PRIVACY AND ONLINE SURVEILLANCE:

INTERNATIONAL LEGAL CHALLENGES

Jeanne Gillet

LLB, LLM

Submitted in fulfilment of the requirements of the Degree of PhD

School of Law, College of Social Sciences

University of Glasgow

October 2019

ABSTRACT

Regulating online surveillance is one of the main challenges of the 21st century. The main goal of this thesis is to identify the different sources of conceptual confusion surrounding the legal discourse on online surveillance. There are two main aspects to the debate: one concerns privacy regulation, while the other focuses on surveillance regulation.

Privacy has been qualified as "a concept in disarray"[1]. If attempts to define the concept have generally not been successful,[2] it is not surprising that the nature and scope of its correlated right have also been difficult to assess. How international law conceptualizes the right to privacy is an important issue when discussing online surveillance. In order to clarify the international conceptualization of the right to privacy, a comparative analysis of the privacy protections of the United States and France is conducted. Analysing how both these national traditions developed their legal apparatus to protect private interests highlights the different approaches (and consequently conceptualizations) to privacy regulation. Two paradigms can be identified: one refers to the value of 'freedom', the other to the notion of 'control'. The existence of an 'international human right to privacy' is not contested but its exact content has however raised many questions. The second chapter explores whether a common conceptualization of the right to privacy exists in international law and if the paradigms identified at the domestic level can help clarify the ambiguous nature of international privacy protection. The field is further complexified by the appearance at the end of the 20th century of data protection frameworks. This legal field is muddled because of the vast amount of regulations, but also the multiple terminologies used to qualify its core principles. A comparative analysis of the European[3] and US systems and their respective conceptualization of data protection is carried on.

The nature of online surveillance activities also questions our understanding of current traditional frameworks. On one hand, cyberspace challenges the principles of jurisdiction under public international law and international human rights- specifically the territoriality principle. On the other hand, the silence of the international community on the legality of peacetime espionage and the difficulties to interpret the existing international provisions on privacy in the context of surveillance have also proven to be challenging.

The international legal discourse on online surveillance regulation finds itself at the crossroad of different broader conceptual issues. These conceptual and normative challenges need to be straightforwardly addressed to understand how to effectively regulate surveillance and consequently enhance individuals' enjoyment of their right to privacy.

[1] Daniel Solove, *Understanding Privacy* (Harvard University Press 2008) 1.
[2] Colin J Bennet, *Regulating Privacy: Data Protection and Public Policy in Europe and the United States* (Cornwell University Press 1992) 25.
[3] Understood in this context as the systems of the European Union and the Council of Europe.

ACKNOWLEDGEMENTS

I would like first and foremost to express my sincere gratitude to my supervisors, Dr Akbar Rasulov and Professor Robin Geiss, for their support, precious advice and all the opportunities they offered me during these last four years.

This journey would not have been possible without the daily encouragements, help and feedbacks of my friends and fellow researchers: Eleni Methymaki, Asli Olcay, Gail Lythgoe, and Joanna Wilson. Being able to share this whole adventure with them was a privilege, and I am forever grateful for the hours we spent together- through tough and good times. Their friendship is the real prize.

I would like to thank our Senior Postgraduate Administrator, Ms Susan Holmes. She has been so kind to me through the years and has been extremely helpful during the whole experience.

A special thanks also needs to be addressed to the staff of Breads Meats Bread, who on top of being incredible colleagues for two years, fed me an incalculable number of burgers and fries to sustain me during the whole writing process.

I am eternally grateful to my husband Matt, for his unwavering support through the storms and his uncanny ability to always make me laugh. Thank you for helping me reach higher. I would also like to thank my parents for… everything. Any less would be an understatement.

Finally, I would like to dedicate this PhD to my grandmothers, who were both incredible women who paved the way for me to be here today.

AUTHOR'S DECLARATION

I declare that, except where explicit reference is made to the contribution of others, that this dissertation is the result of my own work and has not been submitted for any other degree at the University of Glasgow or any other institution.

Printed Name: JEANNE GILLET

Signature:

TABLE OF CONTENTS

Table of Cases

United States

France

Germany

European Court of Human Rights

European Commission on Human Rights

European Court of Justice

International Court of Justice

UN Human Rights Committee

Lopez Burgos v. Uruguay, Communication No. 52/1979 (29 July 1981) UN Doc CCPR/C/13/D/52/1979.

Toonen v Australia, Communication No. 488/1992 (31 March 1994) UN Doc CCPR/C/50/D/488/1992.

Van Hulst v Netherlands, Communication No. 903/1999 (1 November 2004) UN DOC CCPR/C/82/D/903/1999.

IACommHR and IACHR

Atala Riffo v Chile (24 February 2012) Series C, No 239.

Escher et al. v. Brazil (6 July 2009) Series C, No. 200.

Garcia v Peru, 11.006, Report No 1/95 OEA/Ser L/V/II.88rev.1 doc.9. (1995).

Fontevecchia & D'Amico v. Argentina (29 November 2011) Series C, No. 238.

Murillo v Costa Rica (28 November 2012) Series C, No 257.

Rosendo Cantu v Mexico (31 August 2010) Series C, No. 216.

Tristan Donoso v Panama (27 January 2009) Series C No. 193.

`

Table of Legislation

France

French Constitution, du 3 septembre 1791, tit. III.

Article 15, al 2bis of Law of 29 July 1881 on the Press, as amended by Ordonnance of 6 May 1944.

Former criminal code, Article 187. ('Ancien code pénal').

Criminal code, Article 226-15, modified by Ordonnance n°2000-916 of 19th September 2000, Art. 3 (V) JORF 22nd September 2000 in force 1st January 2002.

Criminal code: Art 226-1, para 2; 226-4 (domicile).

Loi n° 70-643 du 17 juillet 1970 tendant à renforcer la garantie des droits individuels des citoyens.

Loi No. 78-17 du 6 Janvier 1978 relative à l'information, aux fichiers et aux libertés, *Journal Officiel de La République Française*, 7 January 1978. repealed by Loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles**.**

Article 368, 1° - now repealed by Loi n°92-1336 du 16 décembre 1992 - art. 372 (V) JORF 23 décembre 1992 en vigueur le 1er mars 1994.

Art 226-1 of the criminal code, modifié par Ordonnance n°2000-916 du 19 septembre 2000 - art. 3 (V) JORF 22 septembre 2000 en vigueur le 1er janvier 2002.

United States

Act. of Mar. 3, 1825, ch. 64, §22, 4 Stat. 102.

Bank Secrecy Act of 1970 Pub. L. No. 91-508.

Cable Act 47 USC §551(a) (2012).

Cable Communications Policy Act of 1984, 42 U.S.C. § 551.

California Penal Code §618 (1872).

Children's Online Privacy Protection Act of 1998, 15 U.S.C. §§ 6501–06.

Computer Matching and Privacy Protection Act of 1988 Pub. L. No. 100-503, 102 Stat. 2507 (codified as amended at 5 U.S.C. § 552a(a)(8)–(13), (e)(12), (o)–(r), (u)).

Constitution of the United States of America (1878). Amend. III, IV and V.

Driver's Privacy Protection Act of 1994, 18 U.S.C. §§ 2721–25.

Electronic Communications Privacy Act of 1986, 18 U.S.C §§ 2510–22, 2701–11, 3121–27.

Employee Polygraph Protection Act of 1988, Pub. L. No. 100-618, codified at 29 U.S.C. § 2001–09.

Fair Credit Reporting Act of 1970, 15 U.S.C. § 1681.

Fair Credit Reporting Act, Pub. L. 114-38, 15 USC § 1681 (2012).

Gramm-Leach-Bliley Act of 1999, Pub. L. No. 106-102, 113 Stat. 1338 (codified at 15 U.S.C. §§ 6801-–09).

Gramm-Leach-Bliley Act 15 USC §§ 6801-6809 (2012).

Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936.

Homeland Security Act of 2002, 6 U.S.C. § 222.

Restatement (Second) of Torts, §§ 652B (Intrusion Upon Seclusion), 652C (Appropriation of Name or Likeness), 652D (Publicity Given to Private Life), 652E (Publicly Placing Person in False Lights) (1977).

Right to Financial Privacy of 1978 Pub. L. No. 95-630.

Privacy Act of 1974, Pub. L. 93-579, 5 USC §552a (1994).

Privacy Protection Act of 1980 Pub. L. No. 96-440, 94 Stat. 1879, codified at 42 U.S.C. § 2000aa.

Stored Communications Act 1986, in the Electronic Communications Privacy Act, Pub. L. No. 99-508, 100 Stat. 1848 (1986) (codified as amended at 18 U.S.C. § 2701 et seq. (1986)).

Telecommunications Act 47 USC § 222(a) (2012).

Telephone Consumer Protection Act of 1991, Pub. L. No. 102-243, 105 Stat. 2394 (codified at 47 U.S.C. § 227).

USA Patriot Act of 2001, Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act (USA PATRIOT Act) of 2001, made changed to FISA and ECPA, See: 18 U.S.C. § 3127(3) as amended by the USA PATRIOT Act § 216 and 50 U.S.C. § 1804(a)(7)(B) as amended by USA PATRIOT Act § 204.

Title II, Sec. 215 'Access to records and other items under the foreign intelligence surveillance act', amending FISA by inserting "Sec. 501. Access to Certain Business Records for Foreign Intelligence and International Terrorism Investigations (a.1.)".

Video Privacy Protection Act of 1988, Pub. L. No. 100-618, 102 Stat. 3195, (codified at 18 U.S.C. §§ 2710–11).

Germany

Grundgesetz für die Bundesrepublik Deutschland [GG] [Basic Law] May 23, 1949, BGBL. 1, arts. 1(1), 2(1).

Hessian Data Protection Act (7 October 1970) GESETZUNO VERORONUNGSBLATT [GVBI] 625.

The Federal Data Protection Act (BDGS) (30 June 2017) (Federal Law Gazette I p. 2097) (BGBl. I S. 2097).

Sweden

The Data Act of 1973, SFS 1973:289, amended at SFS 1982:446 (Swedish Code of Statutes).

National Constitutions

Constitution of the Arab Republic of Egypt (22 September 1971).

Constitution of the Federal Democratic Republic of Ethiopia (21 August 1995).

Constitution of the Grand Duchy of Luxembourg (17 October 1868 (as Amended 8 August 2000)).

Constitution of the Republic of the Philippines (2 February 1987).

Constitution of the Union of Socialist Soviet Republics (5 December 1936, amended 31 January 1924, 7 October 1977).

Constitution of the Federal Republic of Yugoslavia (April 1992).

International Law

Multilateral Treaties

African Union, Convention on Cyber Security and Personal Data Protection (Adopted 27 June 2014, still not into effect) EX.CL/846(XXV).

African Union, Declaration of Principles on Freedom of Expression in Africa, (23 October 2002) ACHPR/Res.62(XXXII)02, Annex.

African Charter on Human and People's Rights, (21 October 1986) CAB/LEG/67/3 rev. 5, 21 I.L.M. 58 (1982).

American Convention on Human Rights (adopted 22 November 1969, entered into force 18 July 1978) 1144 UNTS 123.

American Declaration of the Rights and Duties of Men (2 May 1948)

Cairo Declaration on Human Rights in Islam (5 August 1999) UN Doc A/CONF.157/PC/62/Add.18, (A/45/421-S/21797).

Geneva Convention Relative to the Protection of Civilian Persons in Time of War (adopted 12 August 1949, entered into force 21 October 1950) 75 UNTS 287.

International Convention on the Protection of the Rights of All Migrant Workers and Members of Their Families (18 December 1990) 2220 UNTS 360.

Convention Rights of the Child (20 November 1989) 1577 UNTS 3.

Laws and Customs of War on Land (Hague, IV) (adopted 18 October 1907, entered into force 26 January 1910) 539 UNTS.

Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflict (adopted 8 June 1977, entered into force 7 December 1978) 1125 UNTS 3.

Vienna Convention on the Law of Treaties (23 May 1969) 1155 UNTS 331.

Bilateral Treaties

Agreement on Mutual Legal Assistance between the United States of America and the European Union, (25 June 2003) L181, 19/07/2003, p. 0034.

Agreement between the United States of America and the European Union on the use and transfer of Passenger Name Records to the United States Department of Homeland Security, (14 December 2011) Official Journal L 0215, 11/08/2012, p. 0005 – 0014.

Agreement between the European Union and the United States of America on the processing and transfer of Financial Messaging Data from the European Union to the United States for the purposes of the Terrorist Finance Tracking Program Date of end of validity: 31 October 2010, OJ L 195 27.07.2010, p. 0003.

British–US Communication Intelligence Agreement, UKUSA Signal Intelligence Agreement (adopted 5 March 1946).

Council of Europe

Additional Protocol to the Convention for the Protection of Individuals with Regard to the Automatic Processing of Personal Data, Regarding Supervisory Authorities and Transborder Data Flows (adopted on 8 November 2001, entered into force 1 July 2004) ETS No. 181.

Convention for the Protection of Human Rights and Fundamental Freedoms (adopted 4 November 1950, entered into force 3 September 1953) 213 UNTS 221.

Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (adopted 28 January 1981, entered into force 01 October 1985) ETS 108.

Convention on Cybercrime (adopted on 23 November 2001, entered into force 01 July 2004) ETS 185, 2296 UNTS 167.

European Union

Charter of Fundamental Rights of the European Union (7 December 2000) OJ C364/1, [2007] OJ C303/1, [2012] OJ C326/391.

Consolidated version of the Treaty on the Functioning of the European Union, Official Journal C 326, 26/10/2012 p. 0001 – 0390.

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 (24 October 1995) OJ L 281, 23 November 1995, p. 0031-0050.

Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) (12 July 2002) OJ L 201, 31.7.2002, p. 0037–0047.

Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC (15 March 2006) OJ L 105, 13.4.2006, p. 0054–0063.

Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws (Text with EEA relevance) (25 November 2009) OJ L 337, 18.12.2009, p. 0011–0036.

Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) (Ongoing) COM/2017/010 final - 2017/03 (COD).

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with regards to the Processing of Personal Data on the Free Movement of such Data, and Repealing Directive 95/46/EC, L119, 4 May 2016, p. 0001-0088.

Directive (EU) 2016/680 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 by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free

movement of such data, and repealing Council Framework Decision 2008/977/JHA, *OJ L 119, 4.5.2016, p. 0089–0131.*

Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (Text with EEA relevance.) (23 October 2018) OJ L 295, 21.11.2018, p. 0039–0098.

Treaty of Lisbon amending the Treaty on European Union and the Treaty establishing the European Community (signed 13 December 2007, entered into force 1 December 2009).

United Nations

Charter of the United Nations (adopted 26 June 1945, entered into force 24 October 1945) art 51.

International Covenant on Civil and Political Rights (adopted 16 December 1966, entered into force 23 March 1976) 999 UNTS 171.

Universal Declaration of Human Rights (10 December 1948) 217 A (III) UN Doc A/RES/217(III) A.

United Nations International Law Commission

Draft Articles on Responsibility of States for Internationally Wrongful Acts, adopted by the Commission at its fifty-third session in 2001 (Final Outcome) UN Doc A/56/10, 43, UN Doc A/RES/56/83, Annex, UN Doc A/CN.4/L.602/Rev.1.

United Nations General Assembly Resolutions

UNGA Res 2450 (XXIII) 'Human Rights and Scientific and Technological Developments' (19 December 1968) UN Doc A/RES/23/2450.

UNGA Res 25/2625 (XXV) 'Declaration on Principles of International Law Concerning Friendly Relations and Co-operation among States in Accordance with the Charter of the United Nations', (24 October 1970) UN Doc A/RES/25/2625.

UNGA Res 45/95 'Guidelines for the Regulation of Computerized Personal Data Files' (14 December 1990) UN Doc A/RES/45/95.

UNGA Res 45/117, 'Model Treaty by the UN General Assembly on Mutual Assistance in Criminal Matters' (14 December 1990) UN Doc A/RES/45/117.

UNGA Res 68/167 'The right to Privacy in the Digital Age' (18 December 2013) UN Doc A/RES/68/167.

UNGA Resolution 69/166 'Right to privacy in the digital age (18 December 2014) A/RES/69/166.

UNGA Res 69/397 'Promotion and protection of human rights and fundamental freedoms while countering terrorism: report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Ben Emmerson' (23 September 2014) UN Doc A/69/397.

UNGA Res 19/166, 'The Right to Privacy in the Digital Age' (18 December 2014) UN DOC A/RES/69/166.

UNGA Res 72/180, 'Protection of Human Rights and Fundamental Freedoms while Countering Terrorism' (19 December 2017) UN Doc A/RES/72/180.

United Nations Security Council

UNSC Res 1373 (2001) on threats to international peace and security caused by terrorist acts (28 September 2001) UN Doc S/RES/1373(2001).

Other

ASEAN Human Rights Declaration (19 November 2012).

ECOWAS, Supplementary Act A/SA.1/01/10 on Personal Data Protection (adopted on 16 February 2010) A/SA.1/01/10.

OAS General Assembly, Resolution 1932 'Access to Public Information: Strengthening Democracy' AG/RES. 1932 (XXXIII-O/03).

OAS General Assembly, Resolution 2057 'Access to Public Information: Strengthening Democracy' AG/RES. 2057 (XXXIV-O/04).

OAS General Assembly, Resolution 2121 'Access to Public Information: Strengthening Democracy' AG/RES. 2121 (XXXV-O/05).

OAS General Assembly, Resolution 2252 'Access to Public Information: Strengthening Democracy' AG/RES. 2252 (XXXVI-O/06).

OAS General Assembly, Resolution 2288 'Access to Public Information: Strengthening Democracy AG/RES. 2288 (XXXVII-O/07).

OAS General Assembly, Resolution 2418 'Access to Public Information: Strengthening Democracy' AG/RES. 2418 (XXXVIII-O/08).

OAS General Assembly Resolution 'Model Inter-American Law on Access to Public. Information' AG/RES. 2607 (XL-O/10).

OAS General Assembly, Resolution 2514 'Access to Public Information: Strengthening Democracy AG/RES. 2514 (XXXIX-O/09).

OAS General Assembly, Resolution 2661 'Access to Public Information and Protection of Personal Data' (7 July 2004) AG/RES.2661 (XLI-O/11).

OAS General Assembly Resolution 2727 'Access to Public Information and Protection of Personal Data' (4 June 2012) AG/RES. 2727 (XLII-O/12).

OAS General Assembly Resolution 2811 'Access to Public Information and Protection of Personal Data' (6 June 2013) AG/RES. 2811 (XLIII-O/13).

OAS General Assembly Resolution 2842 'Access to Public Information and Protection of Personal Data' (4 June 2015) AG/RES. 2842 (XLIV-O/14).

Organisation of Eastern Caribbean States, Data Protection Bill (fourth Draft) (6 October 2011).

INTRODUCTION

The regulation of online surveillance is one of the major challenges of the 21st century. In the words of a UK Minister, '[t]he digital revolution through which we are living is bringing about the fastest pace of change that any generation has ever seen'[1]. According to the World Economic Forum Global Risks Perception Survey 2018–2019, cyber-attacks[2], data theft, and the loss of privacy to companies and governments, as well as the lack of sufficient international response to such challenges, are mentioned by the respondents among the major current global risks.[3]

The challenge of regulation triggered by the digital revolution is indeed keenly felt by a myriad of actors: the legal community, of course, but also governments, the civil society, and corporations. Regardless of the opinion on the merits of the practice, the subject of (the lack of) regulation is a matter of intense debate. Some actors are wary of legislative action and strict supervision whereas others favour a firmer approach to legal regulation and monitoring. Furthermore, there are concerns regarding the prioritisation of national security interests or the promotion of respect for human rights (the two not being mutually exclusive). Last but not least, there also significant divergences regarding the use of a hard or soft law instrument, and developing international initiatives or establishing regional consensus. As such, the ramifications of the debate are immense. Therefore, regardless of the differences in approaches to and preferred methods of regulation, all actors in the field of online surveillance would benefit from further clarity on the subject.

Against this backdrop, the main objective of this dissertation is to identify and examine the sources of confusion underpinning the debate on the regulation of online surveillance at the international level, with a view to bringing conceptual clarification and sophistication to the debate. This in turn promises to facilitate the regulatory efforts at both domestic and international levels. The sections below, first, introduce the main sources of the confusion, i.e. the technical aspects of online surveillance and its relation to the right to privacy.

1.1. Challenges to the regulation of online surveillance

There are two main sources of the confusion: one is the "technicalities" of online surveillance, which remain difficult to comprehend even for experts of the field at times, and the other is the intrinsic relationship of online surveillance with the right to privacy.
The first source of confusion is related to the online surveillance practices themselves. New technologies developed over the last 30 years against a background of escalating security concerns since the terrorist attacks of 9/11, which led to the creation of surveillance means of unprecedent scale and scope. For example, it has been proven that: GCHQ[4] has

[1] HC Deb 12 October 2017, vol 629, c498.
[2] A cyber-attack is defined as "a cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects" in *Tallinn Manual on the International Law Applicable to Cyber Warfare*, Michael Schmitt (ed.), (CUP 2013) Rule 30.
[3] World Economic Forum, 'The Global Risk Report 2019: 14th edition' (Word Economic Forum 2019) <http://www3.weforum.org/docs/WEF_Global_Risks_Report_2019.pdf> accessed 17 September 2019.
[4] Government Communications Headquarters: intelligence agency of the United Kingdom.

intercepted 1.8 millions Yahoo! video chats in only six months under its Optic Nerve program and the NSA[5] collects 5 billion records relating to mobile phones' locations *a day*.[6] From a "technical" point of view, these new practices question our traditional understanding of the current legal frameworks. How do we substantially regulate them? Another difficulty brought by online surveillance is the very context in which they operate: online. Cyberspace has challenged our understanding of the traditional principles of international law, especially the territoriality principle which underpins jurisdictional matters.

The second aspect clouding the debate is the fact that the regulation of online surveillance is inseparable from the international regulation of privacy. Regulation of privacy, both at the international and national levels, has proven to be complicated. Privacy, as a concept[7], is amorphous. What is perceived as "private" might vary across societies. It covers a wide range of issues: from nosey neighbours listening to your conversations to the police entering your home, and from corporations tracking your digital history to women's abortions rights, the sphere of what can be considered "private" is very broad. The philosophical, sociological and anthropological aspects of privacy fall outside the scope of this study. What is interesting for this research is the legal understanding of privacy and how online surveillance measures interplay with the legal conceptualisation(s) of privacy. How to regulate such broad range of private interests is a difficult question. Which ones of these interests deserve legal protection? What kind of legal protection? States have been wrestling with these questions since the beginning of the 19th century: first discussing how to protect certain private interests through varied legal constructs, then slowly recognizing a distinct right to privacy. The right to privacy is now accepted around the globe and was recognised in numerous international instruments through the 20th century. Although its legal status is not contested, the scope of the said right to privacy remains controversial. Therefore, when discussing the specific question of online surveillance, through that "limited prism", comes the larger and unresolved question of privacy regulation.

To recapitulate, the field of online surveillance is muddled and complicated for two main reasons: one is the technical challenges it entails, and the second is its link to an amorphous international right to privacy, whose scope remains controversial. This thesis examines each aspect separately. The first part focuses on the conceptualisation of privacy in international law, whereas the second turns to the issue of the international regulation of online surveillance.

