification submitted in accordance with subsection (g) and the targeting and minimization procedures adopted in accordance with subsections (d) and (e), and amendments to such certification or such procedures.

“(B) TIME PERIOD FOR REVIEW.—The Court shall review a certification submitted in accordance with subsection (g) and the targeting and minimization procedures adopted in accordance with subsections (d) and (e) and shall complete such review and issue an order under paragraph (3) not later than 30 days after the date on which such certification and such procedures are submitted.

“(C) AMENDMENTS.—The Attorney General and the Director of National Intelligence may amend a certification submitted in accordance with subsection (g) or the targeting and minimization procedures adopted in accordance with subsections (d) and (e) as necessary at any time, including if the Court is conducting or has completed review of such certification or such procedures, and

shall submit the amended certification or amended procedures to the Court not later than 7 days after amending such certification or such procedures. The Court shall review any amendment under this subparagraph under the procedures set forth in this subsection. The Attorney General and the Director of National Intelligence may authorize the use of an amended certification or amended procedures pending the Court’s review of such amended certification or amended procedures.

“(2) REVIEW.—The Court shall review the following:

“(A) CERTIFICATION.—A certification submitted in accordance with subsection (g) to determine whether the certification contains all the required elements.

“(B) TARGETING PROCEDURES.—The targeting procedures adopted in accordance with subsection (d) to assess whether the procedures are reasonably designed to— “(i) ensure that an acquisition authorized under subsection (a) is limited to targeting persons reasonably believed to be located outside the United States; and “(ii) prevent the intentional acquisition of any communication as to which the sender and all intended recipients are known at the time of the acquisition to be located in the United States.

“(C) MINIMIZATION PROCEDURES.—The minimization procedures adopted in accordance with subsection (e) to assess whether such procedures meet the definition of minimization procedures under section 101(h) or section 301(4), as appropriate.

“(3) ORDERS.— “(A) APPROVAL.—If the Court finds that a certification submitted in accordance with subsection (g) contains all the required elements and that the targeting and minimization procedures adopted in accordance with subsections (d) and (e) are consistent with the requirements of those subsections and with the fourth amendment to the Constitution of the United States, the Court shall enter an order approving the certification and the use, or continued use in the case of an acquisition authorized pursuant to a determination under subsection (c)(2), of the procedures for the acquisition.

“(B) CORRECTION OF DEFICIENCIES.—If the Court finds that a certification submitted in accordance with subsection (g) does not contain all the required elements, or that the procedures adopted in accordance with subsections (d) and (e) are not consistent with the requirements of those subsections or the fourth amendment to the Constitution of the United States, the Court shall issue an order directing the Government to, at the Government’s election and to the extent required by the Court’s order— “(i) correct any deficiency identified by the Court’s order not later than 30 days after the date on which the Court issues the order; or “(ii) cease, or not begin, the implementation of the authorization for which such certification was submitted.

“(C) REQUIREMENT FOR WRITTEN STATEMENT.—In support of an order under this subsection, the Court shall provide, simultaneously with the order, for the record a written statement of the reasons for the order.

“(4) APPEAL.—

“(A) APPEAL TO THE COURT OF REVIEW.—The Government may file a petition with the Foreign Intelligence Surveillance Court of Review for review of an order under this subsection. The Court of Review shall have jurisdiction to consider such petition. For any decision under this subparagraph affirming, reversing, or modifying an order of the Foreign Intelligence Surveillance

Court, the Court of Review shall provide for the record a written statement of the reasons for the decision.

“(B) CONTINUATION OF ACQUISITION PENDING REHEARING OR APPEAL.—Any acquisition affected by an order under paragraph (3)(B) may continue— “(i) during the pendency of any rehearing of the order by the Court en banc; and “(ii) if the Government files a petition for review of an order under this section, until the Court of Review enters an order under subparagraph (C).

“(C) IMPLEMENTATION PENDING APPEAL.—Not later than 60 days after the filing of a petition for review of an order under paragraph (3)(B) directing the correction of a deficiency, the Court of Review shall determine, and enter a corresponding order regarding, whether all or any part of the correction order, as issued or modified, shall be implemented during the pendency of the review.

“(D) CERTIORARI TO THE SUPREME COURT.—The Government may file a petition for a writ of certiorari for review of a decision of the Court of Review issued under subparagraph (A). The record for such review shall be transmitted under seal to the Supreme Court of the United States, which shall have jurisdiction to review such decision.

“(5) SCHEDULE.—

“(A) REAUTHORIZATION OF AUTHORIZATIONS IN EFFECT.—If the Attorney General and the Director of National Intelligence seek to reauthorize or replace an authorization issued under subsection (a), the Attorney General and the Director of National Intelligence shall, to the extent practicable, submit to the Court the certification prepared in accordance with subsection (g) and the procedures adopted in accordance with subsections (d) and (e) at least 30 days prior to the expiration of such authorization.

“(B) REAUTHORIZATION OF ORDERS, AUTHORIZATIONS, AND DIRECTIVES.—If the Attorney General and the Director of National Intelligence seek to reauthorize or replace an authorization issued under subsection (a) by filing a certification pursuant to subparagraph (A), that authorization, and any directives issued thereunder and any order related thereto, shall remain in effect, notwithstanding the expiration provided for in subsection (a), until the Court issues an order with respect to such certification under paragraph (3) at which time the provisions of that paragraph and paragraph (4) shall apply with respect to such certification.

“(j) JUDICIAL PROCEEDINGS.—

“(1) EXPEDITED JUDICIAL PROCEEDINGS.—Judicial proceedings under this section shall be conducted as expeditiously as possible.

“(2) TIME LIMITS.—A time limit for a judicial decision in this section shall apply unless the Court, the Court of Review, or any judge of either the Court or the Court of Review, by order for reasons stated, extends that time as necessary for good cause in a manner consistent with national security.

“(k) MAINTENANCE AND SECURITY OF RECORDS AND PRO-CEEDINGS.—

“(1) STANDARDS.—The Foreign Intelligence Surveillance Court shall maintain a record of a proceeding under this section, including petitions, appeals, orders, and statements of reasons for a

decision, under security measures adopted by the Chief Justice of the United States, in consultation with the Attorney General and the Director of National Intelligence.

“(2) FILING AND REVIEW.—All petitions under this section shall be filed under seal. In any proceedings under this section, the Court shall, upon request of the Government, review *ex parte* and *in camera* any Government submission, or portions of a submission, which may include classified information.

“(3) RETENTION OF RECORDS.—The Attorney General and the Director of National Intelligence shall retain a directive or an order issued under this section for a period of not less than 10 years from the date on which such directive or such order is issued.

“(1) ASSESSMENTS AND REVIEWS.—

“(1) SEMIANNUAL ASSESSMENT.—Not less frequently than once every 6 months, the Attorney General and Director of National Intelligence shall assess compliance with the targeting and minimization procedures adopted in accordance with subsections (d) and (e) and the guidelines adopted in accordance with subsection (f) and shall submit each assessment to— “(A) the Foreign Intelligence Surveillance Court; and “(B) consistent with the Rules of the House of Representatives, the Standing Rules of the Senate, and Senate Resolution 400 of the 94th Congress or any successor Senate resolution— “(i) the congressional intelligence committees; and “(ii) the Committees on the Judiciary of the House of Representatives and the Senate.