1.2. Outline of the Dissertation: From the Two Paradigms of Privacy to the International Regulation of Privacy and Online Surveillance

As mentioned above, the dissertation comprises of two main sections that respectively focus on the regulation of privacy and the international regulation of online surveillance. Before elaborating on the content and structure of the two sections, however, a terminological

[5] National Security Agency: intelligence agency of the United States.
[6] Amnesty International/Privacy International, 'Two Years After Snowden: Protecting Human Rights in an Age of Mass Surveillance' (June 2015) <https://privacyinternational.org/sites/default/files/2017-12/Two%20Years%20After%20Snowden_Final%20Report_EN_0.pdf> accessed 19 October 2017.
[7] For the purpose of this thesis, the Merriam-Webster definition of 'concept' is used: "something conceived in the mind (thought, notion) or an abstract or generalized idea generalized from particular instances".

clarification is in order and the difference between 'privacy' and 'private interests' needs to be pointed out. States started to legislate on interests that, in today's perspective, would be understood as belonging to the "privacy sphere" at a time where "privacy" as legal concept did not exist yet. The "right to privacy" is a complex legal construct that appeared gradually. Yet, certain interests, that now fall under the scope of "privacy", received legal protection before the recognition of a distinct right to privacy. These interests could, and have been, protected through other legal constructs. In order to avoid any legal anachronism, the vocabulary of "private interests" will be used in this thesis to refer to "privacy before privacy", or in order words, interests protected by a variety of legal frameworks before privacy emerged as a legal institution. "Privacy" will be used to discuss the particular interest that is the object of the distinct right to privacy.

1.2.1. The International Regulation of Privacy

There is no doubt that international law regulates privacy. Privacy protections can be found in numerous international instruments, including the Universal Declaration of Human Rights (UDHR),[8] the International Covenant on Civil and Political Rights (ICCPR),[9] or at the regional level, *inter alia*, the European Convention on Human Rights (ECHR),[10] the American Convention on Human Rights,[11] the Arab Charter on Human Rights,[12] and the ASEAN Human Rights Declaration.[13] But how does international law *understand* privacy regulation? Is there a consensus in the international legal community on the scope of these protections or on the conception[14] of "the right to privacy"? There is no straightforward answer to these questions. In this dissertation, it is argued that, to properly understand how international law conceptualizes the right to privacy, it is informative to analyse how privacy protection *can* be, and has been, approached in domestic law. To this end, in Chapter I of the dissertation, a comparative analysis of domestic approaches to privacy regulations is being carried on, namely in the United States and France.

International law's understanding of privacy is influenced by domestic approaches. Looking at these national legal cultures individually and comparatively allows us to understand how different approaches to regulating/protecting the complex concept of privacy have come about and evolved in states' practices, and bring to light the different ways they did so. These different ways to approach the same question (how to protect individuals' privacy) in turn reveal the different conceptualizations of privacy and consequently of its regulations. It is beyond the scope of this study to carry out a comprehensive examination of all, or a large number of, jurisdictions that address "privacy". The selection of the two jurisdictions, the United States and France, is due to two main reasons. Firstly, both of these countries started

[8] UN General Assembly, Universal Declaration of Human Rights (adopted 10 December 1948) 217 A(III), art 12. (hereinafter UDHR).
[9] International Covenant on Civil and Political Rights (adopted 16 December 1966, entered into force 23 March 1976) 999 UNTS 171, art 17. (hereinafter ICCPR).
[10] Convention for the Protection of Human Rights and Fundamental Freedoms (adopted 4 November 1950, entered into force 3 September 1953) 213 UNTS 221, art 8. (hereinafter ECHR).
[11] American Convention on Human Rights (adopted 29 November 1969, entered into force 18 July 1978) 1144 UNTS 123, art 11.
[12] Arab Charter on Human Rights (adopted 22 May 2004, entered into force 15 March 2008) art 21.
[13] ASEAN Human Rights Declaration, General Principle 21.
[14] For the purpose of this thesis, the Merriam-Webster definition of 'conception' is used: "a complex product of abstract and reflective thinking or the sum of a person's ideas and beliefs concerning something".

to engage with questions around privacy regulation since the beginning of the 19th century. They both had lively debate amongst their respective legal communities and at a policy level on how to best protect their citizen's private interests. Secondly, both countries also represent different legal cultures more generally: the common law and the civil approach.
The first chapter of this thesis concern these two domestic traditions respectively. It looks at the evolution of privacy laws in the United States and in France. These two countries not only illustrate two different legal cultures, they also have a long history in legally protecting different private interests. The aim of the comparative analysis is to shed light on the international regulation of privacy. In other words, what is examined is not the two countries' legal approach to privacy as such, but rather their experience with regulating privacy and what these experiences can teach us about how privacy can be regulated and conceptualized under international law.

When looking at how historically these two domestics national traditions developed their legal frameworks to gradually protect private interests, different narratives can be identified in the legal discourse on the subject. These narratives are important because they (have) shape(d) our understanding of current legal practices and conceptualization of how and why privacy should be protected. Accordingly, two main paradigms can be found in the privacy legal discourse in the two domestic legal systems analysed.

The first one is what I refer to as the paradigm of "freedom from interference". It denotes the idea that privacy, as a value, should be legally protected because individuals should have a space free from unwarranted interference. It is focused on preventing undesired intrusions by private and public actors. This paradigm classically approaches privacy as a *space free from interference*. It typically uses a certain terminology referring to "space", "zone" or "area", and violations are referred to as "intrusion", "invasion", or "assault". The end goal of the legal protection of private interests (whether that protection takes the form of a distinct legal right to privacy or ensured through other legal constructs) is to protect a core space free from intrusion, and, as such, it is 'interference-orientated". The second paradigm is understanding privacy protection as a form of "control" and is "individual-orientated". Legal initiative should be taken to provide individuals with the possibility to control certain aspects of his private life. This narrative typically evokes arguments such as the necessity for individuals to have a "choice", to "consent", and to "decide" how their private life is being handled.

Both of these conceptual constructs are found in both domestic systems. Nonetheless the United States and France have not approached the question of privacy regulation from the same angle. When looking at the types of legal constructs used to protect individual's private interests and the debate surrounding the emergence of the right to privacy in their respective systems, the contrast is clear.

On one hand, the United States has developed its privacy laws with a clear focus on protecting individuals' freedom from interference. This is demonstrated by the main legal constructs used to protect private interests in the 19th century: trespass actions and the Fourth Amendment. The clear focus of these regulations is to prevent unwarranted intrusions, either from private actors or governmental authorities. On a general background of distrust towards

unfettered governmental power, Americans hold the value of freedom very close to their hearts, which is translated into their legal regime. Thus, their privacy laws are 'interference-orientated". This also explains their currently fragmented nature. In addition to the protection granted by four privacy torts and the Fourth Amendment, dozens of specific statutes can be found at the federal and state levels. Each of these statutes responds to a specific "privacy threat". This is because the whole system is concerned about specific interferences with privacy.
On the other hand, France approached the regulation of privacy interests in a very different way. Historically, the French system was more focused on granting control to individuals, in order for them to decide how they desire to be portrayed in the public space and have the ability to oppose unwarranted disclosure of their private life. The right to privacy is understood as a personality right.[15] Thus, privacy protections in France are "individual-orientated".

As James Whitman stated "comparative law is the study of relative differences. (…) No absolute generalization about any legal system is ever true."[16] The two paradigms are not mutually exclusive and have shaped the regulation of private interests in both domestic legal systems. The argument that one of the paradigms has been more dominant and influential than the other in the respective domestic legal system does not equate to a suggestion that the motivation to grant control to individuals over their private life is absent in the legal system of the United States or that French law does not aim to protect its citizens from interference. The point of the comparative analysis is not to fall into such an oversimplification of the two legal systems. Rather, it is to highlight that the same notion of a "right to privacy" can be conceptualized differently, and that different paradigms are hidden behind the regulation of private interests.

What is the significance of identifying and examining these paradigms and the different approaches taken by domestic systems? Particularly for the purposes of this dissertation, the significance lies in the fact that these paradigms have influenced the international legal discourse on privacy and consequently the debate on online surveillance regulation. This is the subject of Chapter II of this thesis, which traces the development of the right to privacy at the international level and the evolution of our understanding of its scope. What narratives does the international legal discourse on privacy refer to? Which concepts are behind the protections established by the major international treaties? Is it understood as protecting a "freedom from interference" or as granting individuals "control"? Is it interference or individual-orientated?

There are no straight answers to these questions at the heart of Chapter II. The drafting history of the UDHR and of the ICCPR does not say anything on the drafters' motivations to recognize the right to privacy at the international level. As a result, not only is it difficult to pinpoint what kind of concepts is behind international privacy protections, it also makes their scope ambiguous. The content, and conceptualization, of the protection granted by the

[15] Personality rights are understood as giving "individuals the power to control and regulate the use of various attributes of the self" in Jeanne M Hauch, 'Protecting Private Facts in France: the Warren and Brandeis Tort is Alive and Well and Flourishing in Paris' (1993-1994) 68 Tul. L. Rev. 1219, 1229.
[16] James Q Whitman, 'The Two Western Cultures of Privacy: Dignity versus Liberty' (2004) 113 The Yale Journal 1151, 1163.

ECHR, despite having been interpreted extensively by the ECtHR, is also open to debate and interpretation.

The protections granted by international law on privacy appear to be conceptually somewhat "shallow". They were established without extensive discussion and have not - until recently- raised much questions. They are now under the limelight, but it remains challenging to establish the extent of their relevance in assessing current technological developments, such as online surveillance, as their scope is ambiguous and the broader 'conceptual baggage' the international legal rules on privacy come with has not been sufficiently scrutinized to date. Chapter II aims to bring this 'conceptual baggage' to the forefront of the debate on the international regulation of privacy by drawing on the two paradigms identified and introduced in Chapter I.

Chapter III of the dissertation then turns to the question of data protection in international law. It is not possible to have a conversation about privacy protections in the 21st century (especially when relating to online surveillance) without considering the relatively "new" legal regime of data protection. Data protection originated as a subset of privacy laws, but is now understood as a separate legal regime in European and international law. By contrast, in the United States, what is called 'informational privacy' is still understood as belonging under the general umbrella of privacy laws. Once again, the two different approaches to data protection can be found on both sides of the Atlantic. However, where the United States approaches the question of data regulation from a fragmented point of view (as the existence of several statutes dealing with specific issues demonstrate), Europe has taken a more general approach and enacted omnibus protection to grant data protection the status of fundamental right.

The two paradigms of "freedom of interference" and "control" identified in Chapter I can also be found in different data protection frameworks. International data protection frameworks establish core principles regulating any data processing activity[17]. The rhetoric behind the adoption of these principles generally relates to the grant to individuals more control over the handling of their personal data. But once again, different approaches can be, and has been, taken: the United States responds to specific abusive data processing practices (interference-orientated), while Europe established a fundamental right to data protection (individual-orientated).

To recapitulate, there is a 'conceptual baggage' behind privacy and data protection regulation that remains underexplored at the international level. When looking at online surveillance practices and their relationship with privacy protection, the bigger debate about the scope and the conceptualisation of the right to privacy has to be addressed. Two paradigms can be found in domestic legal discourses on privacy: one understands privacy protection as a safeguard against "freedom from interference", the other constructs privacy protection as enabling individuals to have control over the divulgation of and access to their private lives. Despite shaping domestic approaches such as in the United States and France, this 'conceptual baggage' is not acknowledged at the international level. International safeguards of privacy have amorphous scopes, which reduced their effectiveness and

[17] So-called 'Fair Information Principles'.

relevance in dealing with the realities of the 21st century. To add more confusion to this already muddled field, international data protection frameworks regulate certain personal data processing activities, which is increasingly shaping visions of how best to enhance individuals' enjoyment of their right to privacy in these types of activities.

1.2.2. The International Regulation of Online Surveillance

The second part of this thesis focuses on the substantive challenges raised by online surveillance practices and the attempts to regulate them in international law. Chapter IV starts with an analysis of the jurisdictional challenges raised by online surveillance practices, as the lack of conceptual clarity concerning jurisdictional issues in international law muddles our understanding of the applicable rules. Aiming to contribute to the clarification of the issue of jurisdiction in this context, the chapter examines how the traditional jurisdiction principles are being transposed and understood in the context of digital technology. In this respect, different issues arise under public international law and under international human rights. Once again, to clarify the precise legal discourse on online surveillance, the broader frameworks need to be examined first.

Under general international law, the notion of jurisdiction is based on the territoriality doctrine. Certain extraterritorial assertions of jurisdiction are allowed, but only in specific cases, when supported by permissive rules. Cyberspace challenges the relevance of this traditional model. In addition, specific forms of surveillance raise different jurisdictional problems, and they receive different level of attention and publicity. While there is a conversation concerning practices of accessing data extraterritorially, for example, other means of surveillance such as direct interceptions of communications fall off the radar.

In addition to general international law, an innovative interpretation of traditional standards also needs to take place in international human rights law. The debate surrounding the extraterritorial applicability of human rights treaties is not new, but again, the cyber context, in which online foreign surveillance takes place, needs to be paid particular consideration. The traditional standard of "effective control" established by the European Court of Human Right, for example, needs to be adapted: what does effective control mean in the digital world? What is the object of such control? Traditionally the debate has surrounded control over territory or individuals, but in the context of surveillance, it needs to be asked whether the object, the existence of control over which has to be established in order to trigger human rights responsibility, should be intercepted date. Such significant questions are not yet answered. As mentioned above, the lack of conceptual clarity concerning jurisdictional issues in international law in general and international human rights law in particular muddles our understanding of the rules applicable to online surveillance. Resolving this issue will not only enhance individuals' protection, it will also secure States in the respect of their sovereignty.

Finally, the last chapter of this thesis (Chapter V) analyses the regulation of surveillance activities at the international level. The first part highlights the silence of general public international law on the question of peacetime surveillance, while the second assesses the compliance of electronic surveillance practices with international human rights standards.

What the traditional limitation standards, namely "legality", "necessary" and "proportionality", mean in the context of electronic surveillance is currently being debated. In this context, data protection principles are increasingly extrapolated to the interpretation of general privacy provisions.

However, the debate stays on "technical grounds", meaning that there is almost no conversation about how we conceptualize the interference caused by online surveillance and consequently what kind of conceptual regulatory model should be favoured. The conceptual paradigms behind privacy regulations which were identified in the first part on the thesis, i.e. "freedom of interference" and "control", influence how privacy protection is approached in international law, and hence in surveillance regulation. The two subjects are inseparable. Legislating on surveillance activities mobilizes the two conceptual constructs. On one hand, their legality is being assessed through international provisions that are framed in a vocabulary referring to "external interference", even though, as demonstrated in Chapter II, there is no consensus on how these protections are conceptualised in general. On the other hand, data protection frameworks that represent a vision of control influence and complement traditional privacy safeguards when individuals are confronted with their data being processed, including by State-sponsored surveillance measures. Therefore. when talking about regulating online surveillance at the international level, attention should be paid to the different paradigms hidden in the legal discourse on privacy: what may at first glance seem like purely technical challenges does in fact raise bigger conceptual questions.

1.3. Towards an investigation of the 'conceptual baggage' behind privacy and surveillance

The aim of this dissertation is to shed light on the international legal discourse on privacy and online surveillance regulation, and to bring conceptual nuance and sophistication to the debates on this matter. On one side there are different conceptualizations of privacy regulation, and the two conceptual constructs identified in domestic systems, i.e. "freedom of interference" and "control", influence the international legal discourse on privacy and surveillance. On the other side, surveillance practices bring their own legal challenges on the table. They question our traditional understanding of jurisdictional principles under general international law and international human rights law.

Lacking regulation under general international law, online surveillance is currently being assessed through the prism of existing human rights standards, but this is revealing to be a difficult exercise. As a result, the current international framework often falls short of providing effective protection to privacy in context of online surveillance. This is due to two main reasons: firstly, it struggles to deal with technical challenges raised by cyberspace and new means of surveillance. Secondly, the absence of discussion and acknowledgement of the different conceptualizations of privacy protections both at the domestic and international levels, which eventually shape how privacy is regulated, prevents the emergence of a conceptually-advanced debate that is conducive to producing clear and effective regulation approaches.

Adapting legal standards to new surveillance capabilities is only part of the answer. When assessing the compliance of online surveillance measures with existing frameworks, or when calling for new regulations, one needs to be aware of the complicated 'conceptual baggage' behind privacy and data protection legal regimes. It implies different visions of the protection granted and therefore different choices for policy-makers. This was ignored when privacy protections were established at the international level, but this should be avoided now that the international community is starting efforts to regulate online surveillance.

PART I – CONCEPTUAL CHALLENGES OF PRIVACY REGULATION

CHAPTER I – Comparative Analysis of the United States and French Domestic Legal Systems

Introduction

The international debate surrounding online surveillance regulation is complex not only because of the technical challenges raised by new surveillance means, but also because of the difficulty of assessing of their compliance with international human standards, especially with the right to privacy. The right to privacy is a complex legal construct whose conceptualization and scope have been object of numerous debates. As Judith Jarvis Thomson mentioned: "Perhaps the most striking thing about the right to privacy is that nobody seems to have any clear idea what it is"[1]. This is the case both at domestic and international levels. In an attempt to clarify the current international position on privacy regulation, this chapter proposes to first assess how national traditions have approached this issue. International law's understanding of privacy regulation is influenced by domestic approaches. Comparatively looking into domestic legal systems allows an insight into the different possible approaches to privacy regulation, and consequently different possible conceptualizations of this legal construct.

The right to privacy as a distinct legal construct slowly emerged in different domestic legal systems at the end of the 19th century and started to be recognized during the 20th century. It does not mean however that "privacy" -as we understand it today- was not protected before then. The functions the right to privacy performs today, including protecting certain private interests, such as the intimacy of the home or the confidentiality of letters, were historically protected through other legal regimes. Gradually, privacy as a value started to appear in the legal discourse as an interest worth receiving legal protection. Arguments in favour of the recognition of a "right to privacy" emerged: either as part of an already existing legal framework, or as a distinct right. With time, the legal community of different countries progressively recognised the legal status of a right to privacy. Even though the debate on the exact scope of the right to privacy is still open in many jurisdictions, its status is established and has received international recognition, being now recognised as a constitutional right by most States around the world.[2]

The "process" for the right to privacy to gradually emerge as valid in domestic legal systems was roughly similar in different national systems, but different legal constructs were mobilized along the way. These differences are underpinned by different understandings, or paradigms, on how to regulate what in today's perspective is named privacy. This chapter conducts a comparative analysis between the approaches undertaken by the United States

[1] Judith Jarvis Thomson, 'The right to privacy', in Ferdinand David Schoeman, *Philosophical Dimensions of Privacy* (CUP 1984) 272.
[2] Daniel Solove, *Understanding Privacy* (Harvard University Press 2008) 3.

and France to regulate private interests and how the right to privacy emerged in these two respective jurisdictions. Both these countries have wrestled with the complicated debate around private interest regulation from the late 18th and 19th century. They have a long and rich history on how to "tackle" the slippery concept of privacy in the legal discourse. They have influenced other countries' approaches to privacy[3], and represent different legal systems: common law and civil law. As it will be developed in this chapter, both States approached differently the issue of privacy regulation, which in turn illustrates different paradigms behind privacy regulation.

The aim of this chapter is to learn from these two national traditions' experience with privacy regulation to clarify the current international framework. Their regulatory approaches to privacy are therefore not analysed as such, but in the specific optic of highlighting the different paradigms behind privacy regulations, and how international law integrated these different models. The chapter is therefore trying to identify different approaches - and their correlated understandings - behind privacy *regulation*; not privacy itself. Of course, the two are interlinked- how a system understands privacy will shape how it regulates it- but the focus here is on the conceptual approaches behind the legal constructs protecting private interests. This is what will clarify how international law regulates privacy and consequently, online surveillance regulation. This clarification is important because different approaches to privacy regulation imply different policy choices.

Two main paradigms can be identified when looking at how the United States and France developed their legal apparatus to protect private interests. The first one refers to "freedom" as being the main objective of privacy regulation. It involves the idea that individuals should have a space free from interference, and that privacy as a value should be legally protected to ensure individuals' freedom. The second understands privacy protection as a form of "control". It sees privacy protection as empowering individuals, granting them the ability to manage their private life. Both paradigms can be found in the domestic legal discourse of the United States and France on how to regulate private interests, but this chapter will demonstrate that they actually approach the same subject (how to regulate privacy) from different perspectives. To this end, the first part of this chapter analyses the historical development of privacy protections in the United States, while the second looks at the French experience. The chapter concludes with a comparative analysis of the two traditions and highlights the differences in their respective conceptual approaches to privacy regulation.

Part I – United States

The United States started to discuss how to best protect certain private interests as soon as it proclaimed its independence. What is understood today as privacy received legal attention initially through different legal constructs such as the Fourth Amendment and tort of trespass. Following the publication of a ground-breaking journal article in 1890 arguing the existence of a distinct right to privacy, the US system has not stopped addressing new potential threats to its citizen's privacy. To provide an overview of this historical legal

[3] Eg. For the influence of the United States privacy laws on Chinese development: See Guobin Zhu, 'The Right to Privacy: An Emerging Right in Chinese Law' (1997) 18 Statute Law Rev 208.

evolution, in this part the protection granted to certain private interests through other legal constructs before the recognition of a distinct right to privacy will be detailed first, while the debate surrounding the right to privacy, its recognition and the current privacy laws of the United States will be assessed in the second part.

Section 1. Protection through other legal constructs

A. Protection from State's abuse of power: Fourth Amendment

Due to the colonial background on which the Revolution took place, newly independent Americans did not trust the notion of powerful central government and perceived it as a constant potential threat to their individual's liberties. They therefore ratified a Bill of Rights in 1791 to limit the government's arbitrary power and protect individuals from potential governmental abuses. Certain interests that would be understood from today's perspective as private were protected at the end of the eighteen century by this new Bill of Rights. For example, the Fifth Amendment, amongst other things, prohibits the government to compel individuals to witness against themselves[4]- in other words individuals cannot be forced to divulge personal incriminating information. The main private interest protected by the Bill of Rights however was the sanctity of the home. The Third Amendment prevents governments from requesting private houses to be open to soldiers[5], and the Fourth Amendment grants what is still considered today as one of the strongest protections of private interests in the United States.

It states:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.[6]

Parallel provisions were adopted by States in their own constitutional legislatures. States courts started to deal with search and seizure cases, fleshing out the scope of the protection granted by the Fourth Amendment early on.[7] The Amendment only sought to regulate intrusions by governmental authorities into the private property of Americans and did not concern invasions committed by private citizens.

One of the earliest occasions for the Supreme Court to interpret the Fourth Amendment was in 1878, where the Court decided in *Ex Parte Jackson*[8] that a federal agent, even acting in his function, could not open a sealed letter that was in the Post Office, unless he had a lawful

---

[4] US CONST. amend. V: "No person shall be held to answer for a capital, or otherwise infamous crime, unless on a presentment or indictment of a grand jury, except in cases arising in the land or naval forces, or in the militia, when in actual service in time of war or public danger; nor shall any person be subject for the same offense to be twice put in jeopardy of life or limb; nor shall be compelled in any criminal case to be a witness against himself, nor be deprived of life, liberty, or property, without due process of law; nor shall private property be taken for public use, without just compensation".

[5] US CONST. amend. III: "No Soldier shall, in time of peace be quartered in any house, without the consent of the owner, nor in time of war, but in a manner to be prescribed by law".

[6] US CONST. amend. IV.

[7] 'The Right to Privacy in Nineteenth Century America' (1981) 94 Harvard Law Review 1892, 1897.

[8] 96 U.S. 727 (1878).

warrant authorizing him to do so[9]. Justice Field wrote: "The constitutional guaranty of the right of the people to be secure in their papers against unreasonable searches and seizures extends to their papers, thus closed against inspection, wherever they may be"[10].

In 1886, the Supreme Court ruled on *Boyd v. United States*[11] case. The Court held invalid, under the Fourth and Fifth Amendments, a statute which stated that if an individual refused to produce a document requested by federal authorities, it would be assumed that any claims concerning the content of said document would be true in any potential penalty suit against him under revenues law. The Court famously stated:

> The principles laid down in this opinion affect the very essence of constitutional liberty and security. They reach further than the concrete form of the case then before the court, with its adventitious circumstances, they apply to all invasions on the part of the government and its employés of the sanctity of a man's home and the privacies of life.
> It is not breaking of his doors, and the rummaging of his drawers, that constitutes the essence of the offense; but it is the *invasion* of *his infeasible right of personal security, personal liberty and private property* […] Breaking into a house and opening boxes and drawers are circumstances of aggravation; but *any forcible and compulsory extortion* of a man's own testimony or his *private papers* to be used as evidence to convict him of crime or to forfeit his goods, is within the condemnation of that judgement. In this regards the Fourth and Fifth Amendments run almost into each other[12].

The Court's reasoning illustrates the two paradigms identified in the introduction. The paradigm of "freedom from interference" is clearly referenced in the first part of the Court's reasoning, which uses the terminology of liberty. This is a clear affirmation of the sanctity of the home. But at the same time however, the Court mobilizes a vocabulary of control. The Court clearly states that it is not the physical entry of the house, or the physical searches of boxes, that constitutes the essence of the infraction, but the extortion of a man's testimony or private papers. 'Compulsory extortion' seems to imply the idea of taking away the possibility for the individual to control his papers, and therefore the divulgation of his private information. In this case, 'to be secure in his papers' is to have control over them and not being obliged to turn them over.

If we read the Fourth Amendment and its first interpretations by courts as harbouring a form of a - yet unarticulated- right to privacy, the reasoning behind such protection seems to be of protecting their personal liberty, which meant in practice granting individuals control over certain aspects of their private life: in this case their papers and the information they contain. These two cases confirmed that private papers were protected by the Fourth Amendment.[13]

---

[9] Id. at 735.
[10] 96 U.S. 727 (1878) at 733.
[11] 116 U.S. 616 (1886).
[12] Ibid, 630. (emphasis added).
[13] *Ex Parte Jackson* (n 8) 733: "The constitutional guaranty of the right of the people to be secure in their papers against unreasonable searches and seizures extends to their papers, thus closed against inspection, wherever they may be" and in *Boyd* (n 11) 622: "It is our opinion, therefore, that a compulsory production of

Even if the Supreme Court softened its uncompromising position in subsequent cases[14], *Boyd* is still to this day a ground-breaking case that shaped the legal understanding of privacy regulation in the United States. As Whitman puts it: "the standard history of modern American privacy rights" truly started with "*Boyd*'s fundamental understanding of 'privacy' rights as generalizations of the principle of the 'sanctity of the home'"[15].

The strongest legal protection of private interest in the United States at the end of the 18th century and during the 19th was therefore found in a right against unlawful searches and seizures. This is taking place on the backdrop of a general suspicion towards governmental power. It starts the main trend in the United States privacy regime: ensuring individuals a certain freedom from the State first of all, but also from abusive private actors.

B. Protection from individual's intrusions

B.1. Eavesdropping

Eavesdropping was a criminal offense in nineteenth century America and in common law in general.[16] According to the law, eavesdropping "constituted physical intrusion ('hanging about the dwelling place of another'), interception ('hearing tattle'), and divulgence ('repeating it to the disturbance of the neighbourhood')"[17]. It was for a long time the only legal action available for a victim of a non-physical intrusion[18], but in practice these criminal sanctions were not often applied as prosecutors rarely investigated these claims[19]. Internal informal community sanctions were usually used for cases of eavesdropping[20] and slowly this criminal procedure disappeared as the nineteenth century wore on.

Still, for the purpose of this study, this legal regime illustrates well how certain private interests were protected through other legal regimes before the emergence of a distinct right to privacy. Criminalizing eavesdropping was at the time the legal translation of the belief that "no man has a right to pry into another's business or secrets"[21] and that the certain private spaces should be free from invasion- more specifically a space free from anyone

---

a man's private papers to establish a criminal charge against him, or to forfeit his property, is within the scope of the Fourth Amendment to the Constitution".

[14] *Fisher v United States*, 425 U.S. 391 (1976); *Couch v United States*, 409 U.S. 322 (1973), *Warden v Hayden*, 387 U.S. 294 (1967).

[15] James Q Whitman, 'The Two Western Cultures of Privacy: Dignity versus Liberty' (2004) 113 The Yale Journal 1151, 1213.

[16] Sir William Blackstone defined it as "Eavesdroppers, or such as listen under walls and widows, or the eaves of a house, to hearken after discourse, and thereupon to frame slanderous and mischievous tales, are a common nuisance, and presentable at the court-leet, or are indictable at the sessions, and punishable by fine and finding sureties for their good behaviour" in *Commentaries on the Laws of England,* vol 4 (William Draper Lewis 1922) 168.

[17] David J Seipp 'The Right to Privacy in American History' (Harvard University: Program on Information Resources Policy, 1978) 2. <http://pirp.harvard.edu/pubs_pdf/seipp/seipp-p78-3.pdf> accessed 16 September 2019.

[18] Benjamin E Bratman, 'Brandeis and Warren's Right to Privacy and the Birth of the Right to Privacy' 69 Tenn. L. Rev. 623, 634.

[19] Irwin R Kramer, 'The Birth of Privacy Law: A Century Since Warren and Brandeis' (1989) 39 Cath UL Rev 703, 706.

[20] Such as for example public chastisement, Seipp (n 17) 3.

[21] 'The Right to Privacy in Nineteenth Century America' (n 7) 1896.

behind within earshot. For example, as early as 1831, a court in Pennsylvania explained its reasoning behind prosecuting eavesdropping by stating:

> Every man's house is his castle, were no man has a right to *intrude* for any purpose whatever. No man has right to pry into your *secrecy* in your own house. There are very few families were even the truth would not be very unpleasant to be told all over the country[22].

The offense is framed in term of intrusion, and the accent is on the sanctity of the house. This shows how the house was perceived as a place that should remain free from interference, even non-physical one such as eavesdropping on private conversations.

B.2. Trespass actions

The legal culture in the United States always protected the sanctity of the home, and not exclusively against governmental authorities. An action for trespass was the best relief available for individuals injured by an invasion committed by another private individual[23] and clearly gave the power of the law to the popular proverb "a man's house is his castle". Through the doctrine of trespass, American courts were able to issue criminal penalties and civil remedies to ensure that individuals could enjoy being left alone in their own home.[24] In the 19th century, the terminology of 'privacy' started to emerge in trespass actions.

Slowly, 'domestic privacy' was considered as one of the interests protected by this type of actions. According to a New York court in 1851, damages for trespass included compensation for: "injury, insult, *invasion of the privacy* and *interference* with the comfort of the plaintiff and his family"[25]. In 1880 a Vermont court used the trespass doctrine to ensure the plaintiff the "right of quiet occupancy and privacy"[26] against the unwanted intrusion of her host into her bedroom. These early cases speak about the loss of privacy that occurs when an unwanted physical invasion take place. They use a vocabulary related to "invasions" and "intrusions" and argue for a protection of a certain private space free from invasions- the home.

In 1892, the New York Court of Appeals decided to extend the notion of trespass in the *Moore v. New York Elevated R.R. Co* case.[27] The plaintiff complained that the defendants built an elevated train platform, which led to a direct view on his rooms. The Court held on that matter that:

> The defendants have furnished the means and opportunity for those persons *to invade* the privacy of these rooms. […] No reason appears why the defendants should not be responsible for the consequences of the *loss of privacy* thus occasioned so far as it *depreciated the rental value* of the rooms in the plaintiff's building[28].

[22] *Commonwealth v. Lovett*, 4 Clark 5 (Pa., 1831). (emphasis added).
[23] Kramer (n 19) 805.
[24] 'The Right to Privacy in Nineteenth Century America' (n 7) 1894.
[25] *Ives v. Humphrey*, E.D. Smith 196, 201-202 (N.Y. Ct. C.P. 1851) (emphasis added).
[26] *Newell v. Whitcher*, 53 Vt. 589 (1880) 591.
[27] *Moore v. New York Elevated R.R. Co*., 130 N.Y. 523 (1892) 527.
[28] Id. 528. (emphasis added).

The Court therefore directly stated that an invasion of privacy led to a devaluation of the property[29]. A non-physical intrusion- a direct view on the interior of a flat- was considered in this case as trespass. This case illustrates how judges dynamically interpreted existing provisions in order to respond to demands to have certain private interests protected, at a time where there was no explicit protection of what we consider today as privacy.

B.3. Confidentiality of correspondence

The confidentiality of private correspondence was also legally protected in the United States from the 18th century, well before the recognition of a distinct right to privacy. With each wave of technological developments, means of communications evolved and consequently, legal frameworks followed and adapted.

Initially, there was no colonial institutionalized postal service in America. Interceptions would regularly happen between the hands of colonial postmasters and cities authorities, but one of the main causes of concern before the Revolution was the tampering of letters by the British Government.[30] After the proclamation of Independence, different institutionalized post services emerged: the New American Post Office in 1774, the National Post Office in 1782 and the United States Post Office in 1792. All were prohibited to open, delay or destroy any letter without a valid warrant.[31] The amount of complaints of violations of secrecy of correspondence was still very high[32], but the confidentiality of mails strengthened with time. In 1825 the Postal Act reinforced the legal protection afforded to the secrecy of mail by imposing a fine on anyone (not exclusively postal employees) who would take, open, or delay any letter in transit- which was considered as amounting to obstruction of correspondence and "pry into another's business or secrets"[33]. No exception was established, not even for official authorities.[34] The sanctity of the mails was perceived as absolute.[35] Federal laws didn't change after the Civil War, but certain states like California in 1872 decided to edict their own fines for violations[36] and criminalized "the violation of epistolary correspondence"[37]. Statutes at state level and internal rules in companies also prohibited disclosure by employees[38] in order to "prevent the betrayal of private affairs […] for the promotion of private gain or the gratification of idle gossip"[39].

In addition to the protection afforded by the Fourth Amendment (*Ex Parte Jackson* case), the sanctity of letters was also assured by court injunctions preventing their publication if

[29] Id. 529.
[30] Seipp (n 17) 9.
[31] Ibid, 7-10.
[32] For the anecdote: even George Washington and Thomas Jefferson openly complained that their own correspondence was not protected from the curiosity of postmasters.
[33] Act. of Mar. 3, 1825, ch. 64, §22, 4 Stat. 102.
[34] Seipp (n 17) 12.
[35] A special agent of the Post Office declared in 1855: "The laws of the land are intended not only to preserve the person and material property of every citizen sacred from intrusion, but to secure the privacy of his thoughts, so far as he sees fit to withhold them from others" in J. Holbrook, *Ten Years Among The Mail Bag* (1855) vxiii, quoted in 'The Right to Privacy in Nineteenth Century America' (n 7) 1899. (emphasis added).
[36] Seipp (n 17) 15.
[37] *E.g*. CAL. PEN. CODE §618 (1872).
[38] 'The Right to Privacy in Nineteenth Century America' (n 7) 1899.
[39] *Henisler v. Freedman*, 2 Pars. Eq. Cas. 274 (Pa. Ct. C.P. 1851) quoted in Ibid 1901.

the sender didn't consent to it.[40] These injunctions were granted to ensure the respect of the right to property that the writer possessed on his letters.[41] The legal protection of letters in the 19th century was linked to the right to property. It recognizes that the writer possesses property rights over his own letters, which gives him an exclusive power over it.

The invention of the telegraph challenged the confidentiality of correspondence, as telegrams were read by both operators on the sending and receiving sides. This quickly led to a need of legislative action, in order to cope with the change. Wiretapping became a criminal offence in some states[42], and prohibited anywhere else by laws protecting telegraph company property.[43] In the aftermath of the Civil War, Congress granted itself the authority to subpoena telegrams, which the public highly contested.[44] This launched an intense debate on the status of telegrams, including the arguments in favour and against ensuring their confidentiality[45]. The need to prohibit the disclosure of telegraph contents by employees of private telegraph companies was quickly recognized at the state level[46] and wiretapping was initially assimilated to malicious damage to telegraph companies property.[47]

To summarize, in the 18th and 19th century certain private interests such as the sanctity of the house and the confidentiality of correspondence were protected through certain legal constructs, mainly the Fourth Amendment, trespass actions and specific regulations ensuring the confidentiality of communications.

Section 2. Emergence of a distinct right to privacy

The notion of a distinct right to privacy started to appear at the end of the 19th century. In 1881, the Supreme Court of Michigan ruled on the *De May v. Roberts*[48] case. It is an often overlooked, but precursory, case. It involved a woman in childbirth calling for a doctor to assist her. The doctor came accompanied by another young man, who stayed at the apartment and helped him at some point during labour. The couple had accepted his presence, but

[40] See Eg. *Rice v. Williams*, 32 F. 437, 441 (C.C.E.D. Wis. 1887); *Folsom v. Marsh* 9 F. Cas. 342, 346 (C.C.D. Mass 1841).
[41] Justice Story wrote in the *Folsom v. Marshal* 9 F. Cas. 342, 346 (C.C.D. Mass 1841) case*:* "The general property and general rights incident to property, belong to the writer, whether the letters are literary compositions, or familial letters, or details of facts or letters of business. The general property in the correspondence remains in the writer and his representatives, *a fortiori*, third persons, sanding in no privity with either party, are not entitled to publish them, to subserve their own private purposes of interest, or curiosity or passion".
[42] *E.g*. CAL. PEN. CODE §640 (1872).
[43] *E.g*. 1868 Me. Laws 97; 'The Right to Privacy in Nineteenth Century America' (n 7) 1901.
[44] The New York Times described it as "unconstitutional and indecent […] an outrage upon the liberties of the citizen which no plea of public necessity can justify" in 'Washington – Secrets of the Telegraph' (*New York Times*, 24 June 1876) p.4, col.7 quoted in Seipp (n 17) 31.
[45] Illustrating the old security versus privacy debate: Republican Senator Sherman stated: "in violation of that principle which men born under English institutions have always regarded among the most sacred, that a man's private property, private papers, a man's household, and man's private affairs should be sacred from inspection…" and the opposite's view: the Senator from Vermont declared that "no man has a right to set up his private confidence or his private honor or his private anything when it stands in the way of countervailing consideration of security to the whole body of community or justice…" in Congressional Record, Senate, January 8, 1877, *quoted* in Seipp (n 17) 34-35.
[46] Alan F Westin, *Privacy and Freedom* (IG publishing 2015) 337.
[47] Seipp (n 17) 66.
[48] 46 Mich. 160, 165-66, 9 N.W. 146, 149 (1881) (emphasis added).

learning subsequently that that person wasn't qualified as a doctor, Mr and Mrs Roberts decided to sue. The Court reaches the conclusion that:

> In obtaining admission at such time and under such circumstances without fully disclosing his true character, both parties were guilty of deceit, and the wrong thus done entitles the injured party to recover the damages afterwards sustained, *from shame and mortification* upon discovering the true character of the defendants[49].

It is unclear from the judgement if the claim was for battery or for trespass. By using the vocabulary of "shame and mortification", Justice Marston, speaking for the majority, seems to reject the option of battery, the physical element missing. The cause of action could also be trespass, but again the vocabulary used seems to indicate something else[50]. The defendant is described as someone "who *intruded* upon the *privacy* of the plaintiff"[51] and in a particularly precursory way, the Supreme Court of Michigan declares that:

> The plaintiff had a *legal right to the privacy* of her apartment at such a time, and the law secures to her that right by requiring others to observe it, and to abstain from its violation[52].

The Court recognizes a right to privacy and grants recovery for its intrusion. Even if it is a real forerunner, this case received very little attention, probably because the vagueness of its legal basis. But for the first time, a right to privacy was invoked on its own, granted to repair what was perceived as an intrusion in a private place, at a private moment. The real pivotal moment for the recognition of a distinct right to privacy in the United States occurred nine years later, with a ground breaking article by two Bostonian scholars.

A. Tort Law

Tort law was already protecting certain private interests such as the sanctity of the home through its trespass regime, but at the end of the 19th century, a debate around the existence of distinct right to privacy clearly emerged in the legal discourse in the United States.

A.1. Warren and Brandeis' Article

In 1890, two young lawyers, Samuel D. Warren and Louis D. Brandeis wrote an article entitled *The Right to Privacy*[53] and published it in the Harvard Law Review. They defended the existence of a right to privacy, understood as "a right to be alone". The impact of this article on the development of privacy law in the United States cannot be understated. It was called by many as the "most influential law review article of all time"[54] and many proclaimed

[49] Id. at 149. (emphasis added)
[50] Alberto Bernabe, 'Giving Credit Where Credit is Due: A Comment on the Theoretical Foundation and Historical Origin of the Tort Remedy for Invasion of Privacy' (2012) 29 John Marshall J Inf Technol Priv Law 493, 508.
[51] *De May v. Roberts* (n 48) 146. (emphasis added).
[52] Ibid, 149.
[53] Samuel D Warren and Louis D Brandeis, 'The Right to Privacy' (1890) 4 Harvard Law Review 193.
[54] David J Garrow, 'Privacy and the American Constitution' (2001) 68 Soc Res 55, 57.

that it had given birth to the right to privacy as we know it[55] and was the "best example of the influence of law journals on the development of the law"[56].

The two Bostonian scholars called innovatively for a recognition of the "right to be alone"[57], more specifically of "a general right to privacy for thoughts; emotions and sensations"[58]. They proclaimed that "the private life, habits, acts and relations of an individual" needed to be legally protected.[59] They argued that a broad general principle, which they define as a right to privacy, existed in the common law and should be openly recognized. They concluded their article by stating:

> The existing law affords a principle which may be invoked to *protect the privacy of the individual from invasion* either by the too enterprising press, the photographer, or the possessor of any other modern device for recording or reproducing scenes or sounds"[60].

They based their argumentation on relying on certain English cases, trying to prove that privacy had been protected under the umbrella of other legal theories as intellectual property, defamation and contract laws. According to Warren and Brandeis, all these cases were "implicitly resting on privacy grounds"[61]. They didn't advocate for a "new" right to privacy, but for a recognition of this principle that, in their opinions, had been there all along and that courts commonly applied under the umbrella of other legal theories.

The famous formulation and conceptualization of the right to privacy as right to be let alone[62] obviously invokes the idea of a private sphere that should be free from any interference. It served as a solid theoretical basis on which the emerging actionable right to privacy was subsequently built. Several courts used this formulation when debating on the legality of the right to privacy.[63] The article also refers to the concept of individuals having control over divulgation of their personal information:

> The common law secures to each individual the *right of determining*, ordinarily, to what extent his thoughts, sentiments, and emotions shall be communicated to others"[64] and "the design of the law *must be to protect thos*e persons with whose affairs the community has no legitimate concern, *from being dragged* into an undesirable and undesired publicity and to protect all persons, whatsoever; their position or station, from having matters which they may properly *prefer* to keep private, made public *against their will*[65].

A.2. Debate

[55] Bratman (n 18) 627.
[56] Kramer (n 19) 704.
[57] Warren/Brandeis (n 53) 205.
[58] Ibid, 206.
[59] Ibid.
[60] Warren/Brandeis (n 53) 206. (emphasis added).
[61] Kramer (n 19) 713. Warren and Brandeis (n) 206, 213.
[62] Even if not the first time to term was coined- the first being Judge Thomas Cooley, Ibid. 195.
[63] See following section.
[64] Warren/Brandeis (n 53) 197. (emphasis added).
[65] Warren/Brandeis (n 53) 214. (emphasis added).

The publication of Warren and Brandeis' article sparked a heated debated in the US legal community. The two main point of contention were the nature of such new right (property based or personal?) and the nature of the damage plaintiffs were complaining of (moral or property related? financially assessable?).
The arguments brought forward by the two Bostonian scholars arguing the existence of the right to privacy were heavily discussed by their academic colleagues. In 1895, Hadley openly and vividly rejected the claims made by Warren and Brandeis[66], one of his main objections being that a specific violation of a right to property needed to be proven in order for an equity court to issue an injunction.

In 1903, Archibald McClean wrote down his opinion about the right to privacy:

> The right to privacy is not, however, one of property. It is a personal right, pure and simple. It has been called the *right to be let alone*. […] It is something which is each individual's very own. There is a division line in each one's life, over which the public may not step and demand as of right that which is on the other side. The law says there is such a thing at the privacy of one's life which legally belongs to the individual and which may not be *invaded* without the permission of its owner[67].

Courts also started to debate whether a right to privacy could actually be said as existing in the US legal regime or not. In *Marks v. Jaffa*[68] in 1893, an injunction was granted against a newspaper that published unauthorized images of two actors and proposed to the readers to choose which of the two they found the most attractive. It said:

> The action may seem novel, but […] An individual is entitled to protection in person as well as property, and now the right to life has come to mean the privilege to *enjoy life, without the publicity* or annoyance of a lottery contest waged without authority […] The courts will in such cases *secure to the individual what has been aptly termed the right 'to be let alone'*. […] Private rights must be respected as well as the wishes and sensibilities of people. […] Where they [people] are content with the *privacy of their homes they are entitled to peace of mind* and cannot be suspended over the press-heated gridiron of excited rivalry and voted for against their will and protest. The right of the plaintiff to relief seems too clear, both upon principle and authority, to require further discussion[69].

Surprisingly, freedom of the press and freedom of speech were not brought up. This happened to be a precursory case: the legality of an action for invasions of private life would be debated for many years to come.[70] It was clearly inspired by Brandeis and Warren's article and framed the question around a 'right to be let alone', the home and freedom from the invasions of the press.

---

[66] Herbert Spencer Hadley, 'Right to Privacy' (1895) 3 Northwestern Law Review 1.
[67] W Archibald McClean, 'The Right of Privacy' (1903) 15 Green Bag 494, 494. (emphasis added).
[68] 26 N.Y.S. 908 (N.Y. City Super. Ct. 1893).
[69] At 291-92. (emphasis added).
[70] See for example, 18 years late in 1911 *Hillman v. Star Publishing Co.* 64 Wash. 691 (1911): "we find that plaintiff's case does not fall within any rules so far recognized by the courts, permitting a recovering for an invasion of the *so-called right of privacy* […] Not so much because a primary right may not exist, but because, in the absence of a statute, no fixed line between public and private character can be drawn. […] *A wrong is admitted, but it is said there is no remedy.* We regret to say that this position is well taken. […] This case presents a subject for legislation" at 695-696 (emphasis added).

Most of the first cases discussing the validity of an actionable right to privacy were dealing with questions of appropriation of the plaintiff's image for commercial use. It is while trying to solve these cases at the end of the 19th and beginning of the 20th century, that judges wrestled with the legality of this "new" right. Two main obstacles to its acceptance were usually cited: the lack of physical injury assessable financially[71] and the absence of property rights involved.[72] Even once accepted as existing in common law, there was still a real debate whether the right to privacy was property based or a personal one.[73] The first cases accepting the claim of a right to privacy in cases of non-consented commercial use of one's image mainly based their reasoning around the argument that one has a right to property on his own likeness/image.

One of the most famous case rejecting Brandeis and Warren's proposal of a right to privacy is the *Roberson v. Rochester Folding Box Co*[74] case by the Court of Appeal of New York in 1902.[75] The case involved advertisement for flour found all over the country, which was consisting of printings of the plaintiff's portrait without her consent. She brought the case in front of the court in order to get an injunction to forbid the use of her image on this baking product advertisement.[76] The Supreme Court of New York Appellate Division confirmed the injunction granted by the lower court[77]. In writing his opinion, Judge Rumsey admitted that the argument advanced by the plaintiff was new and might lack authoritative precedents[78], but concluded that equity could protect more than simply property rights[79], and that even if a property right needed to be at stake, the injunction could be granted through the plaintiff's *right to property over her own body.*[80] That judgment was reversed by the New York Court of Appeals.[81] Judge Parker writing for the majority denied the injunction because of the lack of precedent[82], and also because he worried that the courts would become

---

[71] *See Chapman v. Western Union Telegraph Co*., 15 S.E. 901, 903-904 (Ga. 1892): "The body, reputation, and property of the citizen are not to be invaded without responsibility in damages to the sufferer. But, outside these protected spheres, the laws does not attempt to guard the peace of mind, the feelings, or the happiness of every one by giving recovery of damages for mental anguish… *the civil law* is a practical business system, dealing with what is tangible, *and does not undertake to redress psychological injuries*". (emphasis added).

[72] See *Atkinson v. John E. Doherty & Co*, 80 N.W. 285 (Mich. 1899). In this case the Court confirmed the refusal of an injunction which would have forbidden the defendant to manufacture cigars with the name and likeness of the plaintiff. The reasoning behind the decision was that neither the name, nor the image could be considered as property and that therefore, no recognized rights were violated (at 288-89) ; See also several years later *Henry v. Cherry Webb* 30 R.I. 13 (R.I. 1909) in which the court held that a right of action could not be sustained by mental suffering (except in libel and slander cases) at 25-26.