“(2) AGENCY ASSESSMENT.—The Inspector General of the Department of Justice and the Inspector General of each element of the intelligence community authorized to acquire foreign intelligence information under subsection (a), with respect to the department or element of such Inspector General— “(A) are authorized to review compliance with the targeting and minimization procedures adopted in accordance with subsections (d) and (e) and the guidelines adopted in accordance with subsection (f); “(B) with respect to acquisitions authorized under subsection (a), shall review the number of disseminated intelligence reports containing a reference to a United States person identity and the number of United States-person identities subsequently disseminated by the element concerned in response to requests for identities that were not referred to by name or title in the original reporting; “(C) with respect to acquisitions authorized under subsection (a), shall review the number of targets that were later determined to be located in the United States and, to the extent possible, whether communications of such targets were reviewed; and “(D) shall provide each such review to— “(i) the Attorney General; “(ii) the Director of National Intelligence; and “(iii) consistent with the Rules of the House of Representatives, the Standing Rules of the Senate, and Senate Resolution 400 of the 94th Congress or any successor Senate resolution— “(I) the congressional intelligence committees; and “(II) the Committees on the Judiciary of the House of Representatives and the Senate.

“(3) ANNUAL REVIEW.—

“(A) REQUIREMENT TO CONDUCT.—The head of each element of the intelligence community conducting an acquisition authorized under subsection (a) shall conduct an annual review to determine whether there is reason to believe that foreign intelligence information has been or will be obtained from the acquisition. The annual review shall provide, with respect to acquisitions authorized under subsection (a)— “(i) an accounting of the number of disseminated

intelligence reports containing a reference to a United States-person identity; “(ii) an accounting of the number of United Statesperson identities subsequently disseminated by that element in response to requests for identities that were not referred to by name or title in the original reporting; “(iii) the number of targets that were later determined to be located in the United States and, to the extent possible, whether communications of such targets were reviewed; and “(iv) a description of any procedures developed by the head of such element of the intelligence community and approved by the Director of National Intelligence to assess, in a manner consistent with national security, operational requirements and the privacy interests of United States persons, the extent to which the acquisitions authorized under subsection (a) acquire the communications of United States persons, and the results of any such assessment.

“(B) USE OF REVIEW.—The head of each element of the intelligence community that conducts an annual review under subparagraph (A) shall use each such review to evaluate the adequacy of the minimization procedures utilized by such element and, as appropriate, the application of the minimization procedures to a particular acquisition authorized under subsection (a).

“(C) PROVISION OF REVIEW.—The head of each element of the intelligence community that conducts an annual review under subparagraph (A) shall provide such review to— “(i) the Foreign Intelligence Surveillance Court; “(ii) the Attorney General; “(iii) the Director of National Intelligence; and “(iv) consistent with the Rules of the House of Representatives, the Standing Rules of the Senate, and Senate Resolution 400 of the 94th Congress or any successor Senate resolution— “(I) the congressional intelligence committees; and “(II) the Committees on the Judiciary of the House of Representatives and the Senate.

ANNEX 13. STANDARD CONTRACTUAL CLAUSES DECISION

Relevant provision of the Standard Contractual Clauses decision.³⁹⁰

Article 1

The standard contractual clauses set out in the Annex are considered as offering adequate safeguards with respect to the protection of the privacy and fundamental rights and freedoms of individuals and as regards the exercise of the corresponding rights as required by Article 26(2) of Directive 95/46/EC.

Article 4

1. Without prejudice to their powers to take action to ensure compliance with national provisions adopted pursuant to Chapters II, III, V and VI of Directive 95/46/EC, the competent authorities in the Member States may exercise their existing powers to prohibit or suspend data flows to third countries in order to protect individuals with regard to the processing of their personal data in cases where:
 - (a) it is established that the law to which the data importer or a sub-processor is subject imposes upon him requirements to derogate from the applicable data protection law which go beyond the restrictions necessary in a democratic society as provided for in Article 13 of Directive 95/46/EC where those requirements are likely to have a substantial adverse effect on the guarantees provided by the applicable data protection law and the standard contractual clauses;
 - (b) a competent authority has established that the data importer or a sub-processor has not respected the standard contractual clauses in the Annex; or
 - (c) there is a substantial likelihood that the standard contractual clauses in the Annex are not being or will not be complied with and the continuing transfer would create an imminent risk of grave harm to the data subjects.
2. The prohibition or suspension pursuant to paragraph 1 shall be lifted as soon as the reasons for the suspension or prohibition no longer exist.
3. When Member States adopt measures pursuant to paragraphs 1 and 2, they shall, without delay, inform the Commission which will forward the information to the other Member States.