[73] See: *Chapman v. Western Union Telegraph Co*., 15 S.E. 901 (Ga. 1892): "the civil law is a practical business system, dealing with what is tangible, and does not undertake to redress psychological injuries" 903-904; *Atkinson,* Ibid. 288-89; *Schuyler v Curtis saga:* 15 N.Y.S. 787 (N.Y. Spec. Term 1891); 19 N.Y.S. 264 (N.Y. Gen. Term 1892); 24 N.Y.S. 509 (N.Y. Spec. Term 1893); 42 N.E. 22 (N.Y. 1895).

[74] *171 N.Y. 538 (1902).*

[75] This case is often considered as the first time a high court had to consider the existence of the right to privacy (Leon R Yankwich, 'Right of Privacy: Its Development, Scope and Limitations' (1951) 27 Notre Dame Lawyer 499, 503.)

[76] *Roberson v. Rochester Folding Box Co*., 64 N.E. 442 (N.Y. 1902).

[77] *Roberson v. Rochester Folding Box Co*., 71 N.Y.S. 876 (N.Y. App. Div. 1901).

[78] Ibid, 877.

[79] Ibid, 879-883. relying on *Schuyler v. Curtis* and *Marks v. Jaffa* and English cases cited by Brandeis and Warren in their article (n 53).

[80] Ibid, 880. (emphasis added).

[81] *Roberson v. Rochester Folding Box Co.*, 171 N.Y. 538, 544 (N.Y. 1902).

[82] "An examination of the authorities leads us to the conclusion that the so-called 'right to privacy' has not yet found an abiding place in our jurisprudence".

overwhelmed by pointless cases[83]. He called on the legislative body to intervene and settle the question[84] and reminded that libel laws might offer some kind of protection[85].

Judge Gray dissented and wrote:

> The right to life has come to mean the right to enjoy life to enjoy life – *the right to be let alone* […] and the term 'property' has grown to comprise every form of possession – intangible, as well as tangible"[86] and "in the existing state of society, new conditions affecting the relations of persons demand the broader extension of those legal principles, which underlie the *immunity of one's person from attack.*[87].

He therefore supported extending the right to property of an individual to his likeness and portrait[88], but also framed it as *a protection from attack*. This decision by the New York Court of Appeals was criticized by many and even led to an uproar by the general public[89] and in the legal profession.[90] It even catalysed the legislative process of the State of New York[91].

Things turned in favour of a legal recognition of the right to privacy by courts in 1905. The Supreme Court of Georgia was the first court of last resort to accept a cause of action for invasion of privacy in *Pavesich v. New England Life Insurance Co* case.[92] The facts of the case were quite similar to the *Roberson v. Rochester Folding Box Co* one, the portrait of the plaintiff was used without his consent in an advertisement, in this case for a life insurance company. The Court recognized the right to privacy as deriving from natural law[93]. It held:

> Each person has a liberty of privacy derived from natural law.[94] […] As to certain matters the individual feels and knows that he has a *right to exercise the liberty of privacy*, and that he has a *right to resent any invasion* of this liberty[95].

The Court clearly affirmed that: "The *liberty of privacy* exists, has been recognized by the law, and is entitled to continual recognition"[96].

---

[83] "If such a principle be incorporated into the body of the law through the instrumentality of a court of equity, the attempts to logically apply the principle will necessarily result, not only in a vast amount of litigation, but in litigation bordering upon the absurd".
[84] Ibid, 545.
[85] Ibid, 557.
[86] Ibid, 563.
[87] Ibid, 563-64.
[88] This view was contested by the Supreme Court of Rhode Island in the *Henry v Cherry Webb* case (n 72) in which the Court wrote: "In our opinion, the analogy [made by Judge Gray considering the right of privacy as a form of property] is not a sound one […] It is obvious that a right can not be one of person and of property at one and the same time. The conclusion would seem that if the right of privacy exists, and has been recognized by the law, it must be as a personal tort right. It can not be a right of property" at 22-25.
[89] *New York Times*, 23 August 1902, quoted in Denis O'Brien, 'The Right of Privacy' (1902) 2 Columbia Law Rev 437, 437–38.
[90] The American Law Review wrote: "The decision under review shocks and wounds the ordinary sense of justice of mankind. We have heard it alluded to only in terms of regrets", in Note (July-August 1902) 36 American Law Review 636.
[91] The following year, a statue was adopted making a misdemeanour to take advantage of an individual's name or image for commercial purpose, without that person's content: 1903 N.Y. Laws 132, §1.
[92] *Pavesich v New England Life Insurance Co*., 50 S.E. 68 (Ga. 1905).
[93] Ibid, 69-70.
[94] Ibid, 69-71.
[95] Ibid, 77.
[96] Ibid, 73.

The vocabulary used by the Court shapes the protection conceptually as a "liberty of privacy", which refers to the idea of protecting individuals from unwarranted interference. This decision was highly praised by academics[97] and had a tremendous impact on the legislative process of several states. Many courts followed the example and based their reasoning on *Pavesich*[98].

In another case, while arguing in favour of conceptualizing a potential right to privacy as a personal one and not property based[99], the Supreme Court of Rhodes Island wrote in *Henry v Cherry Webb*:

> It is obvious that a right can not be one of person and of property at one and the same time. The conclusion would seem that if the right of privacy exists, and has been recognized by the law, it must be as a *personal tort right*. It can not be a right of property. The *gravamen of the offense* in a violation of the right of privacy is the *interference with the seclusion of the individual*, and not the publication[100].

Once again, the offence is framed in term of seclusion, invasion of private space. It also shows a shift in the legal discourse: the conceptualisation of the offense is gradually evolving from a violation of property right to a personal tort right. This constellation of legal judgments created the legislative basis for the current discussion on privacy regulation in the United States.[101]

In 1960, William Prosser published an extensive study of over three hundred cases that followed Brand and Warren's article and discussed the existence of a right to privacy.[102] He concluded that all the law of privacy comprised four distinct privacy torts: (1) intrusion upon seclusion, solitude and private affairs; (2) public disclosure of private facts, (3) false light or 'publicity' and (4) appropriation of the plaintiff's name or likeness. The vast majority of states recognize these four torts, and they have been incorporated into the Second Restatement of Tort[103].

---

[97] *Michigan Law Review* 3 (May 1905) 559-63; *Case and Comment* 12 (June 1905) 2-4; *Virginia Law Register* 12 (June 1906) 91-99.

[98] For example in cases of unwanted commercial use of one's picture: *Edison v. Edison Polyform Mfg. C,* 67 A. 392, 395 9N.J. Ch. 1907.; *Foster-Millburn Co. v. Chinn,* 120 S.W. 364, 366 (Ky. 1909); *Munden v. Harris*, 134 S.W. 1076, 1079 (Mo. Ct. App. 1911) or in case of prisoners being able to view into the plaintiff's home: *Pritchett v. Bd. Of Comm'rs*, 85 N.E. 32.33 (Ind. App. 1908).

[99] For an example of court recognizing a right to privacy as a property one: See *Munden v. Harris,* Ibid, paras 658 and 660.

[100] *Henry v. Cherry Webb* (n 72) 25. (emphasis added).

[101] Judith Wagner DeCew, *In Pursuit of Privacy- Law, Ethics, and the Rise of Technology* (Cornell University Press 1997).

[102] William L Prosser, 'Privacy' (1960) 48 California Law Review 383.

[103] Restatement (Second) of Tort, § 652B: intrusion upon seclusion: "one who intentionally intrudes, physically or otherwise, upon the solitude of another or his private affairs or concerns, is subject to liability to the other for invasion of his privacy, if the intrusion would be highly offensive to a reasonable person, §652D: public disclosure of private facts: "One who gives publicity to a matter concerning the private life of another is subject to liability to the other for invasion of his privacy, if the matter publicized is of a kind that (a) would be highly offensive to a reasonable person, and (b) is not of legitimate concern to the public."; §652E: False light: "One who gives publicity to a matter concerning another that places the other before the public in false light is subject to liability to the other for invasion of his privacy if (a) the false light in which the other was placed would be highly offensive to a reasonable person, and (b) the actor had knowledge of or acted in reckless disregard as to the falsity of the publicized matter and the false light in which the other would be placed"; §652C: Appropriation of name or likeness: "One who appropriates to his own use or benefit the name or likeness of another is subject to liability to the other for invasion of his privacy" (1977).

B. The Fourth Amendment

With new technologies came new means of governmental intrusions into people's homes. As with the telegraph before it, the invention of the telephone created new potential threats to privacy. The early 20th century saw the telephone emerge as the main tool of communications, and consequently new methods of wiretapping were developed. Crucial Fourth Amendment cases involving private interests dealt with wiretapping situations.[104]
In 1928, the Supreme Court decided the *Olmstead v United States* case. The question at stake was whether wiretapping by federal officers fell under the scope of the Fourth Amendment. To answer this question, the Court had to identify what core interest was protected by the Amendment. Was it physical privacy (in which case wiretapping would not be subject to the Fourth Amendment) or should a broader concept of privacy be considered?[105] Instead of trying to answer this question, the Court simply focused on whether trespass occurred or not. It held that as trespass didn't occur wiretapping was not subject to the Fourth Amendment. By reaching this conclusion, the Court implied that only physical privacy was protected by the Fourth Amendment, more specifically "the interest in not having *one's solitude*, one's *physical privacy*, broken in by the police"[106]. This illustrates the most basic form of the 'sphere free from interference' argument, supporting the protection for a physical space – and therefore a physical understanding of privacy.

Brandeis wrote in a famous dissent opinion to this case:

> The makers of our Constitution […] sought to protect Americans in their beliefs, their thoughts, their emotions and their sensations. They conferred, as against the Government, the *right to be let alone*, the most comprehensive of rights and the right most valued by civilized men. To protect that right, every *unjustifiable intrusion* by the government upon the *privacy* of the individual, whatever the means employed, must be deemed a violation of the fourth amendment[107].

The contemporary majority view agrees today with Brandeis opinion. It is considered that wiretapping was a technological advancement that the Constitution's drafters could not have predicted, but that it is in reality not different from any conventional police searches.[108] This passage of Brandeis' dissent opinion is worth pointing out for two reasons. Firstly, Brandeis claims the existence of a constitutional right to be let alone, without any written basis in the Constitution. It is a bold position that, as developed *infra*, will be followed by the Supreme Court in subsequent cases. The second interesting point is the idea that, whatever the means employed, any privacy intrusion by governmental authorities should be covered by the Fourth Amendment. This conceptualizes the protection granted by the Fourth Amendment

[104] Priscilla M Regan, *Legislating Privacy: Technology, Social Values, and Public Policy* (University of North Carolina Press, 1995) 35.
[105] Richard A Posner, 'The Uncertain Protection of Privacy by the Supreme Court' (1979) 1979 Supreme Court Rev 173, 178.
[106] *Olmstead v United States,* 277 U.S. 438 (1928)178-80.
[107] Ibid, 478. (emphasis added).
[108] Posner (n 105) 178-80.

as a general right to be free from governmental *interferences*[109], regardless of the form they take. Brandeis' conceptual approach is broader than the Supreme Court's position, which "stuck" with the traditional requirement of having to prove physical trespass in several subsequent judgements[110]- illustrating a more restrictive vision of the Amendment's scope as protecting the secrecy and seclusion of physical space.

Progressively through the 20th century, the terminology of "privacy" starts to appear regularly in the Supreme Court's vocabulary. It illustrates that privacy is gradually recognised as an essential interest protected by the Fourth Amendment. In *Prince v. Massachusetts*, Justice Rutedge spoke of "the private realm of family life which the state cannot enter"[111]. Two years later, the Court linked the right to privacy and law of searches and seizures.[112] In his opinion in *McDonald v. United States*, Douglas mentioned "the constitutional *barrier* that protects the privacy of the individual" and "privacy of the home" [113]. In 1958, Douglas again, spoke in his dissent opinion in *Public Utilities Commission v. Pollak* of a "constitutional *right to be let alone*"[114] being 'the beginning of all freedom'[115] and said that "liberty in the constitutional sense must mean more than freedom from unlawful government restraint; it must include privacy as well, if it is to be a *repository of freedom*" [116].

In all these cases, the vocabulary of "realm", "barrier", "liberty" clearly references the conceptual apparatus of what I have called "freedom from interference". The notion of privacy is used in this context as referring to a physical space that cannot be entered by the State, where individuals have the "right to be alone". This right to be left alone is identified as a "repository of freedom". Protecting privacy is therefore conceptualized as a means to protect freedom. Being free from unwarranted interference is, in these cases, the value behind the Fourth Amendment. Even though the Court has at times used the terminology of "choice", the main conceptual paradigm behind the privacy protection granted by the Fourth Amendment remains one of freedom, and more specifically freedom from the State. The protection is still "interference-orientated".

C. Constitutional Right to Privacy

It has been demonstrated that the Fourth Amendment plays a vital role in the protection of privacy in the United States. But the Supreme Court did not limit itself to recognise a right to privacy in the limits of this Amendment. In the context of search and seizures problems the previous section detailed how the Supreme Court interpreted privacy protection as entailing a certain freedom from the government, especially within the sanctity of the home- but not exclusively. This understanding of privacy as liberty was extended in important ways by the Court in subsequent cases.[117] From the mid-sixties, the Supreme Court recognised an autonomous distinct constitutional right to privacy.

---

[109] Ibid, 181-82.
[110] In *Goldman v United States*, 316 U.S. 129 (1942); *Silverman v United States* 365 U.S. 505 (1961).
[111] 321 U.S. 158, 166-167 (1944).
[112] *Davis v United States*, 328 U.S. 582 (1946) 587.
[113] 335 U.S. 451, (1948) 455-56.
[114] 343 U.S. 451 (1958) 468.
[115] Ibid, 467.
[116] Ibid, 468
[117] Whitman (n 15) 1214.

The first time it did so was in the *Griswold v. Connecticut* case[118]. The case looked at the constitutionality of a Connecticut statute banning the use and advertisement of contraceptives.[119] The Court decided that the criminal statute was violating marital privacy, which it deemed included in the Constitution and therefore struck the Connecticut statute down. The vocabulary used by the Court to justify the existence of a right to privacy in the Constitution – without a written basis- is worth pointing out. Justice Douglas found that the right to privacy was part of the Constitution, most specifically in "the penumbras" and "emanations" of guarantees of the Bill of Rights. These guarantees created what he named: *zones of privacy.*[120] Justice Goldberg, Marshall Harlan and White all wrote concurring opinions, stating that the due process clause was protecting privacy. Justice Goldberg also relied on the Ninth Amendment.[121] This innovative judgment received a lot of attention, and although many agreed with the overall decision, numerous commentators criticized Douglas's "nebulous language"[122]. Garrow summarized it by writing:

> Douglas's use of so distinctive a word [penumbras] became a prime target for those who were either methodologically uncomfortable or substantively opposed to constitutional recognition of a right to privacy[123].

In the *Whalen v. Roe*[124] case, in 1977, the Supreme Court stated:

> The cases sometimes characterized as protecting 'privacy' have in fact involved at least two different kinds of interests. One is the individual interest in avoiding disclosure of personal matters, and another is the interest in independence in making certain kinds of important decisions[125].

The last interest described by the Court is the one recognized in Griswold and other cases relating to decisional privacy. The first one however had not been yet defined by the Court and will ground what has been called the "constitutional right to information privacy". The

---

[118] 381 U.S. 479 (1965).

[119] The same statute had been brought in front of the Court four years earlier, but the Court decided at the time to dismiss the case on the basis that the plaintiffs lacked standing because the law was never enforced: *Poe v. Ullman* 367 U.S. 497 (1961) at 501, 508 and 509.

[120] He detailed his opinions by writing: "The foregoing cases suggest that specific guarantees in the Bill of Rights have penumbras, formed by emanations from those guarantees that help give them life and substance. […] Various guarantees create zones of privacy. The right of association contained in the penumbra of the First Amendment is one, as we have seen. The Third Amendment, in its prohibition against the quartering of soldiers "in any house" in time of peace without the consent of the owner, is another facet of that privacy. The Fourth Amendment explicitly affirms the "right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures." The Fifth Amendment, in its Self-Incrimination Clause, enables the citizen to create a zone of privacy which government may not force him to surrender to his detriment. The Ninth Amendment provides: "The enumeration in the Constitution, of certain rights, shall not be construed to deny or disparage others retained by the people" at 484.

[121] Ibid, 487.

[122] Garrow (n 56) 61. Douglas's opinion was criticized for being unclear and ambiguous (Paul G Kauper, 'Penumbras, Peripheries, Emanations, Things Fundamental and Things Forgotten: The Griswold Case' [1965] Mich Law Rev 235, 242–44.) ; confusing marital privacy and access to information (Robert G Dixon, 'The Griswold Penumbra: Constitutional Charter for an Expanded Right of Privacy?' [1965] Mich Law Rev 197, 214–17.) and others even calling it "a malformation of constitutional law which thrives because of the conceptual vacuum surrounding the legal notion of privacy" (Hyman Gross, 'The Concept of Privacy' [1967] N Y Univ Law Rev 34, 35.) One of the main point of criticism was directed at the use of the word "penumbra", even though – contrary to most opinions – not the first time used by the Court (Garrow (n 56) 62.)

[123] Garrow (n 56) 61.

[124] 429 U.S. 589 (1977).

[125] Ibid, 599-600 (emphasis added).

same year, that interest was recognized again by the Court in *Nixon v. Administrator of General Service.*[126] By extending certain 'zones of privacy' already constitutionally protected since *Griswold* to a general interest for an individual to avoid unwanted disclosure of personal information, the Court approaches the question of constitutional protection of privacy with a focus on the individual as main actor.

Because there is no explicit written basis in the Constitution, and because the cases invoking it are so varied, this constitutional right to privacy has been heavily criticised[127], and the Court never continued to develop the notion of a specific right to information privacy. In the 80s, the Supreme Court started to use the vocabulary of "freedom" when dealing with cases that would normally fall under what is traditionally understood as privacy-related.[128] It is usually stated that this is because of the weak argumentation of Justice Douglas in the *Griswold* case and the legal community was not convinced by the constitutional argument put forward in subsequent cases. But another, additional, explanation might be related to the conception of the right to privacy itself- as a right to freedom: freedom from interference in their homes, and in making certain decisions related to their private lives independently.

D. Federal Privacy laws

Through the 20th century, federal laws were enacted sporadically to counter specific conducts that could infringe individual's privacy. This led to a fragmented framework of different privacy laws, each of them tackling different privacy concerns. Each wave of new technologies led to corresponding legislative actions. In the seventies, the financial sector became the object of concerns and therefore several regulations were enacted at the federal level: the Fair Credit Reporting Act of 1970[129], Bank Secrecy Act of 1970[130], Right to Financial Privacy of 1978[131]. The growth in federal privacy regulatory frameworks only grew further in the 80s: the Privacy Protection Act of 1980[132], the Cable Communications Policy Act of 1984[133], the Computer Matching and Privacy Protection Act of 1988[134], Employee Polygraph Protection Act of 1988[135], Video Privacy Protection Act of 1988[136], Electronic Communications Privacy Act of 1986[137]… It then continued in the 90s, every time to tackle a specific area of concern: the Telephone Consumer Protection Act of 1991[138], the Driver's Privacy Protection Act of 1994[139], the Health Insurance Portability and Accountability Act of 1996[140], the Children's Online Privacy Protection Act of 1998[141], The

[126] 433 U.S. 425 (1977) 457.
[127] Wagner DeCew (n 101) 21.
[128] See Garrow (n 56).
[129] 15 U.S.C. § 1681.
[130] Pub. L. No. 91-508.
[131] Pub. L. No. 95-630.
[132] Pub. L. No. 96-440, 94 Stat. 1879, codified at 42 U.S.C. § 2000aa.
[133] 42 U.S.C. § 551.
[134] Pub. L. No. 100-503, 102 Stat. 2507 (codified as amended at 5 U.S.C. § 552a(a)(8)–(13), (e)(12), (o)–(r), (u)).
[135] Pub. L. No. 100-618, codified at 29 U.S.C. § 2001–09.
[136] Pub. L. No. 100-618, 102 Stat. 3195, (codified at 18 U.S.C. §§ 2710–11).
[137] 18 U.S.C §§ 2510–22, 2701–11, 3121–27.
[138] Pub. L. No. 102-243, 105 Stat. 2394 (codified at 47 U.S.C. § 227).
[139] 18 U.S.C. §§ 2721–25.
[140] Pub. L. No. 104-191, 110 Stat. 1936.
[141] 15 U.S.C. §§ 6501–06.

Gramm-Leach-Bliley Act of 1999[142],… The beginning of the 21st century focused on increasing law enforcements powers and the USA Patriot Act of 2001[143] and Homeland Security Act of 2002[144], amongst others, were enacted.
This long (non-exclusive) list shows how fragmented the privacy legal regime of the United States is, but also demonstrates how "interference-orientated" the whole system is. Each new potential interference with privacy is addressed through a specific statute, with each sector having multiple frameworks addressing different issues.

Section 3. Conceptual Approach

After reviewing the historical development of privacy protections in the United States, it is clear that its approach to regulating and protecting private interests is orientated towards the prevention of external interferences. From the 18th century, the individual is conceived as master of his own home and different legal constructs were mobilized by courts in order to ensure that his freedom would be respected and that interferences with the sanctity of his house would be limited. Even once the notion of a right to privacy emerged, and during the legal debate it provoked, privacy protection is still very much understood as guaranteeing a form of freedom. Furthermore, numerous statutes were enacted to address specific privacy threats- illustrating well the focus in the United States conception of privacy regulation on interferences and the need for regulatory action to protect individuals from abusive practices. This is arguably influenced by the liberal thinking dominant in the US and the conception of the "state" as the "prime enemy" of individual freedoms.[145] France, on the other hand, approached the exact same questions from a very different point of view as the next part will illustrate.

Part II – France

From the 18th century, France addressed the issue of protecting certain aspect of private life with a different approach than the United States'. With the introduction of the concept of "free press" after the Revolution, the French legal community was immediately aware of the potential negative repercussions such a notion could spark. The first legal protections granted to individuals to ensure the respect of their private lives were therefore specifically enacted in response to abusive press practices. Thanks to defamation laws and the specific interpretation of the civil responsibility regime, courts started to flesh out a legal regime protecting people's public image and granting them the right to oppose unwarranted disclosure of private facts or misappropriation of personal images. The notion of a 'right to privacy' appeared in the judicial and scholarly discourses from the end of the 19th century but rooted in specific legal constructs. It is only in 1970 that the legislator recognised a general and distinct right to privacy in the civil code. This historical evolution will be

[142] Pub. L. No. 106-102, 113 Stat. 1338, (codified at 15 U.S.C. §§ 6801-–09).
[143] Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act" (USA PATRIOT Act) of 2001, made changed to FISA and ECPA, See: 18 U.S.C. § 3127(3) as amended by the USA PATRIOT Act § 216 and 50 U.S.C. § 1804(a)(7)(B) as amended by USA PATRIOT Act § 204.
[144] 6 U.S.C. § 222.
[145] See Regan (n 104) 3; Whitman (n 15) 3.

explored in this part firstly by examining how certain private interests were protected through other legal constructs and then by explaining how a distinct right to privacy was established - first by the courts in the regime of civil responsibility, then as a distinct right.

Section 1. Protection through other legal constructs

As in the United States at the same time, specific provisions in French law were indirectly protecting certain private interests in the 18th and 19th century - well before any discussion or recognition of a distinct right to privacy. Whereas their American counterparts were mainly worried about protecting the sanctity of the house from State and private intrusions, French legislators and courts of the time focused on protecting their citizens honor and intimacy from misrepresentation and abusive practices from the press.