³⁹⁰ 2010/87/: 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 (notified under document C(2010) 593) (Text with EEA relevance), 039 OJ L § (2010). Available on: <http://data.europa.eu/eli/dec/2010/87/oj/eng>. Accessed February 23, 2023.

ANNEX 14. SCHREMS II PRELIMINARY QUESTIONS

In Schrems II case the High Court of Ireland requested preliminary ruling on following 11 questions:

1. In circumstances in which personal data is transferred by a private company from a European Union (EU) Member State to a private company in a third country for a commercial purpose pursuant to [the SCC Decision] and may be further processed in the third country by its authorities for purposes of national security but also for purposes of law enforcement and the conduct of the foreign affairs of the third country, does EU law (including the Charter) apply to the transfer of the data notwithstanding the provisions of Article 4(2) TEU in relation to national security and the provisions of the first indent of Article 3(2) of Directive [95/46] in relation to public security, defence and State security?
2. In determining whether there is a violation of the rights of an individual through the transfer of data from the [European Union] to a third country under the [SCC Decision] where it may be further processed for national security purposes, is the relevant comparator for the purposes of [Directive 95/46]:

the Charter, the EU Treaty, the FEU Treaty, [Directive 95/46], the [European Convention for the Protection of Human Rights and Fundamental Freedoms, signed at Rome on 4 November 1950] (or any other provision of EU law); or
 - (i) the national laws of one or more Member States?
 - (ii) If the relevant comparator is (ii), are the practices in the context of national security in one or more Member States also to be included in the comparator?
3. When assessing whether a third country ensures the level of protection required by EU law to personal data transferred to that country for the purposes of Article 26 of [Directive 95/46], ought the level of protection in the third country be assessed by reference to:
 - (a) the applicable rules in the third country resulting from its domestic law or international commitments, and the practice designed to ensure compliance with those rules, to include the professional rules and security measures which are complied with in the third country;

or
 - (b) the rules referred to in (a) together with such administrative, regulatory and compliance practices and policy safeguards, procedures, protocols, oversight mechanisms and non-judicial remedies as are in place in the third country?
4. Given the facts found by the High Court in relation to US law, if personal data is transferred from the European Union to the United States under [the SCC Decision] does this violate the rights of individuals under Articles 7 and/or 8 of the Charter?

Given the facts found by the High Court in relation to US law, if personal data is transferred from the European Union to the United States under [the SCC Decision]:
 - (a) does the level of protection afforded by the United States respect the essence of an individual's right to a judicial remedy for breach of his or her data privacy rights guaranteed by Article 47 of the Charter?

If the answer to Question 5(a) is in the affirmative:

- (b) are the limitations imposed by US law on an individual's right to a judicial remedy in the context of US national security proportionate within the meaning of Article 52 of the Charter and do not exceed what is necessary in a democratic society for national security purposes?
5. What is the level of protection required to be afforded to personal data transferred to a third country pursuant to standard contractual clauses adopted in accordance with a decision of the Commission under Article 26(4) [of Directive 95/46] in light of the provisions of [Directive 95/46] and in particular Articles 25 and 26 read in the light of the Charter?
 6. What are the matters to be taken into account in assessing whether the level of protection afforded to data transferred to a third country under [the SCC Decision] satisfies the requirements of [Directive 95/46] and the Charter?
 7. Does the fact that the standard contractual clauses apply as between the data exporter and the data importer and do not bind the national authorities of a third country who may require the data importer to make available to its security services for further processing the personal data transferred pursuant to the clauses provided for in [the SCC Decision] preclude the clauses from adducing adequate safeguards as envisaged by Article 26(2) of [Directive 95/46]?
 8. If a third country data importer is subject to surveillance laws that in the view of a data protection authority conflict with the [standard contractual clauses] or Article 25 and 26 of [Directive 95/46] and/or the Charter, is a data protection authority required to use its enforcement powers under Article 28(3) of [Directive 95/46] to suspend data flows or is the exercise of those powers limited to exceptional cases only, in light of recital 11 of [the SCC Decision], or can a data protection authority use its discretion not to suspend data flows?
 9. For the purposes of Article 25(6) of [Directive 95/46], does [the Privacy Shield Decision] constitute a finding of general application binding on data protection authorities and the courts of the Member States to the effect that the United States ensures an adequate level of protection within the meaning of Article 25(2) of [Directive 95/46] by reason of its domestic law or of the international commitments it has entered into?

If it does not, what relevance, if any, does the Privacy Shield Decision have in the assessment conducted into the adequacy of the safeguards provided to data transferred to the United States which is transferred pursuant to the [SCC Decision]?
 10. Given the findings of the High Court in relation to US law, does the provision of the Privacy Shield ombudsperson under Annex A to Annex III to the Privacy Shield Decision when taken in conjunction with the existing regime in the United States ensure that the US provides a remedy to data subjects whose personal data is transferred to the United States under the [SCC Decision] that is compatible with Article 47 of the Charter?
 11. Does the [SCC Decision] violate Articles 7, 8 and/or 47 of the Charter?' ³⁹¹

³⁹¹ Data Protection Commissioner v. Facebook Ireland Limited and Maximilian Schrems (Schrems II), §68.

ANNEX 15. PRIVACY SHIELD DECISION

Relevant provision of the Privacy Shield decision.³⁹²

Article 1

1. For the purposes of Article 25(2) of Directive 95/46/EC, the United States ensures an adequate level of protection for personal data transferred from the Union to organisations in the United States under the EU-U.S. Privacy Shield.
2. The EU-U.S. Privacy Shield is constituted by the Principles issued by the U.S. Department of Commerce on 7 July 2016 as set out in Annex II and the official representations and commitments contained in the documents listed in Annexes I, III to VII.
3. For the purpose of paragraph 1, personal data are transferred under the EU-U.S. Privacy Shield where they are transferred from the Union to organisations in the United States that are included in the 'Privacy Shield List', maintained and made publicly available by the U.S. Department of Commerce, in accordance with Sections I and III of the Principles set out in Annex II.

Annex VI – Conclusion

The United States recognizes that our signals intelligence and other intelligence activities must take into account that all persons should be treated with dignity and respect, regardless of their nationality or place of residence, and that all persons have legitimate privacy interests in the handling of their personal information. The United States only uses signals intelligence to advance its national security and foreign policy interests and to protect its citizens and the citizens of its allies and partners from harm. In short, the IC does not engage in indiscriminate surveillance of anyone, including ordinary European citizens. Signals intelligence collection only takes place when duly authorized and in a manner that strictly complies with these limitations; only after consideration of the availability of alternative sources, including from diplomatic and public sources; and in a manner that prioritizes appropriate and feasible alternatives. And wherever practicable, signals intelligence only takes place through collection focused on specific foreign intelligence targets or topics through the use of discriminants.

U.S. policy in this regard was affirmed in PPD-28. Within this framework, U.S. intelligence agencies do not have the legal authority, the resources, the technical capability or the desire to intercept all of the world's communications. Those agencies are not reading the emails of everyone in the United States, or of everyone in the world. Consistent with PPD-28, the United States provides robust protections to the personal information of non-U.S. persons that is collected through signals intelligence activities. To the maximum extent feasible consistent with the national security, this includes policies and procedures to minimize the retention and dissemination of personal information concerning non-U.S. persons comparable to the protections enjoyed by U.S. persons. Moreover, as discussed above, the comprehensive oversight regime of the targeted Section 702 FISA authority is unparalleled. Finally, the significant amendments to U.S. intelligence law

³⁹² 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 (notified under document C(2016) 4176) (Text with EEA relevance), 207 OJ L § (2016). Available on: http://data.europa.eu/eli/dec_impl/2016/1250/oj/eng. Accessed February 23, 2023.

set forth in the USA FREEDOM Act and the ODNI-led initiatives to promote transparency within the Intelligence Community greatly enhance the privacy and civil liberties of all individuals, regardless of their nationality.