This is not to say that other private interests were not protected under French law in the 19th century. The civil code of 1804 guaranteed individuals intimacy in their own house by regulating neighbour's direct view on said property[146], and from 1810 intruding the home by state agents or private individuals was considered a crime and punished by law. The secrecy of correspondence was also protected by criminal law. It was prohibited to open someone else letters since 1810, regardless if the interception was undertaken by a state agent, or by a private individual.[147] Nonetheless, it is in the context of issues raised by the free press that explicit reference to "private life" and "private interests" appeared and these two concepts received their first explicit legal protection.

A. Protection against the Press

The notion of 'private life' appeared in the legal discourse as worth protecting for the first time at the end of the 18th century, in the context of defamation. The principle of 'freedom of expression' was introduced just after the Revolution but the French legal community had soon become aware of its corelated negative consequences and legal safeguards against potential abuses were put in place. Constitutional efforts to protect the freedom of the press were joined by guarantees to preserve private life. Ensuring that citizens' private lives were respected was considered as an essential part of safeguarding their "personal honor", which in turn was understood as vital to preserve the freedoms acquired by the Revolution.[148]

The Constitution of 1791 established protections for the press but also prohibited "calumnies and insults relative to private life"[149]. The authors of this provision followed a certain scholarly trend at the end of the Ancien Regime that pushed for a merger between the old regime of 'insults and calumnies' into what was going to become the legal notion of

[146] arts 675-679.
[147] Former criminal code, Article 187. ('Ancien code pénal')
[148] Whitman (n 15) 1172.
[149] CONST. du 3 septembre 1791, tit. III, ch. V, art. 17 (« les calomnies et injures contre quelques personnes que ce soit relatives aux actions de leur vie privée, seront punies sur leur poursuite »).

'diffamation'[150].[151] The first legal definition of diffamation is found in the Law of 17 May 1819. It states that truth was not accepted as a valid defense when the defamation targeted private individuals.[152] There was no express reference to private life or private interests in the law itself, but the law was influenced by a famous speech given by Pierre-Paul Royer-Collard, a high-profile politician who was a strong advocate of the reform of the legal regime regulating press activities. He advocated for private life to be "walled off"[153], to protect it from defamation and insults. His opinion was that the press could only operate in the public space and that truth could not be used as an excuse to lawfully publish facts about the private lives of individuals.

The Statute of 11 May 1868, enacted under Napoleon III, made it a criminal offense to publish any 'fact relating to private life'[154], but the Statute was abrogated in 1881[155]. The situation changed with the Third Republic, and the enactment of new Law of the Press of 29 July 1881. It kept the prohibition of truth as valid defense in cases of defamation concerning the private life of individuals.[156] This law establishes the defamation regime and includes criminal sanctions. One of the requirements to prove defamation is the "malicious intent"; if good faith can be proven then there is no defamation. This is not the case however when the information relates to private life. In this case neither the truth, nor the good faith has any impact. Private life, as a general notion, was therefore protected from a criminal perspective through this legal construct.[157]

These legal developments relating to press publications, show the emergence of the notion of 'private life' being worthy of legal protection, admittedly only in cases of defamation. The protection granted through the Law on the Press of 1881 was limited: a simple publication of an information concerning a private individual was not sufficient. To qualify as defamation, the plaintiff needed to prove that the allegation made against him constituted an infringement upon his honor.[158] Still, if the allegation concerning the private life of an

---

[150] This term invoking violation/atteinte of reputation was used sporadically since the 16th century. In Halperin (n 155) 60.

[151] Halperin (n 155) 60. To know more about regime of insults See Stephan Balthazar, 'Vérité et Secret: la Protection de la 'vie privée' dans l'ancien droit allemande, français et anglais' (2006) 74 Tijdschrift voor Rechtsgeschiedenis 337.

[152] Whitmann (n 15) 1173.

[153] "murée"

[154] art 11.

[155] Still, in 1874, the Cour de Cassation considered publishing in a newspaper the names of people participating in a pilgrimage as a violation of private life (even though the pilgrimage was public). The Cour extended the protection of private life from the 'citizen's home' to facts relating to 'personal domain'('domaine interieur), which was a matter of 'freedom of conscience' in Dalloz Periodique, 1874, I, 273 in Jean-Louis Halperin, 'Protection de la vie privée et privacy : deux traditions juridiques différentes ?' (2015) 48 Nouveaux Cahiers du Conseil Constitutionnel, 61.

[156] Law of 29 July 1881 on the Press, as amended by Ordonnance of 6 May 1944, art 15 al2bis.

[157] In the 20th century, when courts dealt with this provision, they never expressively defined the notion of "private life" in this context, but analyzed the subject on a case-by-case basis: See: Cass. Crim. (7 March 1932) Gaz. Pal. 1932, 2, 18; Cass. Crim. (12 December 1934) Gaz. Pal. 1935, 1, 239; Cass. Crim. (3 March 1949) J.C.P. 1949, II, 4978, note Colombini; D. 1949, 205, note A.L.P; Cass. Crim. (10 July 1959) J.C.P. 1960, II, 11441, note Mimin).

[158] Article 29 defines defamation as: "« Toute allégation ou imputation d'*un fait qui porte atteinte à l'honneur ou à la considération de la personne ou du corps auquel le fait est imputé est une diffamation.* La publication directe ou par voie de reproduction de cette allégation ou de cette imputation est punissable, même si elle est faite sous forme dubitative ou si elle vise une personne ou un corps non expressément nommés, mais dont l'identification est rendue possible par les termes des discours, cris, menaces, écrits ou imprimés, placards ou affiches incriminés ». (emphasis added).

individual was found as impacting his honor, it would be qualified as defamation *even if it was true*. This protection was not available for American citizens at the time.[159]

This illustrates the close link between the first legal protections of private life and the notion of honor. Honor was considered an essential aspect of life, and it was protected by the defamation laws described above. When the defamation (the infringement upon honor) related to private life, it was considered that additional protection should be granted: even the truth behind the divulgation would not be accepted. This refers to the idea of granting individuals some form of "control" over their private life. It does not matter if the fact divulged is true or not- what matters is that the individual's private life- and therefore his honor- is being infringed upon. He, and him only, should have the ability to decide how he was to be portrayed in the public place. The fact that the first legal arrangement protecting explicitly "private life" was relating to defamation cases shows how the French legal regime of the time was orientated towards individuals, more specifically their honor.

During the 19th century, this was the only statutory provision specifically protecting private life as such. However, the notion of "right to privacy" slowly emerged in scholarly work and various court judgments.

Section 2. Emergence of a distinct right to privacy

The right to respect of private life was only recognized as an independent right by the legislation in 1970, but from the beginning of the twentieth century courts faced litigation relating to violations of certain private interests. The majority of first decisions concerned celebrities asking for injunctive relief for disclosure of private information or publication of their image.[160] Moving from the criminal sphere of defamation to the civil domain, courts used general provisions of the civil code[161] and slowly constructed, on a case-by-case basis, a solid legal protection of private interests. By doing so, French courts showed that, contrary to common belief the principle of *stare decisis* was accepted in the French system.[162]

The progressive recognition of a right to respect of private life by courts took place in the 20th century against the backdrop of another debate: the scholarly development of the notion of "personality rights"[163]. This concept appeared in the legal scholarship in the nineteenth century, initially in Germany and Switzerland, to then emerge in France in the beginning of

[159] Under common law, truth was accepted as defense in a civil action. Therefore, this libel action was not a viable option when the private information shared was true. In 1769, William Blackstone said about it: "a libel must appear to be false, as well as scandalous; for, if the charge be true, the plaintiff has received no private injury, and has no ground to demand a compensation for himself, whatever offense it may be against the public space: and therefore, upon a civil action, the truth of the accusation may be pleaded in bar of the suit" in William Blackstone, *Commentaries on the Laws of England* (1769) reedited in (The University of Chicago Press, 1979) 150. Contrary to the French system, this characteristic of libel laws made it quite inappropriate to deal with issues relating to private aspect of people's life in the United States.
[160] Halperin (n 155) 62.
[161] such as Article 1382 regulating civil responsibility.
[162] Wencelas J Wagner, 'The development of the theory of the right to privacy in France' (1971) 1971 Wash. U. L. Q. 45, 49.
[163] In French: "droits de la personnalité".

the 20th century.[164] Initially mentioned in the context of legal theory[165], it is mainly in the field of civil law that the concept of personality rights was elaborated. Perreau wrote in 1909 a ground-breaking article advocating for the legal recognition of personality rights in the French system, arguing that the civil code should not exclusively regulate patrimonial rights and that a theoretical background recognizing human beings as "individual distinct from all others" should be established.[166] This article triggered an important debate in the French legal community[167], and in the second half of the 20th century the concept of personality rights was finally accepted. The Court of Cassation consecrated them for the first time in 1968 in its annual report.[168] The legislator followed in 1994 in introducing a section specifically named "violations of personality" in the Code penal- personality being understood in this context in the same way as personality rights[169]. The debate still continued however, on the classification of certain rights as belonging to personality rights or not, but also on the question whether a general right to personality should be recognized, as it is in Germany for example.[170] The French system settled on not recognizing a general personality. The logic behind distinguishing different personality rights was not to list them but rather to establish a general classification that would allow recognition of existing personality rights and include potential new ones.[171] Personality rights were understood as giving "individuals the power to control and regulate the use of various attributes of the self"[172].

This debate is worth mentioning because the right to respect of private life- once officially recognized- is now considered as a personality right, meaning it is intrinsically linked to the personality of its holder. This is another element showing how the French "privacy regime" is orientated towards the individual himself. It is also noteworthy to keep in mind when analyzing the development of the protection granted by courts to "private life" through the civil responsibility regime, because the idea that personal harm, not exclusively damage to property, could be granted recovery was expressly discussed by scholars at the time- making it easier for courts to accept and implement it (in comparison, for example, to their American counterparts).

This does not mean that courts never used the legal basis of property rights to offer redress to individuals complaining of infringement upon their private life. For example, a case in front of the Cour d'Appel of Paris in 1954 involved the unauthorized publication of Marlène Dietrich's own recollections of her private life. The Court of Paris sided with Dietrich and stated:

[164] Repertoire de Droit civil, Dalloz, Titre 1. Notion et identification des droits de la personnalite, 4.
[165] Boitsel, *Philosophie du Droit*, t1 (1889) n131 ss. Was of the idea that every man was born with a specific set of rights, including personality rights.
[166] Perreau, 'Des droits de la personnalité' (1909) Rev. Trim Dr. Civ. 501.
[167] Demogue, *Traite des obligations en general,* t. IV(1924) n 417.
[168] Repertoire droit civil Dalloz (n 164) 6.
[169] Ibid.
[170] Pierre Kayser, 'Les droits de la personnalité : Aspects théoriques et pratiques' (1971) 69 *Rev. Trim Dr. Civ.* 447.
[171] Ibid, 457. To read more on different specific personality rights and their legal regime: See Ibid, 457- 488.
[172] Jeanne M Hauch, 'Protecting Private Facts in France: the Warren and Brandeis Tort is Alive and Well and Flourishing in Paris' (1993-1994) 68 Tul. L. Rev. 1219, 1229.

> The recollections of each individual concerning her private life are part of her *moral property* (…) no one may publish them, even without malicious intent, without the express and unequivocal authorization of the person whose life is recounted[173].

As it will be shown in the following sections, courts were willing to grant individuals the ability to oppose unwarranted disclosure of private facts. They did so by interpreting the existing frameworks at their disposal: property rights, but mainly the regime of civil responsibility.

A. Civil Responsibility Regime

The role French courts played in the elaboration of the right to respect of privacy cannot be underestimated. As Hauch puts it:

> The development of privacy rights in France was a remarkably 'uncivil' process in the sense that, without benefiting of any legislative guidance on the subject, French judges essentially created the right to oppose the publication of private facts[174].

Because of the lack of specific legal protection of private life, civil judges used general rules to offer protection to claimants, in particular the regime of civil responsibility under Article 1382. These general principles, broader than specific causes of action, offered a fertile ground for growing new rights, in particular one protecting private interests.[175]

The Article 1382 of the Code civil is the pillar of French civil responsibility. It states:

> Any act by which a person causes damage to another makes the person by whose fault the damage occurred is liable to make reparation for such damage.[176]

To be granted recovery under Article 1382, three elements need to be proven: a fault, a damage and a causal link between the two. This regime includes the possibility to offer recovery for moral damage, which was useful for courts to build a better protection for personality rights, including what would become the right to respect of private life[177]. Since the nineteenth century, French courts have admitted the possibility that the required damage under Article 1382 may be nonmaterial, including so-called moral damage. At the time, the moral damage was understood as caused by a "violation of the sentiment of modesty as concerns personal and family life"[178]. As mentioned in the first part of this chapter, US courts had a different experience: they debated for many years whether a moral damage could be accepted and struggled with the complexity of financially assessing it. On the other hand, the French civil courts progressively ensured individuals the respect of their private life-

[173] 1855 D.S. Jur, 295.
[174] Hauch (n 172) 1231.
[175] James K Weeks, 'Comparative Law of Privacy' (1963) Clev. Marshall L. Rev. 484, 502.
[176] Art 1382 Code civil: 'Tout fait quelconque de l'homme, qui cause a autrui un dommage, oblige celui par la faute duquel il est arrive, à le réparer'.
[177] Roger Nerson, 'La protection de la vie privée en droit français' (1971) 23 *RIDC* 737, 755.
[178] Hauch (n 172) 1232; Pierre Kayser, *La Protection de la vie privée* (1984) 9-13.

considering any intrusion as a fault resulting in prejudice[179] and also interpreted Article 1382 as ensuring confidentiality of letters.[180]

A.1. Concrete examples

One of the areas in which Article 1382 was useful- and very much utilized by courts- to protect what we understand now as falling under the scope of private life, is the appropriation by a third party of an individual's image, without the latter consent. Contrary to their American counterparts, French courts did not hesitate to grant recovery in these cases. This is linked to the fact that they accepted moral damages. When confronted with the question of whether individuals had certain rights over their own image, French courts did not hesitate to answer in the positive: the debate then concerned the scope of such rights, not its existence.[181]

The *Rachel* affair[182] in 1858 seems to be the first case in which the general regime of civil responsibility was used to protect private interests in the nineteenth century. It was a precursory case involving the reproduction of sketches of a famous actress (Rachel) after her death. The facts are as follows: when Rachel died, her sister asked a photographer to take some pictures of her deceased sibling on her deathbed, with the clear agreement that no copies could be made. A short while later, sketches representing the deathbed scene emerged in local stores, their resemblance to the photographs leaving no doubt that their author had had access to the private pictures. Rachel's sister thus decided to bring the photographer and the sketches' artist in front of the courts, requesting all copies of the sketches and photographs to be seized and destructed. The Court agreed to such measures, ordering the destruction of all the sketches and photographs and found the sketches' publication to be illegal.[183] It stated that:

> No one may, without the explicit consent of the family, reproduce and bring to the public eye the image of an individual on her deathbed whatever the celebrity of the person involved.[184]

Under Article 1382, the three requirements were found: a fault, consisting in the publication of private matters without consent, causing a damage. By stating that the mere publication without consent amounts to a fault, the court actually created a strict liability tort. The defendant's intentions or reasonableness were thus found irrelevant.[185] Interestingly the court also added:

> The *right to oppose* this reproduction is *absolute*. It finds its foundation in the respect which the *suffering* of families demands, and it cannot be ignored without stirring the most intimate and respectable sentiments.[186]

[179] TGI Seine (24 November 1965) D. 1965 457.
[180] More on this *infra.*
[181] Wagner (n 162) 50.
[182] *Affaire D Rachel*, Trib. pr. inst. de la Seine (16 June 1858) 1858 D.P. III 62 (Fr.).
[183] Ibid, 62.
[184] Ibid.
[185] Hauch (n 172) 1234.
[186] *Rachel* (n 182) 62. (emphasis added).

This quote highlights different important elements. The terminology of a 'right to oppose' indicates that the protection is framed under the paradigm of control. This vision of granting individuals a "right to oppose" unwarranted reproduction of their image will shape the vision of privacy regulation in French in the following years. It is also noteworthy to point that the court states that the "suffering of families" is at the foundation of the need of protection. The focus is thus on the emotional damage of the plaintiff. This shows the very early acceptance and recognition of French courts of an "emotional injury". It also implies that the court doesn't require the revelation to be objectively offensive to grant compensation[187], the focal point of the analysis being the 'emotional damage' of the plaintiff.[188]

This case also illustrates the inclination of French courts to grant specific relief, rather than financial, in privacy claims. As this decision shows, courts actively tried to protect private interests and did not shy away from ordering measures of seizure, alteration or destruction, even without clear legislative authorization.[189] They wanted to give individuals an effective protection of their private interests, in this case their images, and this protection was understood as giving effective action to oppose undesired disclosure.

Other cases in the second part of the 19th century and 20th century dealt with the misappropriation of individual's images without their consent, and a large part of the case-law that essentially constructed the right to private life did so through these cases. It usually involved celebrities, for example Alexandre Dumas[190] or Brigitte Bardot[191]. The right to image[192] was later recognized as a distinct personality right, that even if connected to private life[193], was nonetheless conceptually separated. But at the end of the 19th century and beginning of the 20th, these types of litigation are the ones that mainly sparked the legal conversation around the recognition of a right to respect of private life.

They were not the only ones: the confidentiality of correspondence was another subject that was regularly protected by courts. Criminal law punishes opening someone else's letters since 1810, either by a state agent, or by a private individual[194]. The current criminal code punishes the fact of intercepting, opening, eliminating or diverting any correspondence, electronic or not[195]. The confidentiality of letters has also been protected under civil law, more specifically thanks to creative civil judges. As mentioned *supra*, judges used the civil responsibility regime to sanction violating the secrecy of correspondence, interpreting the tryptic requirements of "a fault causing a damage" on a case-by-case basis. They decided that the content of secret private letters could only be divulged with the author's consent. An individual failing to respect this was therefore considered as having committed a fault. This

[187] Which again is different than the US regime: See Restatement (Second) of Torts para 652D (1977) which requires the matter published to be "highly offensive to a reasonable person".
[188] Hauch (n 172) 1234.
[189] Hauch (n 172) 1235.
[190] *Dumas v Liberté*, CA Paris (25 May 1867) 13 A.P.I.A.L. 247 (discussing whether Dumas had a property right over his image or a right to privacy- see Whitman (n 15) 1175).
[191] Tribunal de la Seine (24 October 1965), Cour de Paris (27 February 1967).
[192] "droit à l'image"
[193] Both have their current legal basis in the Article 9 of the civil code: the Cour of Cassation linked the right to image to the article 9 in 1998: Civ. 1 (16 July 1998) Bull. N 259, 181.
[194] Former criminal code, art 187. ('Ancien code pénal')
[195] Criminal code, art 226-15, modified by Ordonnance n°2000-916 of 19th September 2000, Art. 3 (V) JORF 22nd September 2000 in force 1st January 2002.

fault was deemed as almost always causing damage (often a moral one) for the person concerned by the letter's secret. Therefore, the conditions to trigger Article 1382 were met.[196] By ensuring the confidentiality and secrecy of letters through the civil responsibility regime, courts granted individuals a right to oppose unsought disclosure of the private information contained in their correspondence. [197]

A.2. Complications

One of the issues with protecting private interests through the regime of Article 1382, is that the strict requirement of civil responsibility needed to be proven in each case: only conducts amounting to a fault causing damage could be redressed by the courts based on Article 1382. In theory, if the victim could not prove he suffered a damage, recovery could not be granted[198]. In order to be able to provide relief to more applicants, courts started to interpret the tryptic requirements of civil responsibility regime quite broadly and easily accepted the existence of fault and damage when the case was related to an intrusion upon private life. For example, the element of fault was interpreted very loosely by certain courts: "*the simple fact of publishing* a photographic portrait of another without his consent amounts to a fault for which reparation is due"[199]. The assessment of 'damage' was also conducted quite flexibly, certain judgements declaring: "Every infringement on the personality right *implies* damages"[200] and "there are cases in which the plaintiff was granted actual damages even though he did not show that he was really injured by the defendant, except for the fact that *his right was infringed upon*"[201]. This created a debate in the doctrine, certain scholars accepting this loose interpretation of Article 1382,[202] others wishing courts stuck to a strict interpretation of the three required elements[203].

By using Article 1382 in a regular and coherent way for years, the French judicial body *de facto* created a right to respect of private life, and completely shaped it: from its holder, its powers and its limits.[204] Nerson summarized it by stating: "by the consistency and regularity of their judgments; the courts have fashioned the contours of a real right to the secrecy of private life"[205]. As it will be developed *infra*, this notion of right to privacy as a right to secrecy is essential to the specific conceptualization of the right to respect of private life in the French legal system.

This creative judicial thinking had however proved insufficient in addressing the issues concerning infringements upon private life. Certain conduct impacting private interests could not be sanctioned through the existing legal framework.[206] Judges, even with

[196] Nerson (n 177) 756.
[197] Kayser, 'Les droits de la personnalité' (n 170) 466. To know more on this including an analysis of the case law, see Pierre Kayser, 'Le principe du secret des lettres confidentielles et ses rapport avec le principe de droit public de la liberte et de l'inviolabilite de la correspondence' in *Melanges Pierre Voirin* (1966) 437-465.
[198] Nerson (n 177) 756.
[199] *Bardot v. Beaverbrook Co*., trib. gr. inst. 3d ch., Seine (1966) J.C.P. II. 14521 (emphasis added)
[200] *De Lartigne v. Soc. Gevaert,* trib. civ., Seine) (1956) Gaz. Pal. I. 284 (emphasis added).
[201] Eg. *Bardot v. Beaverbrook* Co (n 199) in Wagner (n 162) 63.
[202] Stoufflet, *Le droit de la personne sur son image*, vol I (J.C.P 1957) 1374.
[203] L Martin, 'Le secret de la vie privée' (1959) Rev. Trim. Dr. Civ. 227, 255
[204] Nerson (n 177) 757.
[205] quoted in Hauch (n 172) 1232.
[206] Agathe Lepage, 'Repertoire de Droit civil' (*Recueil Dalloz*, September 2009, last update November 2017) 41.

innovative interpretations, could not create a fully developed independent protection of privacy interests. Legal scholars therefore called on legislative action to be taken to put an end to the uncertainties caused by the situation. They called for a right to respect of privacy to be consecrated by law and to be recognized as an autonomous independent right. For example, Badinter wrote: "The protection of private life, based at the beginning on general principles of tortious responsibility, later departed from it in order to lead to the recognition of a genuine subjective right"[207] and "in the matter of protection of private life, it is thus up to the legislator to intervene at the present time"[208]. Their demands were addressed by the Law of 17 July 1970.[209]

B. Legislative Recognition

In 1970 the legislator finally recognized the right to respect of private life as an independent right by adding new provisions in the civil and criminal codes.

B.1. Civil Code

In 1970, after years of debate around the suitability to legislate on the right to respect of private life and sanction what courts had been doing for the last century, Article 9 was introduced in the Civil Code.[210] It states that:

> Everyone has the right to respect for his private life.
> Judges may, without prejudice to reparation for damages suffered, prescribe any measures, such as sequestration, seizures and others, proper for the prevention or cessation of encroachment on the intimacy of private life; such measures may, in case of urgency, be injunctions.[211]

For Article 9 to offer recovery, there must be a « reference or allusion to the life of the person who claims the violation » [212]. The broad way in which the first paragraph of the article is written shows that the legislator did not try to assess every specific situation in which private life could be violated but establishes a general principle and trusts courts to apply it on a case-by-case basis.[213] The judicial body plays an important role in interpreting this 'catch-all' provision and developing the protection of private interests in France. This broad rule has also the advantage of allowing future potential adaptations for "societal evolutions"[214].

The second paragraph of the provision grants power to judges to offer other types of redress, seizure of the publication and emergency interim procedures[215] (something that the Cour de

[207] Robert Badinter, 'Le droit au respect de la vie privée' (1968) J.C.P.I. 2136, para 24.
[208] Ibid, para 44.
[209] Loi n° 70-643 du 17 juillet 1970 tendant à renforcer la garantie des droits individuels des citoyens
[210] By enacting Ibid, art 22.
[211] Translation by John H. Crabb, *The French Civil Code – Revised Edition* (as amended to 1 July 1994) (Fred B. Rothman and Co 1995) 3.
[212] Cass Civ. 2e (22 mai 1996) Bull. n106, 66. « référence ou une allusion à la vie de la personne qui entend se prévaloir de l'atteinte »
[213] Nerson (n 177) 763.
[214] Lepage (n 206) 43.
[215] Nerson (n 177) 759.

cassation desired[216]). The range of measures is wide: escrow, seizure, penalty, elimination of certain passages in a book, destruction of all the copies of a publication…[217] It is worth pointing out that the second paragraph refers to the "intimacy of private life" whereas the first only refers to "private life". This seems to indicate that the legislator invites judges to distinguish the two concepts: private life on one hand, and intimacy- understood in this context as "the most secret part of private life"[218] on the other. Only encroachments of the latter allow the measures described in the second paragraph to be prescribed.

The protection regime under Article 9 for the respect of private life (extended to right to its own image[219]) is autonomous, it does not follow the same rules as civil responsibility. The main advantage of a specific provision consecrating an independent subjective right to respect of private life is that, contrary to the protection granted under Article 1382, a simple violation of this right- if found- triggers liability and redress. There is no more reliance on civil responsibility principles, no requirement of proving the existence of a specific fault causing a specific damage anymore. It therefore offered a more effective and complete protection, as some indiscretions might not be damaging but be nonetheless unwarranted.[220] Private life then becomes the object of protection of an independent personality right, whose value is shown by the fact that the existence of 'damage' does not need to be proven.[221] The insertion of Article 9 in the civil code confirms and validates the judicial use of "right's rhetoric" when assessing cases involving private interests, despite the fact that the legal basis was actually in tort law. [222] As such, the right to respect of private life was proclaimed to be a derivative constitutional principle.[223]

B.2. Criminal Code

The Law of 1970 also added and changed certain articles in the criminal code. For instance, spying has been prohibited by criminal law since 1810.[224] The mere fact of spying is criminalized: the fact of violating the *intimacy of someone's private life* by capturing, recording or transmitting any private or confidential remarks made by him without his consent.[225] It is also criminalized to keep hold, divulge, let be divulged to the public or any third party, or to use in any way, any recording or document obtained by spying.[226]

As new technologies gave the possibility to not only listen to, but also record, conversations held in a private space, the legal framework had to adapt and granted individuals the right to oppose any form of tapping of his speech when in a private place without consent.[227] Once again, the Law of the 17 July 1970 clarified any doubt by enacting a criminal provision on

[216] Cass Civ. (12 juillet 1966) D.S. 1967, 181.
[217] Nerson (n 177) 759.
[218] Kayser, 'Les droits de la personnalité' (n 170) 440.
[219] Cass Civ. 1ere (13 January 1998) n 95-13.694 J.C.P. 1998.
[220] Lepage (n 206) 62.
[221] Courts repeatedly confirmed this: amongst others: Civ. 1ere (25 February 1997) JCP 1997. II. 22873; Civ. 1ere (5 November 1996) JCP 1997 II. 10805.
[222] Hauch (n 172) 1244.
[223] Cour. Const. (23 July 1999) D. 2000 Somm. 265 obs L. Marino, CCE 1999 Somm. 52, obs R Desgorce (1999) RTD Civ.724.
[224] Criminal Code, former art 368.
[225] Criminal Code, art 226-1, 1°.
[226] Criminal Code, art 226-2.
[227] Kayser, 'Les droits de la personnalité' (n 170) 469.

the subject[228]. When first enacted in 1970 the protection only concerned 'speech held in a private place'; but the actual provision changed the scope of the protection and is now targeting 'any private or confidential speech'[229]. This demonstrates that the legislator in 1970 aimed to strengthen the legal protection of private life.

Section 3. Conceptual Approach

In France, the right to respect of private life is intrinsically linked with the notion of individuals. It is now considered a personality rights. In 1966, the Cour de Paris stated that: "the private life of any individual belongs to him, as the extension of his personality".[230] Robert Badinter agreed: "the right to respect of private life is recognized as an essential prerogative of human personality"[231].

This general "orientation" towards individuals can also be shown when looking at the historical development of how private interests were protected through different legal constructs and how a distinct right to private life came to be accepted by courts, scholars and eventually legislators.

In the 19th century, protections of private life were intrinsically linked to the notion of honor. From the Revolution on, legislators had a clear goal of protecting private life from any unwarranted disclosure that might infringe upon honor or reputation. It was considered that every citizen should have the possibility to defend his honor- and for the majority of the 19th century, this honor was linked to the notion that private life should stay confidential.[232] As it has been shown in this chapter, when courts progressively asserted the existence of a right to respect of private life at the end of the 19th century and during the main part of the 20th, they did so mainly under the general umbrella of the Article 1382 of the civil code. One of the first prerogatives courts estimated this 'new' right included was the ability for individuals to oppose any revelation or representation they did not agree to - as illustrated by the Rachel affair in 1858.[233] It slowly emerged as a substantive right to oppose unwarranted disclosure of private life.

In the twentieth century, the legal scholarship seemed to conceptualize the protection of private interests in the same way. The first articles written on the question tend to convey the general idea that by protecting private life, it was actually the *secret* of private life that was the object of protection. For example, in 1959 Martin wrote an article making this point.[234] He wrote: "There is no right to privacy: the right appears only when there is a possibility that it will be revealed to others. In other words, it is the secrecy, not privacy, which can be subject matter of a right"[235]. A couple of years later, Robert Badinter wrote: "The right to respect of private life is an absolute right, applicable to all, which is exercised in a discretionary manner, in

[228] Art 368, 1° - now repealed by Loi n92-1336 of 16 December 1992, art. 372 (V) JORF 23 December 1992.
[229] "paroles prononcées à titre privé ou confidentiel" in Criminal Code, art 226-1, modified by Ordonnance n°2000-916 (19 septembre 2000) art. 3 (V) JORF 22 September 2000.
[230] *Consorts Blier v France Editions et Publications* (Paris, 24 November 1966). Rough translation by the author, the original stating: "le domaine de la vie privée de toute personne physique lui appartient en propre comme le prolongement de sa personnalité".
[231] Badiner (n 207) para 24.
[232] Halperin (n 155) 67.
[233] See *supra*.
[234] Martin (n 203) 227.
[235] Ibid, 239.

the sense that only the right holder is *master of the disclosure of the secrets* of his private life".[236]

The notion of secrecy is the paradigm that underpinned doctrinal work through the 20th century, rather than the issue of freedom of private life.[237] This illustrates how the French privacy regime is orientated towards secrets, and therefore individuals. Legally protecting private interests is done through empowering individuals to decide the conditions under which his secrets (and his own portrait) can be divulged. According to Pierre Kayser:

> the right to secret of correspondence and the right over image are only specific prerogatives of the right of the individual to oppose the disclosure of his private life. The mode/way of disclosure does not matter […] and the way the author learned about the information does not matter either […]. The person whose private life is at stake has the power to oppose any disclosure of it[238].

This terminology of "power to oppose disclosure" refers to what has been identified as the paradigm of control. Historically, it is clear that the individual is conceived as being the center of the conceptual apparatus: he is the master of his honor, image and private facts- he is the one who decide how he should be portrayed in the public space. When French courts talk about the "rights" to reputation, of confidentiality of letters, right over one's image, or public disclosure of private information: they are conceptualizing it as a right of control.[239] A court stated in 2004 that "the right to respect of private life – which consists in a right of control over personal information- allows an individual to oppose revelation of information relating to his private life"[240]. The revelation amounting to a breach of private life can be independent from any preceding interference.[241]

This of course does not mean that French law does not guarantee individuals any protection against interferences. Criminal law clearly forbids interference with private life[242] and the Cour de cassation was clear that any arbitrary interference with someone else private life was illicit.[243] But initially, the need to protect opposition from unwarranted interference as part of a broader protection of private life was not specifically recognised by the scholarship[244] and it is mainly in response to indiscrete revelation and unconsented use of one's image that the legal protection of private life was built on.[245]

Conclusion

[236] Badinter (n 207) para 68.
[237] Lepage (n 206) 96.
[238] Kayser, 'Les droits de la personnalité' (n 170) 468.
[239] Whitman (n 15) 1167.
[240] TGI Nanterre (10 November 2004) Legipresse 2005, I, 32.
[241] Lepage (n 206) 103.
[242] Art 226-1, para 2; 226-4 (domicile).
[243] Civ. 1ere (6 March 1996) n 94-11.273 (Bull. Civ. I, n124, D. 1997 IR7); Civ. 2e (3 June 2004) n 02-19.886, D. 2004. 2069, note J Ravanas and 2005. Pan. 2651, obs L Marino.
[244] Lepage (n 206) 106; J Carbonnier note sous T corr. Grasse (1 February 1952) 712: about misappropriate of one's image, but the reasoning can be applied to private life.
[245] Lepage (n 206) 102.

The United States and France took different approaches in regulating private interests from the 18th century. The historical analysis of the development of privacy laws in the French and American national traditions highlights two paradigms behind the legal discourse around private interests: one that associates the protection with preserving freedom, and another that conceptualizes it as a form of control. These two narratives can be found in the vocabulary used by legal actors when discussing the emergence, the validity and the scope of the right to privacy in their respective frameworks. This terminology reflects deeper conceptual visions of the purpose and the nature of the right to privacy. These differences can be seen not only in the terminology used in the debate around the validity of an independent right to privacy, but also by the types of frameworks that were historically mobilized by courts to protect individuals in the absence of such a distinct right to privacy.

The United States clearly developed its legal protection of privacy with a clear emphasis on freedom and on shielding the individual from unwarranted interference, it is a system that is "interference-orientated". France, on the other hand, has tried to empower its citizens with a right to control how their private lives would be disclosed, or portrayed in the public space. The right to privacy is understood as a right to oppose unwarranted disclosure- because ultimately the individual should be in control. It is "individual-orientated". Furthermore, historically, the 'individual' has been conceived in different ways by the legal community of both countries. In the United Sates, the individual is understood as "master of his own home", while in France he is "the master of his secrets".

These two orientations can be seen by the types of legal constructs used before the recognition of a distinct right to privacy. The United Sates very much focused on limiting interferences by the State and by other private actors: the theory of trespass and the Fourth Amendment were the two pillars of private interests' protection in the 18th and 19th century. This is also how it was interpreted by courts when discussing the legality of a right to privacy, and further on when recognizing it a constitutional status. In a (over)simplified way, the right to privacy in the United States is assimilated to a right to freedom.

In France, defamation laws played a very important role in protecting individuals from unwarranted disclosure of their private lives. This was an essential legal construct to defend people's honour (which was very important to French society) and paved the way to how regulation of private interests would be understood in the future: a way to defend the way one is portrayed in the public space, and the individual having a choice in how this is conducted. The courts followed this paradigm when interpreting the civil regime to ensure the respect of private life. Once recognised by the legislator, there was no debate on the *nature* of the right to privacy: it is a personality right. Private life and personality are understood as inseparable. The right to respect of private life is therefore interlinked with personal expression and individuality.

This link between privacy and individuality is perceived in both domestic jurisdictions, but the United States approaches it by focusing on society's intrusions and limiting their impact, while the French model looks at empowering the individual himself. Of course, no generalization is absolute, and both countries have complex legal systems that mobilize both

paradigms. There is nonetheless no doubt that they have approached the same issue from different points of view, and consequently different conceptual apparatuses.

The goal behind this domestic comparative analysis was to highlight the different approaches these two countries took on the issue of regulating private interests, not their whole privacy regime as such. This chapter only focuses on domestic experiences in regulating privacy in order to clarify international law's understanding of privacy protection. As demonstrated, the different approaches underlined in this chapter are underpinned by different conceptual paradigms and how these paradigms play out at the international level is the subject of the next chapter.

CHAPTER II: The Right to Privacy in International Law

Introduction

The Universal Declaration of Human Rights (UDHR)[1] and the International Covenant on Human Rights (ICCPR)[2] both protected 'privacy' from the outset. If the existence of an 'international human right to privacy' has been clear and unambiguous, agreeing on its exact content revealed itself to be a completely different story. This chapter looks at the provisions relevant to the right to privacy in international instruments protecting the rights of individuals, focusing in particular on the UDHR, the ICCPR and the European Convention on Human Rights (ECHR). The main purpose is to explore whether there is a common, generally accepted conception of the right to privacy in international law. Such a right was explicitly recognized in the major international human rights instruments of the twentieth century, but the question remains as to what the drafters meant by the notion of 'privacy' and how they envisaged the scope of such protection.

The protection granted by the main international human rights instruments, especially the UDHR (which has reached customary status) and the ICCPR (which has 173 States parties), can help hold States accountable for abuses of privacy and therefore be a powerful tool to enhance individuals' enjoyment of their right to privacy. Increasing attention is given on questions of enforcement and applicability of the provisions, in order to respond to novel threats caused by new technologies and new surveillance measures. However, the underlying conceptual assumptions and how they have evolved are not sufficiently interrogated in the scholarship on the right to privacy; an in-depth understanding of these protections is therefore necessary. The application and enforcement of a right, which suffers from conceptual and definitional ambiguities, proves problematic. As such, the lack of understanding of the scope and content of the right to privacy leads to increasing difficulties.[3] Without an advanced understanding of 'privacy' as a concept it is neither possible to clarify the scope of the provisions on the right to privacy, nor to examine whether they can be applied to online surveillance practices that currently challenge, and at times evade, the traditional international legal frameworks and protections.

It is not uncommon that international legal provisions are formulated in general and underspecified terms leading to controversies and ambiguity regarding their scope and interpretation, and therefore the 'broadness' of the provisions on privacy is not unique.[4] However, this general problem seems to be somewhat accentuated in the case of the right to

[1] Universal Declaration of Human Rights (10 December 1948) 217 A (III) UN Doc A/RES/217(III) A. (hereinafter 'UDHR').
[2] International Covenant on Civil and Political Rights (adopted 16 December 1966, entered into force 23 March 1976) 999 UNTS 171 (hereinafter 'ICCPR').
[3] Toby Mendel et. al., 'Global Survey on Internet Privacy and Freedom of Expression' (Unesco Series on Internet Freedom, Unesco Publishing 2012) 51. (hereinafter 'Global Survey on Internet Privacy').
[4] James Michael, *Privacy and Human Rights- An International and Comparative Study, with special reference to developments in information technology* (Darmouth Unesco Publishing 1994) 19.

privacy. As Frank La Rue states: 'As the right to privacy is a qualified right, its interpretation raises challenges with respect to what constitutes the private sphere'.[5]

Against this backdrop, this chapter aims to clarify the discourse on the right to privacy at the international level by examining the extent to which the two privacy paradigms identified in the legal discourse on privacy, through the comparative analysis of the US and French jurisdictions in Chapter I, finds echoes at the level of the international discourse, namely the "interference-orientated" "freedom from interference" paradigm and the "individual-orientated" privacy protection as a form of "control".

To this end, the first part of the chapter focuses on universal international human rights instruments. The drafting history of the UDHR (section 1) and the ICCPR (section 2) is analysed in detail to highlight the drafters' understanding of the protection granted to private interests under these instruments and the relevant provisions. The work of UN Bodies (section 3) is then examined, with the goal to reveal which conception of the right to privacy has been more dominant and influential at UN level. The second part of the chapter then turns to the protection offered by regional treaties. Special attention is given to the European Convention of Human Rights (ECHR) (section 1) and how it developed and interpreted the notion of 'private life' and the scope of the protection offered by Article 8. The case-study of a regional system focuses on the ECHR because it provides a comprehensive protection for human rights which has over the decades consolidated through the caselaw of the European Court of Human Rights (ECtHR) and the Convention practice. Others regional instruments are then considered in section 2.

Part I – Privacy at the Universal Level

A right to privacy is recognized at the international level, among others, by both the UDHR and the ICCPR. Additionally, certain subject-specific instruments such as the United Nations Convention on Migrant Workers[6] and the UN Convention on the Rights of the Child ('CRC')[7] safeguard the right to privacy within their remit. The respective provisions in these instruments, Article 14 of the Migrant Workers Convention and Article 16 of the CRC, have followed the wording of the UDHR and the ICCPR.

The UDHR and the ICCPR, along with the ICESCR, are considered as constituting the International Bill of Rights. Thus, to an extent, the rationale for their adoption and part of their drafting history is shared. The International Bill of Rights was a project undertaken by the Commission on Human Rights under a mandate from the Economic and Social Council ('ECOSOC')[8] to enhance the 'promotion and observance of human rights' but no decision

[5] UNHRC 'Report Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue' (17 April 2013) A/HRC/23/40, para 21. (emphasis added).
[6] (adopted 18 December 1990, entered into force 1 July 2003) 2220 UNTS 3, art 14.
[7] (adopted 20 November 1989, entered into force 2 September 1990) 1577 UNTS 3, art 16. For a commentary see John Tobin/Sarah M Field, 'Article 16' in John Tobin (ed), *The UN Convention on the Rights of the Child: A Commentary* (OUP 2019) 559–99.
[8] ECOSOC Res 9(II) (21 June 1946) UN Doc E/RES/9(II), para 6.

was reached on the nature of such instrument(s).[9] A debate therefore ensued about the binding nature and the level of enforcement that the framework should have.[10] The only point of agreement among the Human Rights Commission members was that one or more international conventions had to be enacted, even if a non-binding declaration was put in place first.[11] As a result, the Commission worked simultaneously on two different instruments: a declaration and an international convention[12]. This part will first discuss the UDHR which preceded the ICCPR and which is commonly considered as having inaugurated a new epoch for the protection of human rights following the Second World War.[13] The drafting history of the Declaration will be discussed and analysed with the aim to discover how it conceptualizes the protection it grants to privacy. The analysis will then turn to the ICCPR as the international convention with potential universal reach.

Section 1. Universal Declaration of Human Rights

The right to privacy is protected under Article 12 of the UDHR, which provides:

> 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 protection of the law against such interference or attacks.

Under this provision, a protection against arbitrary interreference is granted to all individuals' privacy, family, home and correspondence. By enumerating these four 'interests', the provision shows that they are understood to be distinct, but potentially overlapping. As will be discussed in detail, during the drafting of the UDHR it was decided to include the 'umbrella term' of privacy as an interest to be protected on its own and independently from the family life and from the sanctity of home and the confidentiality of correspondence. As it was developed in Chapter I, protection of the home and correspondence is sometimes understood as being part of a more general protection of privacy, but in this instance they are separated.

According to James Michael the wording of the provision makes evident that: "the concept of individual privacy has thus been extended to include the kinship 'zone' of the family"[14]. A literal reading of the text reveals that the protection granted to the individual's family is not conceived as a subset of his or her privacy, but rather as something separate According to Article 31 of the VCLT, which is generally considered as reflecting the customary international rules on the interpretation of international treaties and other instruments,[15] a provision has to be interpreted in good faith according to its text and in light of its object and purpose. Not only the text of the provision of Art 12 makes evident that privacy is protected on top of the protection afforded to an individual's family, home and correspondence, but

[9] Ibid, para 7; see Commission on Human Rights, 2nd Session, Summary Record of the 29th Meeting (8 December 1947) E/CN.4/SR/29, 4.
[10] See for example Commission on Human Rights, 2nd Session, Summary Record of the 28th Meeting (4 December 1947) E/CN.4/SR/28 ('Commission Summary Record 28').
[11] See Drafting Committee on an International Bill of Rights, Report on its 1st Session (1 July 1947) E/CN.4/21, 3.
[12] Commission Summary Record 28 (n 10).
[13] Ed Bates, 'History' in Daniel Moeckli, et al. (eds), *International Human Rights Law* (2dn, OUP 2014) 28.
[14] Michael (n 4) 19.
[15] Vienna Convention on the Law of Treaties (23 May 1969) 1155 UNTS 331, art 31. (hereinafter 'VCLT').

also the object and purpose of the UDHR, an instrument geared towards the protection of the rights of individuals, affirms this conclusion.
'Privacy' and 'family' are abstract concepts and neither the provision nor the UDHR provide a definition of these terms. This can potentially lead to different and arbitrary definitions. On the other hand, 'home' and 'correspondence' are closer to 'physical zones of protection (…) which may go very far from the physical home'[16]. The analysis will now turn to the drafting history of this provision to investigate how its drafters conceptualize the protection they were granting.

A. Drafting History

Taking into consideration that no definition of 'privacy' is included in the Declaration and that the term has no clear meaning, according to Article 32 of the VCLT we need to turn to the drafting history of this instrument in order to uncover what the drafters of the Universal Declaration meant by the word 'privacy'.[17] The preparatory work (or *travaux preparatoires*) are generally accepted as a supplementary means of interpretation of international treaties and other instruments in order to confirm the meaning of a provision resulting from the application of Article 31 of VCLT or when the meaning of a provisions remains (among others) ambiguous even when Article 31 of the VCLT has been applied.[18]

From the very beginning of the negotiations in—already in 1946-48—it became obvious that legal protection would be granted to 'privacy' under the UDHR, in one form or another. The evolution of the provision will be briefly summarized here.

The UDHR drafting process was a complex task and a rather complicated process. It involved different bodies, several rounds of consultations, and numerous changes to the text.[19] The first phase of the project concerned the formulation of a 'preliminary draft'[20]. To assist the Drafting Committee in its task to write the first draft, a working paper entitled 'the Secretariat Outline'[21] was prepared by John P. Humphrey, Director of the United Nations Division of Humans Rights. This Secretariat Outline included, among others, a provision relating to privacy, which reads:

> No one shall be subjected to arbitrary *searches or seizures*, or to *unreasonable interference* with his person, home, family relations, reputation, *privacy*, activities, or personal property. The secrecy of correspondence shall be respected.[22]

---

[16] Michael (n 4) 19.
[17] Article 32 of the VCLT reads:

> Recourse may be had to supplementary means of interpretation, including the preparatory work of the treaty and the circumstances of its conclusion, in order to confirm the meaning resulting from the application of article 31, or when the interpretation according to article 31: a) leaves the meaning ambiguous or obscure; or b) leads to a result which is manifestly absurd or unreasonable.

[18] See, Mark Villiger, 'Article 32' in id (ed), *Commentary on the 1969 Vienna Convention on the Law of Treaties* (Martinus Nijhoff 2009) 442–49 and Oliver Dorr/Kirsten Schmalenbach, 'Article 32' in id (eds), *Vienna Convention on the Law of Treaties: A Commentary* (Springer 2012) 571–86.
[19] Timetable of the codification See Cf. ECOSOC Res 46(IV) (28 March 1947) E/RES/46(IV) 32.
[20] The Drafting Committee wrote a first draft that was then submitted to the Commission on Human Rights, amended by a working group, submitted again to ECOSCO and Member States to revise.
[21] Drafting Committee on an International Bill of Human Rights, Report on its First Session (1 July 1947) E/CN/4/21, Annex A. (hereinafter 'Secretariat Outline').
[22] Article 11 in Secretariat Outline: Drafting Committee on an International Bill of Human Rights, Report on its First Session, 1 July 1947, E/CN/4/21, Annex A. ('Drafting Commission Report 21') (emphasis added).

The terms 'search and seizures' used in this provision hinges to an influence of the US Constitution and its 4th Amendment.[23]

The Drafting Committee used the Secretariat Outline as a departure point for its proposition of Articles of an International Declaration of Human Rights.[24] René Cassin- the Committee member in charge- changed substantially the provision relating to privacy in the two drafts he presented[25].

The first draft of the provision was worded as follow:

> Private life, the home, correspondence and reputation are inviolable and protected by law.[26]

The notion of 'private life' replaced 'privacy' and the 'personal property' aspect was dropped. The second draft changed course and stated:

> The privacy of the home, and of correspondence and respect for reputation shall be protected by the law.[27]

Here, not only the notion of privacy was reintroduced, but only a "sectorial privacy": privacy of the home and of correspondence. No explanation can be found for this substantial change. In July 1947, this second draft was submitted to the Commission on Human Rights.