ANNEX 16. REGULATION OF INVESTIGATORY POWERS ACT 2000

Relevant provisions of the Regulation of Investigatory Powers Act 2000.³⁹³

Section 65(1)

There shall, for the purpose of exercising the jurisdiction conferred on them by this section, be a tribunal consisting of such number of members as Her Majesty may by Letters Patent appoint.

Section 8(4)

Subsections (1) and (2) shall not apply to an interception warrant if—

- (a) the description of communications to which the warrant relates confines the conduct authorised or required by the warrant to conduct falling within subsection (5); and
- (b) at the time of the issue of the warrant, a certificate applicable to the warrant has been issued by the Secretary of State certifying—
 - (i) the descriptions of intercepted material the examination of which he considers necessary; and
 - (ii) that he considers the examination of material of those descriptions necessary as mentioned in section 5(3)(a), (b) or (c).

Section 16

1. For the purposes of section 15 the requirements of this section, in the case of a warrant in relation to which there is a section 8(4) certificate, are that the intercepted material is read, looked at or listened to by the persons to whom it becomes available by virtue of the warrant to the extent only that it—
 - (a) has been certified as material the examination of which is necessary as mentioned in section 5(3)(a), (b) or (c); and
 - (b) falls within subsection (2).
2. Subject to subsections (3) and (4), intercepted material falls within this subsection so far only as it is selected to be read, looked at or listened to otherwise than according to a factor which—
 - (a) is referable to an individual who is known to be for the time being in the British Islands; and
 - (b) has as its purpose, or one of its purposes, the identification of material contained in communications sent by him, or intended for him.
3. Intercepted material falls within subsection (2), notwithstanding that it is selected by reference to any such factor as is mentioned in paragraph (a) and (b) of that subsection, if—
 - (a) it is certified by the Secretary of State for the purposes of section 8(4) that the examination of material selected according to factors referable to the individual in question is necessary as mentioned in subsection 5(3)(a), (b) or (c); and

³⁹³ Investigatory Powers Act 2016 (King's Printer of Acts of Parliament). Available on: <https://www.legislation.gov.uk/ukpga/2016/25/part/1/enacted>. Accessed April 1, 2023.

- (b) the material relates only to communications sent during a period of not more than three months specified in the certificate.
4. Intercepted material also falls within subsection (2), notwithstanding that it is selected by reference to any such factor as is mentioned in paragraph (a) and (b) of that subsection, if—
 - (a) the person to whom the warrant is addressed believes, on reasonable grounds, that the circumstances are such that the material would fall within that subsection; or
 - (b) the conditions set out in subsection (5) below are satisfied in relation to the selection of the material.
 5. Those conditions are satisfied in relation to the selection of intercepted material if—
 - (a) it has appeared to the person to whom the warrant is addressed that there has been such a relevant change of circumstances as, but for subsection (4)(b), would prevent the intercepted material from falling within subsection (2);
 - (b) since it first so appeared, a written authorisation to read, look at or listen to the material has been given by a senior official; and
 - (c) the selection is made before the end of the first working day after the day on which it first so appeared to that person.
 6. References in this section to its appearing that there has been a relevant change of circumstances are references to its appearing either—
 - (a) that the individual in question has entered the British Islands; or
 - (b) that a belief by the person to whom the warrant is addressed in the individual's presence outside the British Islands was in fact mistaken.