The Working Group on the Declaration of Human Rights started working on a new draft, on the basis of Cassin's revised draft and a proposal made by Panama.[28] Once again, the provision relating to private interests was completely redrafted:

> Every one shall be entitled to protection under law from *unreasonable interference* with his reputation, his *privacy* and his family. His home and correspondence shall be inviolable.[29]

As evident from the text of the provision, the Working Group seemed to move away from the approach of the revised Cassin draft, which protected only specific private interests. 'Privacy' as a general term was reintroduced, in a list of other concepts worth protecting- such as reputation and family. The concept of "unreasonable interference" is also reinstated. The Article is written in a way that seems to indicate a (clearer) distinction between the protection of the law from interference with privacy on the one hand and the inviolability of the home and correspondence on the other. However, no explanation or details can be found in the records to affirm this conclusion.

---

[23] See first part of Chapter I of this thesis.

[24] Drafting Commission Report 21 (n 22).

[25] Oliver Diggleman/Maria Nicole Cleis, 'How the Right to Privacy Became a Human Right' (2014) 4 Human Rights Law Review 441, 445.

[26] Article 9 in Drafting Committee on an International Bill of Human Rights, Report on its First Session (1 July 1947) E/CN/4/21, Annex D. (hereinafter 'Casin Draft').

[27] Article 12 in Drafting Committee on an International Bill of Human Rights, Report on its First Session (1 July 1947) E/CN/4/21, Annex F (hereinafter 'Revised Casin Draft').

[28] Statement of Essential Human Rights presented by the Delegation of Panama (26 April 1946) E/HR.3. 24 countries participated to the elaboration of this proposal (also called 'Declaration of Philadelphia')under the banner of the American Law Institute and submitted it to the UN in 1946: see Working Group on the Declaration on Human Rights, Report to the Commission on Human Rights (10 December 1947) E/CN.4/57 (hereinafter 'Working Group Report 57') 3.

[29] Article 12, Ibid, 8. (emphasis added).

This draft was submitted by the Commission on Human Rights to the ECOSOC at the end of 1947,[30] while Member States were asked for their input in the beginning of 1948. Once the Member States submitted their comments back to the Drafting Committee, the latter decided to revise its first draft and – surprisingly- decided to remove any mention of 'privacy' or 'private life'. The article was formulated this way:

> Everyone is entitled to protection under the law from unreasonable interference with his reputation, family, home or correspondence.[31]

No justification was given for such a drastic change.[32] It is possible that the Committee members thought that they were not making a big substantive change; the Australian delegate even called the texts 'very similar'.[33] An issue, however, that was the subject of debate in the Committee was whether the safeguard should have been framed as 'protection from interference' or as a 'freedom from interference'. The difference between the two phrasings was that 'protection from interference' implied more responsibilities on States than only respecting a freedom from interference.[34]

This Revised Draft from the Drafting Committee was submitted to the Commission on Human Rights, which decided to again substantially change the text of the provisions. The new text read:

> No one shall be subjected to *unreasonable interference* with his *privacy*, family, home, correspondence or reputation.[35]

In this version, the notion of 'privacy' was reintroduced. As with the previous changes of the text, the Committee gave no explanation nor did it debate the change and the reasons behind the re-introduction of the term. The records only show that different variations of the text were discussed and that it is the Chinese one that was eventually adopted.[36] Looking at the rationale of the Chinese proposal itself it is not clear why they decided to reintroduce the word 'privacy'.[37]

The draft of the Commission on Human Rights was subsequently submitted to the ECOSOC, which did not make any changes,[38] and was subsequently passed on to the General Assembly. Some changes were made to provision relating to privacy, but not in a substantial way. The final text read:

---

[30] Commission on Human Rights, Report on its 2nd Session (17 December 1947) E/600.
[31] Article 9 in Drafting Committee on an International Bill of Human Rights, Report on its 2nd session (21 May 1948) E/CN.4/95, Annex A, 7 (hereinafter 'Drafting Commission Report 95')
[32] For the Drafting Committees discussion of Article 9 of the Revised Draft, See Drafting Committee on an International Bill of Human Rights, 2nd Session, Summary Record of the 36th Meeting (17 May 1948) E/CN.4/AC.1/SR.36, 5-7 (hereinafter 'Drafting Committee Summary Record 36').
[33] Ibid, 6.
[34] Digglemann/Cleis (n 25) 447.
[35] Commission on Human Rights, Report on its 3rd Session (28 June 1948) E/800 at Annex A, art 10. (emphasis added).
[36] Commission on Human Rights, 3rd Session, Summary Record of the 55th Meeting (15 June 1948) E/CN.4/SR.55, 2-3.
[37] Ibid.
[38] ECOSOC Res 151(VII) (26 August 1948) E/RES/151(VII).

> 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 attack.[39]

The provision was adopted by the General Assembly as Article 12 of the UDHR on 10 December 1948.[40] The word 'privacy' was finally included in the text, as an 'umbrella term'.[41] The reasons for this inclusion, however, are not clear as the drafting history (or rather, as explained above, the lack thereof) indicates. The next section will analyse the conceptual consequences that such a complicated drafting history has on the overall understanding of the scope and nature of the right to privacy established by Article 12.

B. Analysis

As shown in the previous section, the drafting history of Article 12 of the UDHR does not reveal much about the drafters' understanding of the concept of 'privacy' or about the reasons they decided to include the term in the final text of the provision. At the various stages of the drafting of the Declaration, no explanation or justification was given for the different changes to the provision. This was even the case when modifications were drastic, such as when the concept pf 'privacy' was removed from the text altogether.

Digglemann and Cleis identify three potential explanations concerning the silence of the drafting records on the matter. A first possible explanation is that the different modifications were not considered as fundamental. The members could have understood such modifications as mere editorial changes, and therefore as not changing substantially the nature and scope of the protection.[42] A second possible explanation relates to the multi-linguistic context in which the drafting process took place.[43] The different members were working in different languages, and confusion might have arisen from imprecise translation. René Cassin, for example, was working in French. In his case, the use of the term 'private life' might actually have been due to a direct translation rather than a real difference of opinion on the nature of 'privacy' or on the scope of the article. John P. Humphrey recognized this difficulty and mentioned that the translation of Cassin's draft into English led to a text that seemed 'further removed from the original than it really was'[44]. A third explanation is that there was no need to discuss in much detail the content of the provision because there was a general common understanding of the issue at hand, and that the existence of a right to privacy was broadly accepted by the UN Member States at the time. The two first explanations are plausible, and the silence of the records is probably resulting from a mixture of the two. One aspect that is not mentioned however is the fact that, as demonstrated in the previous chapter, different domestic traditions had different experience in regulating privacy.[45] Representatives of different countries were maybe not realizing that

[39] Article 13 Draft Universal Declaration of Human Rights, Report of the Third Committee to the 3rd Session of the General Assembly (7 December 1948) A/777 at 4.
[40] Universal Declaration of Human Rights (10 December 1948) 217 A (III) UN Doc A/RES/217(III) A, 71.
[41] Digglemann/Cleis (n 25) 447.
[42] Ibid, 448.
[43] Ibid, 448.
[44] John P Humphrey, *Human Rights & The United Nations: A Great Adventure* (Dobbs Ferry: Transnational Publishing 1984) 43.
[45] Chapter I of this thesis.

they were conceptualizing differently how to approach the issue of privacy regulation- but that might explain certain differences in wording highlighted *supra*. What might have been considered as editorial change was actually influenced by different domestic understanding of privacy regulation.

The third explanation however seems unlikely. A working paper entitled 'Human Rights Commission Member's Observations'[46] was given to the Drafting Committee alongside the 'Secretariat Outline' to help in the drafting of the Declaration. The document compiled all the different national provisions granting protection to certain private interests in all UN Member States in 1947. Interestingly, not a single national constitution mentioned 'privacy' or 'private life' as a general term at the time. All the protections that existed were formulated as safeguarding 'selective aspects of privacy', and more specifically the 'privacy of the home[47] and/or the correspondence'- and usually framed as protecting their 'inviolability' or 'secrecy'[48]. The only mention of a broader protection of "privacy" as such was found in the 'Statement of Essential Rights' brought by Panama, for its part, guaranteed '*freedom* from unreasonable interference with his person, home, reputation, *privacy*, activities, and property'[49].

It is therefore clear that there was no common acceptance or understanding among Member States of what a general right to privacy entailed at the international level, as such a guarantee did not exist in national constitutions prior to the adoption of the UDHR. It is likely that the Declaration's drafters did not realize the implications implied by each change in wording.[50] If indeed they were not conscious, not just of the different vocabulary they were using in each modification of the provision, but also of the implications such vocabulary could have, it is not surprising that the scope of the Article has proven difficult to understand. The concept of 'privacy' is in itself very complicated- if not impossible- to define precisely. Adding on top of it a lack of awareness to the nuances that it involves, it is obvious that its legal protection at the international level was ambiguous and vague from the very start.

Section 2. International Covenant on Civil and Political Rights

The International Covenant on Civil and Political Rights ('ICCPR') is one of the most important treaties on human rights at the international level. It has a general subject matter and potentially universal reach. One of the objectives of the Covenant was to reinforce the protections of the UDHR in a binding treaty.[51] This section first examines the content of the article protecting privacy in the Covenant (A), then turns to the drafting history (B) and finally an analysis of the meaning of privacy in the ICCPR is offered, in the light of, inter alia, the General Comments of the Human Rights Committee (C).

---

[46] Drafting Committee on an International Bill of Human Rights, Documented Outline (11 June 1947) E/CN.4/AC.1/3/Add.1 ('Drafting Commission Documented Outline').
[47] With very varying conceptions of the home and the legal protection attached to it, in certain South American countries, for example, the level of protection granted varied depending of the time of the day.
[48] Johannes Morsink, *The Universal Declaration of Human Rights- Origins, Drafting and Intent* (University of Pennsylvania Press, 1999) 136.
[49] Statement of Essential Human Rights presented by the Delegation of Panama (26 April 1946, E/HR/3) (emphasis added).
[50] Digglemann/Cleis (n 25) 449.
[51] Michael (n 4) 19.

Article 17, the provision protecting private interests in the ICCPR, reads:

> 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.

This Article is deemed to be the most important legally binding provision on the protection of 'privacy' at the international level.[52] Despite the Article having been adopted seventeen years after the Universal Declaration, its wording is almost identical to Article 12 of the UDHR. The only difference is that the provision not only prohibits *arbitrary* interferences with the enumerated interests, but also *unlawful* ones.

A. Drafting History

At first glance, one might think that the drafters of the ICCPR simply transposed Article 12 of the UDHR to the text of the Covenant. This might not be completely untrue, but it is still a very simplistic view on the whole process. The analysis of the main drafting stages can still be revealing concerning the prevailing understanding of the scope of protection at the time.

Even before the adoption of the UDHR, during the process of creating an 'International Bill of Rights', a 'British Draft International Bill of Rights' was drawn up and submitted to the Drafting Committee by Lord Dukeston, the United Kingdom representative on the Commission on Human Rights.[53] This document did not protect any private interests;[54] not even some form of privacy of the home and correspondence (which, as discussed above, was at the time commonly accepted at both the national and international levels[55]). However, this British Draft was supplemented by a Draft Resolution[56] which was to be adopted by the General Assembly simultaneously with the Bill of Rights. The Resolution mentioned 'the sanctity of the home' and 'the privacy of correspondence' as being worthy of legal protection[57] Still, because the British Draft never mentioned any general term of 'privacy' or 'private life' as interests to be protected, the ICCPR's first draft written by the Drafting Committee did not grant any form of protection to any private interests.[58] In May 1948, the Australian delegation suggested for the first time a provision protecting privacy[59] but was

---

[52] UNHRC, 'Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Martin Scheinin' (28 December 2009) UN Doc A/HRC/13/37, 11.
[53] Digglemann/Cleis (n 25) 450.
[54] Drafting Committee on an International Bill of Human Rights, Report on its 1st Session (1 July 1947) E/CN/4/21, 29-40. (hereinafter 'Drafting Commission Report 21')
[55] See Drafting Commission Documented Outline (n 46).
[56] Drafting Commission Report 21 (n 54).
[57] Ibid, 27.
[58] Ibid, paras 14 and 18. For the 'Draft Articles on Human Rights and Fundamental Freedoms to be Considered for Inclusion in a Convention' see ibid. at Annex G, paras 82-86.
[59] Article 9 see Australia: Draft of Additional Articles for the Draft International Covenant on Human Rights, 6 May 1948, E/CN/4/AC.1/21 ('Australian Proposal') at 1; and Drafting Committee on an International Bill of Human Rights, 2nd Session, Summary Record of the 29th Meeting (20 May 1948) E/CN.4/AC.1/SR.29 at 9.

never accepted. Two years later, the Philippines proposed a provision directly influenced by Article 12 of the UDHR[60] but the debate around the provision was intensified due to more controversial matters.[61] The adoption of the UDHR in 1948 had an impact on the ICCPR negotiation/drafting process, and it seems to have had a positive influence towards an 'overall inclination' to include a provision protecting private interests in the Conference.[62] Still, it is only in 1953 that the Philippines' proposal was incorporated in the ICCPR's draft as Article 17.[63]

The Third Committee of the General Assembly discussed draft Article 17, as suggested by the Philippines, in 1960 and did not modify it. The provision was eventually adopted by the General Assembly in Resolution 2200A (XXI) on the 16th December 1966. No major debate took place concerning Article 17 because, in the words of the UN Secretary-General, there were 'no differences of opinion… as to the principle involved'.[64] Additionally, it was deemed that 'privacy, the sanctity of the home, the secrecy of correspondence and the honour and reputation of persons were protected under the constitution or laws of most, if not all, countries'.[65]

As discussed in the previous section concerning the UDHR, at least in the beginning of the drafting process, this statement does not seem to have been true.[66] Although, a lot of the national constitutions compiled in the Documented Outline[67] protected certain specific private interests such as the 'inviolability' (and not the 'privacy') of the home and the 'secrecy' of correspondence, not a single one granted a general protection to 'privacy' or 'private life'.[68] The very few times that the concept of 'privacy' was itself mentioned, it was always in relation to the sectorial protection of one specific private aspect, namely the privacy of correspondence.[69]
The debate in the Commission on Human Rights focused on specific questions about how to word the Article, such as the addition of the adjective 'unlawful'. An uncertainty existed among the members of the drafting committee concerning whether it would be appropriate

[60] Commission on Human Rights, Report on its 6th Session (29 May 1950) E/CN.4/507; Commission on Human Rights, Comments on Governments on the Draft International Covenant on Human Rights and Measures of Implementation (16 January 1950) E/CN.4/353/Add.3 at 10; cf. Commission on Human Rights, Observations of Governments of Member States on the Draft International Covenant on Human Rights, 26 February 1951, E.CN.4/515/Add.6.
[61] Such as economical and social rights: Commission on Human Rights, Report on its 6th Session (29 May 1950) E/CN.4/507, 6.
[62] Digglemann/Cleis (n 25) 450.
[63] Commission on Human Rights, Report on its 9th Session, 6 June 1953, E/CN.4/689, para 71. (hereinafter 'Commission Report 689')
[64] Annotations of the Secretary General on the ICCPR draft and in the Report of the Commission on Human Rights on its ninth session: Commission on Human Rights, Report on its 9th Session (6 June 1953) E/CN.4/689, para 67.
[65] Commission Report 689 (n 63) para 67.
[66] Digglemann/Cleis (n 25) 451.
[67] Drafting Commission Documented Outline (n 46) 78.
[68] See above.
[69] More precisely, only seven countries protected the '*privacy* of correspondence/letters/communications': Constitution of Belgium Article 22 (p 79), Royal Rescript No. 42 Egypt Article 11 (p 83), Constitution of Ethiopia Article 26 (p 84), Constitution of Luxembourg Article 28 (p 88), Constitution of the Philippines Article 3 Section 1 (5) (p 90), Constitution of the Union of Soviet Socialist Republics Article 128 (p 94), Constitution of Yugoslavia Article 30 (p 94) in Drafting Commission Documented Outline (n 46).

to transpose the general principle of Article 12 of the UDHR into treaty law, [70] which would imply precise legal terms, applicable in all the different legal systems[71]. Nonetheless, the Commission on Human Rights insisted on the necessity to provide a general rule protecting private interests despite these doubts.[72] The only concern raised was that the precise legal consequences and the scope of the terms 'privacy, home and correspondence' were unclear.[73] The Third Committee of the General Assembly deliberated[74] and then adopted the final version.

Paragraph 2 of Article 17 of the ICCPR provides that: 'Everyone has the right to the protection of the law against such interference or attacks'. The necessity to add this additional sentence to the Article was debated[75] and in the end was recognized as 'not superfluous'.[76]

Analysing the codification process of the ICCPR leads us to roughly the same conclusion than the UDHR's. There was no major debate about the term 'privacy', or what was understood by it and the scope of the protection attached to it.

B. Analysis of the ICCPR regime on privacy

The Article 17 of the ICCPR grants individuals a right to individual to not be subjected to interference with his privacy, and this right should be guaranteed against all interferences whether they emanate from State authorities or natural or legal persons.[77] Under this provision, States are required to adopt legislative and other measures to give effect to this protection and to the prohibition of such interferences[78]. This is the protection granted at first sight on a textual basis, but the Human Rights Committee has interpreted the scope of the protection further.

The Human Rights Committee is the body of independent experts tasked with monitoring and supervising the implementation of the ICCPR.[79] On top of receiving Members States' reports on the implementation of their obligations under the Covenant,[80] it can also receive

---

[70] UN Secretary-General, Annotations on the Text of the Draft International Covenants on Human Rights (1 July 1955) A/2929, para 99.

[71] (once transposed into domestic legal orders for the dualist systems)

[72] Annotations on the Text of the Draft International Covenants on Human Rights (n 70) para 99: "Against this view, it was argued that the covenant would suffer a serious omission if it failed to include an article on such an elementary right as the right to privacy, home, correspondence, honour and reputation". It was decided that a general rule should be provided by the Covenant, letting a certain room of manoeuvre for potential exceptions to Member States. Ibid.

[73] Ibid, para 102.

[74] Third Commission Report to the 15th Session of the GA (8 December 1960) A/4625 at para 37 (reproduced in Bossuyt, *Guide to the Travaux Préparatoires of the International Covenant on Civil and Political Rights* (Martinus Nijhoff Publishers 1987) 343).

[75] Annotations on the Text of the Draft International Covenants on Human Rights (n 70) para 104. Especially considering the fact that Article 2 of the draft covenant already stipulated that each State party should make sure to 'take the necessary steps […] to adopt such legislative or other measures as may be necessary to give effect to the rights recognized in this Covenant'.

[76] Ibid.

[77] UNHRC, 'General Comment No. 16: Article 17 (Right to Privacy): The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation' (8 April 1988) UN Doc HRI/GEN/1/Rev.9, 1.

[78] Ibid.

[79] ICCPR (n 2) art 28. For the four functions of the Human Rights Committee in monitoring the ICCPR see Sarah Joseph/Melissa Castan, *The International Covenant on Civil and Political Rights: Cases, Materials and Commentary* (3rd edn, OUP 2013) 15.

[80] Article 40.

individual's communications from victims of violations if the State concerned has acceded to the Optional Protocol.[81] In this latter function, the Human Rights Committee does not act as a judicial body, but as stressed in General Comment No 33:

> the views issued by the Committee under the Optional Protocol exhibit some important characteristics of a judicial decision. They are arrived at in a judicial spirit, including the impartiality and independence of the Committee members, the considered interpretation of the language of the Covenant, and the determinative character of the decisions.[82]

According to the Committee, its views 'represent an authoritative determination' regarding the interpretation of the ICCPR.[83] Additionally, under Article 40(4) the Human Rights Committee has the competence to adopt General Comments on specific themes or articles of the Covenant.[84] The General Comments are not themselves legally binding but as they are issued by the competent treaty monitoring body, they should be given 'great weight' with regard to the interpretation of the Covenant.[85] The Human Rights Committee examined specifically Article 17 of the ICCPR and the right to privacy in its General Comment No. 16.[86]

General Comment No. 16 does not itself provide much detail on what should be understood by the term 'privacy' in Article 17. It only mentions that:

> As all persons live in society, the protection of privacy is necessarily relative. However, the competent public authorities should only be able to call for such information relating to an individual's private life the knowledge of which is essential in the interests of society as understood under the Covenant.[87]

It adds:

> States parties are under a duty themselves not to engage in interferences inconsistent with article 17 of the Covenant and to provide the legislative framework prohibiting such acts by natural or legal persons'.[88]

It otherwise focuses on defining the terms 'unlawful'[89] and 'family'[90], and on unpacking the notion of 'arbitrary interference'[91] and the conditions in which an interference with the right to privacy could still conform to the Covenant.[92] The Comment also addresses the issue of

---

[81] Optional Protocol to the International Covenant on Civil and Political Rights (adopted on 16 December 1966, entered into force on 23 March 1976) 999 UNTS 302 (OP-1).
[82] UNHRC, 'General Comment No 33: The Obligations of States Parties under the Optional Protocol to the International Covenant on Civil and Political Rights' (5 November 2008) UN Doc CCPR/C/GC/33, at 2, para 11.
[83] Ibid, 3, para 13.
[84] ICCPR (n 2) art 40.
[85] *Ahmadou Sadio Diallo* (Republic of Guinea v DRC) [Merits] 2010 ICJ Rep 663–64 [66]; also Nisuke Ando, 'General Comments/Recommendations' in Max Planck Encyclopedia of Public International Law, <opil.ouplaw.com> accessed 11 September 2019, MN 41; Helen Keller/Leena Grover, 'General Comments of the Human Rights Committee and their Legitimacy' in Helen Keller/Geir Ulfstein (eds), *Human Right Treaty Bodies: Law and Legitimacy* (CUP 2012) 116, at 129.
[86] General Comment No 16 (n 77).
[87] Ibid, 7.
[88] Ibid, 9.
[89] Ibid, 3.
[90] Ibid, 5.
[91] Ibid, 4.
[92] Ibid, 8: "Relevant legislation must specify in detail the precise circumstances in which the interferences may be permitted. A decision to make use of such of such authorized interference must be made only by the

confidentiality of correspondence and surveillance,[93] as well as the gathering and holding of personal information.[94]

The General Comment No. 16 was enacted in 1988, at a time when the consequences of new technologies on the enjoyment of the right to privacy were hardly realised.[95] The Human Rights Committee has been called by NGOs and other stakeholders to issue a new General Comment on Article 17, which would take into account the new technological means used by States and (powerful) non-state actors and replace the current Comment, which is considered as too succinct and as not 'reflect[ing] the bulk of the Committee's practice that has emerged during the more than 20 years since its adoption'.[96]

The Comment remains 'superficial' in its analysis of the right to privacy. It does not question the theoretical (and more abstract) subject of 'privacy' as a concept and as the object guaranteed by the Article 17 of the ICCPR. It is therefore still complicated to assess how the protection granted by this provision is conceptualized. The following section analyses positions taken by different UN bodies on the question of privacy regulation in order to further clarify the scope and conceptual nature of the well-established, but amorphous, international right to privacy.

Section 3. UN Bodies

Outside the context of the UDHR and the ICCPR, discussions on the right to privacy are relatively recent at UN level. The General Assembly, the Human Rights Council[97] (and its Special Rapporteurs) and the Office of the High Commission for Human Rights have all looked at this issue. This section examines the main documents by various UN organs and agencies on the protection of private interests. It will not discuss every such document in detail but will rather focus on sections that could help illuminate the conception of privacy and the scope of the protection advanced at the international level by international bodies. Most of these documents address primarily either the facts behind surveillance practices or offer their own interpretations of the specific limitations to the right provided for in Article 17 of the ICCPR, such as the notions of 'prescribed by law', 'legitimate aim', 'proportionality', 'necessity'[98]. They also usually limit themselves to repeat almost word for word the provisions of Article 12 of UDHR and Article 17 of the ICCPR and to reaffirm their importance.[99] In some cases, however, they do describe the concept of privacy and

---

authority designated under the law, and on a case-by-case basis" (similar approach than the ECHR system of clear legal basis and legitimate aim- more on this *infra*). This will be more detailed in Chapter V of this thesis.

[93] Ibid, 8: "Correspondence should be delivered to the addressee without interception and without being opened or otherwise read. Surveillance, whether electronic or otherwise, interceptions of telephonic, telegraphic and other forms of communication, wire-tapping and recording of conversations, should be prohibited".

[94] Ibid, 10: "The gathering and holding of personal information on computers, data banks and other devices, whether by public authorities or private individuals or bodies, must be regulated by law".

[95] La Rue (n 5) para 25.

[96] (Now 30 years) in Scheinin (n 52) para 19. See also Chapter V of this thesis.

[97] Which replaced the Human Rights Commission: UNGA Res 60/251 (15 March 2006) UN Doc A/RES/60/251.

[98] These criteria will be developed in more detail in the Chapter V of this thesis.

[99] UNGA Res 68/167, 'The Right to privacy in the Digital Age' (18 December 2013) UN Doc A/RES/68/167, 1; UNGA Res 69/166, 'The Right to privacy in the Digital Age' (18 December 2014) UN

their understanding of the right to privacy and this is what this section will focus on. The year 2015 has been chosen as a 'separation point' because this is when a Special Rapporteur on the Right to Privacy was established to focus explicitly on the right to privacy, illustrating the clearer focus of the international community on the question of privacy protection.

A. Before 2015

In 1968, a resolution was adopted by the UN General Assembly on Human Rights and Scientific and Technological Developments.[100] The resolution requested the Secretary-General to launch a 'study of the problems in connexion with human rights arising from developments in science and technology, in particular […] the right for the privacy of individuals […] in the light of advances in recording and other techniques'.[101] Following this resolution, the Secretary General submitted numerous reports in 1973 and 1974 to the United Nations Human Rights Commission.[102]

In 2009, the Special Rapporteur on counter-terrorism of the time, Martin Scheinin, dedicated a large part of his report to the right to privacy.[103] This report is quite significant because the definitions it provides of the concept of privacy have been subsequently used abundantly by other Special Rapporteurs and UN bodies. According to Scheinin:

> *Privacy* is a fundamental *right* that has been defined as the presumption that individuals should have an *area* of autonomous development, interaction and liberty, a 'private sphere' *with or without interaction* with others and *free from* State intervention and *free from* excessive unsolicited intervention by other uninvited individuals.[104]

By using this definition the Special Rapporteur framed privacy- and therefore the protection attached to it- as an almost spatial conception: a zone individuals can retreat to and be free

Doc A/RES/69/166, 1-2; HR Council, 'Resolution: the right to privacy in the digital age' (23 March 2017) A/HRC/RES/34/7, 2, 4; HR Council, 'The Right to Privacy in the Digital Age' (24 March 2015) A/HRC/28/L.27, 2.

[100] GA Resolution 2450 (XXIII) (19 December 1968) 54.

[101] Ibid, 1.

[102] Report of the Secretary-General, Respect for the Privacy of Individuals and the Integrity and Sovereignty of Nations in the Light of Advances in Recording and Other Techniques, 29 UN ECOSOC 10 n6, UN Doc E/CN.4/1116 (23 January 1973); Id. UN Doc E/CN.4/1116/Add.1 (5 March 1973); Id. UN Doc E/CN.4/1116/Add.2 (19 March 1973); Id. UN Doc E/CN.4/1116/Add.3 (23 February 1973); Id. UN Doc E/CN.4/1116/Add.4 (8 January 1974); Report of the Secretary-General, Uses of Electronics which may affect the rights of the Person and the Limits which should be Placed on such Uses in a Democratic Society, 30 UN ECOSOC, UN Doc C/CN.4/1142 (January 1974). – Look details of reports Check report 1975 calling to respect right to privacy and 1976 'possible inclusion in draft international standards concerning respect for the privacy of the individual in the light of modern recording and other device' quoted in Michael (n 4).

[103] Scheinin (n 52).

[104] Ibid, para 11. (emphasis added); Lord Lester/D Pannick (eds) *Human Rights Law and Practice* (Butterworth 2004) para 4.82.

from any unwanted intrusions of both private and public nature. This definition will subsequently be used again several times, in 2013,[105] in 2014[106] and 2018.[107]

The first part of the definition needs also to be highlighted, i.e. that '*[p]rivacy* is a fundamental *right* that has been defined as the presumption that individuals should have…'. There are different elements at play here: one is the concept of privacy in itself, the second is the right to privacy. The two elements are here entangled: the concept of privacy is defined as a right ('privacy is a fundamental right'). The definition seems to confuse privacy as a concept in itself and the right to privacy, which is a legal construction in place to protect aspects of 'privacy'. A distinction must be drawn between 'privacy' and 'the right to privacy'; between the object of protection and protection itself. For example, no one would define 'life' as a right. Rather, one might define 'life' as 'the condition that distinguishes animals and plants for inorganic matter' or 'the existence of a human being or animal'. A *right* to life is then recognized in most domestic legal systems. The same is true about 'privacy' and the right attached to it.

The use of the word 'presumption' is therefore interesting as it is used to describe a right… A right is or is not; it grants legal prerogatives or it doesn't. A presumption (that individuals should have an area of autonomous development) can be a reason why a legal protection should be granted, but it is not the legal protection itself. Unless the presumption is the definition of 'privacy'? The confusion of the report on these matters is clear. This might be simple linguistic mistakes, but they are actually very illustrative of the conceptual confusion surrounding the concept of privacy in itself, which carries on its regulation.

The Special Rapporteur also details two dimensions of the right to privacy found in the various international instruments:

> The right to privacy has evolved along two different paths. Universal human rights instruments have focused on the *negative* dimension of the right to privacy, prohibiting any arbitrary *interference* with a person's privacy, family, home or correspondence[108], while some regional and domestic instruments have also included a *positive* dimension: everyone has the *right to respect* for his/her private and family life; his/her home and correspondence[109], or the right to have his/her dignity, personal integrity or good reputation recognized and respected.[110]

[105] La Rue (n 5) para 22.
[106] Almost identical in: UNGA, 'Promotion and protection of human rights and fundamental freedoms while countering terrorism: Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Ben Emmerson' (23 September 2014) UN Doc A/69/397, para 28: "Privacy can be defined as the presumption that individuals should have an area of personal autonomous development, interaction and liberty free from State intervention and excessive unsolicited intrusion by other uninvited individuals".
[107] UNHRC, 'The Right to Privacy in the Digital Age: Report of the Office of the United Nations High Commissioner for Human Rights' (3 August 2018) UN Doc A/HRC/39/29, 5.
[108] UDHR (n 1) art 12; ICCPR (n 2) art 17; International Convention Protection Migrant Workers (adopted 18 December 1990, entered into force 1 July 2003) 2220 UNTS 3, art 14; Convention Rights of the Child (adopted 20 November 1989, entered into force 2 September 1990) 1577 UNTS 3, art 16.
[109] ECHR (n 1) art 8, Cairo Declaration on Human Rights in Islam (A/45/421-S/21797) art 188.
[110] Scheinin (n 52) para 11. (emphasis added). African Charter on Human and People's Rights, art 11; African Union's Declaration of Principles on Freedom of Expression in Africa, art 4(3); American Declaration of the Rights and Duties of Men art 5.

After recognizing that the right to privacy is valued in nearly all national jurisdictions under a form or another,[111] the universal and fundamental character of the right to privacy is reminded.[112] According to Special Rapporteur Scheinin protection needs to be granted because '[p]rivacy is necessary to create *zones* to allow individuals and groups to be able to think and develop ideas and relationships. Other rights such as freedom of expression, association, and movement all require privacy to be able to develop effectively'.[113] We find, once again here, the idea of a 'zone', of a certain space necessary for individuals to be able to grow as human beings; their own personality and their relationship with others. This perception can be found in scholarship and is related to the conception of privacy as 'autonomy', enabling 'human dignity'.[114]

In 2013, Frank La Rue, Special Rapporteur to Freedom of Opinion and Expression acknowledged the ambiguous character of the concept of privacy; and the consequences of this unclarity in the concrete application and enforcement of the right attached to it:

> Despite the widespread recognition of the obligation to protect privacy, the *specific content of this right was not fully developed by international human right protection mechanisms at the time of its inclusion in the above-mentioned human rights instruments.* The lack of explicit articulation of the content of this right has contributed to difficulties in its application and enforcement. As the right to privacy is a qualified right, its interpretation raises challenges with respect to what constitutes the private sphere and in establishing notions of what constitutes public interest.[115]

La Rue defined privacy the same way as Scheinin had done four years before him:

> [A] fundamental right that has been defined as the presumption that individuals should have an *area* of autonomous development, interaction and liberty, a 'private sphere' *with or without interaction* with others and *free from* State intervention and free from excessive unsolicited intervention by other uninvited individuals.[116]

Although this sentence is rather conventional, he then interestingly continues: 'The right to privacy is *also* the *ability* of individuals to *determine* who holds information about them and how is that information used'.[117] This is something worth pointing out because it illustrates two conceptions of the right to privacy that were highlighted in Chapter I. The first part of

[111] Scheinin (n 52) para 11: "While privacy is not always directly mentioned as a separate right in constitutions, nearly all States recognize its value as a matter of constitutional significance. In some countries, the right to privacy emerges by extension of the common law of breach of confidence, the right to liberty, freedom of expression or due process. In other countries, the right to privacy emerges as a religious value."
[112] Ibid, para 11.
[113] Ibid, para 33. (emphasis added).
[114] For more on this, *See* Daniel Solove, *Understanding Privacy* (Harvard University Press 2008).
[115] "The rapid and monumental changes to communications and information technologies experiences in the recent decades have also irreversibly affected our understandings of the boundaries between private and public spheres." in La Rue (n 5) para 21. (emphasis added).
[116] Ibid, para 22 ; Lester/Pannick (n 104) para 4.82.
[117] Ibid, para 22. (emphasis added).

the definition of the right to privacy conceptualises the scope of protection as allowing individuals to have a 'zone' free from any unwanted intrusions, an area 'for him/her' away, protected from any interference. The second part then offers another vision of the right to privacy: a vision of control. A person should have the ability to 'manage' her personal information as she wishes. The critique outlined above concerning this definition of privacy applies equally here. But the confusion is exacerbated by the second part of the definition, which seems to describe a prerogative of the right to privacy: the *ability* to control information.

The vision of control is reaffirmed further later in the report in the context of confidentiality of communications: 'In order for individuals to exercise their right to privacy in communications, they must be *able to ensure* that these remain private, secure and, if they *choose*, anonymous'.[118]. But then, still talking about communications the Special Rapporteur said: 'Privacy of communications infers that individuals are able to exchange information and ideas in a *space* that is *beyond the reach* of other members of society, the private sector and ultimately the State itself.'[119] This is again a vision of 'a zone free from interference'. The Special Rapporteur passes from one paradigm to another, perhaps without realising; in four paragraph he constantly switches between the two visions. It is not here argued that one vision is more valid than the other, or that it is wrong to use both. Rather, the analysis aims to show how both visions are interlaced and sometimes confused in conversations about the concept of privacy and its legal protection.[120]

In 2014, Ben Emmerson, then Special Rapporteur on counter-terrorism,[121] asserted:

> *The duty to respect* the privacy and security of communications implies that individuals have the right to share information and ideas with one another *without interference* by the State (or a private actor), secure in the knowledge that their communications will reach and be read by the intended recipients alone.[122]

It is interesting that the Special Rapporteur decided here to use the word 'duty to respect', a formulation more common at the regional rather than at the international level. This duty still refers, at first, to the more 'classic' conception of privacy as freedom of interference. However, he then adds: 'The right to privacy also encompasses the right of individuals to know how holds information about them and how that information is used'[123]. This conceptualisation of the right resonates with the 'paradigm of control' set out above.

The way the different Special Rapporteur have addressed the subject of privacy and its correlated right is not straightforward. They seem to mobilize the two paradigms set out in the first chapter of this thesis: one conceptualizing privacy as a zone, worthy of legal protection to avoid unwarranted intrusions; and another looking at empowering individuals in their choices to decide how to manage aspects of their private life. In 2015, two years after

[118] Ibid, para 23. (emphasis added).
[119] Ibid, para 23. (emphasis added).
[120] See Chapter I of this thesis.
[121] Then Special Rapporteur on counter terrorism.
[122] Emmerson (n 106) para 28. (emphasis added).
[123] Ibid, para 28.

Snowden's revelations, the need to explore these questions and strengthen the international provisions on privacy was more acutely felt and a Special Rapporteur on the right to privacy was appointed.[124]

B. After 2015: a Special Rapporteur on Privacy

From 2015 onwards, the attention of the international community seems to focus more clearly on the right to privacy. At the end of 2014, the UN General Assembly adopted resolution 69/166 on the right to privacy in the digital age,[125] inviting the Human Rights Council to consider establishing a special procedure on the right to privacy.[126] A Special Rapporteur on the right to privacy (SRP) Joseph Cannataci, was subsequently appointed in March 2015.[127] One year later the Special Rapporteur submitted his first report to the Human Rights Council. In the report, he first acknowledged the difficulties arising from the lack of a universally accepted definition of the concept of privacy.[128] In his words:

> The existence and usefulness of this framework (Article 12 UDHR and Article 17 ICCPR) is however seriously handicapped by the lack of universally agreed and accepted definition of privacy. In some cases it may prove to be next to useless if we were to have 193 nations signed up to the principle of protecting privacy if we do not have a clear understanding of what we have agreed to protect.[129]

From the beginning the SRP was very clear that his exclusive focus would be on informational privacy.[130] The report also declares that:

> To understand the *right* better it is necessary to think of it from two perspectives. First, it should be considered what the positive core of the right encompasses. Secondly, the question arises how to delimit the right in the form of a negative definition. It would appear we are some distance from having completed these two tasks.[131]

---

[124]UNGA Res 69/166 'Right to privacy in the digital age (18 December 2014) UN Doc A/RES/69/166.
[125] Ibid.
[126] Ibid, para 5.
[127] UNHRC, 'Resolution: The Right to Privacy in the Digital Age' (24 March 2015) UN Doc A/HRC/28/L.27, 4.
[128] UNHRC, 'Report of the Special Rapporteur on the right to privacy, Joseph A Cannataci' (8 March 2016) UN Doc A/HRC/31/64, para 20: "While the concept of privacy is known in all human societies and cultures at all stages of development and throughout all of the known history of humankind it has to be pointed out that there is no binding and universally accepted definition of privacy." (hereinafter 'Cannataci Report March 2016').
[129] Ibid, para 21.
[130] "the function and role of privacy in determining the flows of information in society and the resultant impact of the development of personality of individual citizens as well as almost inextricably related issues such as the distribution of power and wealth within society, and this to the exclusion of subjects such as abortion" in Ibid, para 24.
[131] Ibid, para 20. (emphasis added). The SRP mentions the same approach when it comes to defining the concept of privacy (different the right to privacy): "An improved, more detailed understanding of privacy should be developed by the international community. This understanding should possibly result in some flexibility when it comes to addressing cultural differences at the outer fringes of the right or in privacy-neighbouring rights while clearly identifying a solid and universally valid core of what privacy means in the digital age." And "This global concept of privacy has to pass the test of being positively describable and definable as a precious substantive right on the one hand. On the other hand there also needs to be a negative understanding of the right which hints at legitimate limitations should it be legitimate and necessary to

Entering into the heart of the debate, the SRP writes:

> In order to help focus a fresh, structured debate on fundamentals the SRP intends to provocatively posit *privacy as being an enabling right as opposed to being an end in itself*. Several countries around the world have identified an over-arching fundamental right to dignity and the free, unhindered development of one's personality.[132]

This is an important statement. In a paragraph about 'the debate on the understanding of what privacy is and should be',[133] the SRP seems to move the conversation from the concept of privacy to the advantages of protecting privacy. These are two different issues. The first issue relates to the content and the scope of a concept (privacy) or of a right (right to privacy); the other is about the end goals of legally protecting a specific interest (enhancing individual's dignity and free development of his personality). There is nothing wrong about positing privacy as an enabling right- but one needs to be aware of the distinction[134].

According to the Special Rapporteur:

> This study responds to the crying need identified of achieving a better *understanding of what privacy is or should be* across cultures in 2016 in a way which makes understanding the right more relevant to the digital age where the internet operates without borders. In asking the question 'why privacy?' and positing *privacy as an enabling right as opposed to being an end in itself,* the SRP is pursuing an analysis of privacy as an essential right which enables the achievement of an over-arching fundamental right to the free, unhindered development of one's personality.[135]

As explained *supra*, it seems that there are two different elements in the same paragraph. The first part talks about understanding the scope and content of the concept of privacy ('understanding what privacy is or should be'), but the second sentence (what the SRP proposes) is actually about the purpose and function of the right to privacy ('enabling the fundamental right to free, unhindered development of one's personality'). A suggestion to theorize the right to privacy as an enabling right has its advantages, but it is not the same

---

restrict privacy in a proportionate manner (sic)." in Ibid, Annex III- Further reflections about the understanding of privacy, A.1-2.

[132] Ibid, para 25. (emphasis added). The paragraph continues by stating that: "Countries as geographically far apart as Germany and Brazil have this right written into their constitution and it is the SRP's contention that a) such right to dignity and the free unhindered development of one's personality should be universally applicable and b) that already-recognized rights such as privacy, freedom of expression and freedom of access to information constitute a tripod of enabling rights which are best considered in the context of their usefulness in enabling a human being to develop his or her personally in the freest of manners."

[133] Ibid, para 25.

[134] The SRP explains in more details his position: "Positing privacy and better still, the question '*Why* Privacy' in the context of a wider debate about the fundamental right to dignity and the free, unhindered development of one's personality reflects the realities of life in the digital age and should help all participants in the debate, irrespective of the country or culture they may hail from, to focus on the fundamentals of the development of one's personality and what kind of a life they would like *privacy to help* protect rather than loose too much time on what privacy-relevant traditions in any given culture they would need to focus upon or defend/promote." In Ibid. (emphasis added).

[135] Ibid, para 8. (emphasis added).

thing as 'responding to the need of understanding what privacy is or should be across cultures'.

In August 2016, the SRP submitted a report to the UN General Assembly, in which he wrote:

> Privacy has developed over time, and much evidence has been identified prior to the creation of the Special Rapporteur mandate and the appointment of the incumbent which shows how the understanding of privacy and the exercise of the right has varied across the dimensions of 'Time, Place and Space'. Contrary to what some may think, recognizing this reality does nothing to undermine the existence of the right nor its universality. Instead, it makes *one reflect about the complex set of values that underpin the right and the way that our understanding of the right needs to change as circumstances change in order for the underlying values to continue to be protected* and indeed, as much as possible, have their protection increased.[136]

In 2017, the SRP repeated that he was 'analysing privacy, inter alia, as an essential right, enabling an overarching fundamental right to the free, unhindered development of one's personality'.[137] In February 2018, an expert workshop on the right to privacy in the digital age was organised by the Office of the High Commissioner for Human Rights in Geneva. The SRP participated to the event and presented a paper in which he discussed the dynamic nature of the right to privacy and the challenges raised by surveillance practices. The SRP touched upon the two issues raised in the introduction of this chapter, namely the meaning of 'privacy' in international legal framework and the way to implement international safeguards effectively in practice. When addressing the question of how to understand 'privacy' and the legal framework protecting it, the SRP reaffirmed that '[p]rivacy is a fundamental human right recognized as such under international law. It is also a universal right'.[138] He acknowledged that new contexts might bring new threats, and called for a comprehensive, detailed, legal framework to be put in place:

> Due to its complexity, the right to privacy requires a comprehensive legal framework in order to operationalize it in a number of different contexts. […] Each context brings with it the need of a detailed and constantly up-dated understanding of how privacy could be threatened within that particular context and an identification of safeguards that protect it, and remedies available t citizens which may be specific to that context. The devil, literally, is in the detail, and privacy requires very detailed rules which spell out the level and modes of protection that privacy may be accorded in a particular

[136] UNGA, 'Right to Privacy: Note by the Secretary General transmitting the Report of the Special Rapporteur of the Human Rights Council on the Right to Privacy, Joseph A Cannataci' (30 August 2016) UN Doc A/71/368, para 22. (emphasis added).
[137] UNGA, 'Right to Privacy: Note by the Secretary General transmitting the Report of the Special Rapporteur of the Human Rights Council on the Right to Privacy, Joseph A Cannataci' (19 October 2017) UN Doc A/72/540, para 13.
[138] Joseph Cannataci, 'Paper presented at Expert Workshop on the Right to Privacy in the Digital Age' (Office of the High Commissioner for Human Rights, Geneva, 19-20 February 2018) UN Doc A/HRC/37/62, Annex A, para 1: "(it) should be enjoyed everywhere by everybody, as such it should be respected everywhere by everybody, by States as well as by non-State actors, irrespective of the ethnicity, nationality, gender, religious, philosophical or political beliefs of any given individual or any other status." (hereinafter 'Cannataci Workshop Paper').

> context as well as the remedies that a citizen may resort to if his or her privacy is breached in that context.[139]

He also called for a debate on how to interpret dynamically the notion of privacy and bring it up-to-date to accommodate new developments:

> The importance of this level of detail is even greater in the case of privacy since there exists *no universally accepted definition of privacy*. In other words, people across the world have agreed that the right to privacy exists and that everybody is entitled to such a right but *they have not spelt out precisely what the right is or what it entitles a person to in a wide variety of circumstances.* This fact has both advantages and disadvantages: too narrow a definition of privacy would restrict its ability to be protected as circumstances and privacy-threats change and also as we develop our understanding of what constitutes privacy-infringing behaviour in a number of changing or new contexts[140].

The SRP detailed the shortcomings of the international framework currently in place. He wrote that '[i[nternational law such as art 12 UDHR and art 17 ICCPR only provides an answer to the question "Why" as in "Why should we protect privacy" i.e. because we have agreed that it is a universal fundamental right'. But as demonstrated *supra*, why the drafters of these instruments actually agreed that the right to privacy was fundamental and should be included in these international instruments is not clear.

The report then regrets the absence of answers to other important questions:

> They however do not provide answers to the question: When? Which? What? How? Who? When should privacy be protected? How should privacy be protected? Which are the privacy-relevant safeguards to be created in a particular context? Which new contexts pose the greatest risks to privacy? What should be done to protect privacy in given circumstances? Which are the remedies most appropriate and possible in those cases where, despite all the safeguards provided, a breach of privacy still occurs? Who has special duties and obligations in the case of privacy protection, in which circumstances, what measures are the minimum to discharge these obligations and how should such persons be held accountable?[141]

These questions are important and have been now receiving increasing attention- from States, international organisations and legal scholars alike. But the answer to the first question—'Why should we protect privacy'—is not itself readily apparent. It seems a bit of a shortcut to answer the question 'why?' by 'because it is fundamental'. And why is it fundamental? This 'step further' in the reasoning is not as straightforward at it seems. The 'obvious' fundamental character of the right to privacy can be implied by its presence in several international treaties and in many national systems. However, details to understand

[139] Ibid, para 2.
[140] Ibid, para 2. (emphasis added).
[141] Ibid, para 6.

why it was included in these international instruments in the first place are sparse- especially considering that at the time of codification, national systems did not recognize a legal protection to the umbrella term of 'privacy'.

In August 2018, the OHCHR wrote a report according to which: 'The protection of the right to privacy is not limited to private, secluded *spaces*, such as the home of the person, but *extends* to *public spaces any information* that is publicly available[142] […] The public sharing of information does not render its substance unprotected'.[143] Two elements stand out in this paragraph. The first one is the clear focus on 'information' as the object of protection of the right to privacy. Given that may other definitions focus on the spatial element of privacy regulation (ie. framing the protection as 'zones' or 'areas' that should stay free from interference) it is worth pointing the change in focus and the inclusion of information as an object included in the scope of protection. Second, the fact that sharing publicly an information does not make it lose its protection shows a different approach than the United States' – which uses the criteria of 'expectation of privacy' as a reference point.[144]

To date, the most recent document published at the UN level on the right to privacy is the latest report of the SRP in February 2019. In this report, the SRP links the right to privacy to 'the right of all individuals to their personal autonomy'[145], once again positing the right to privacy as essential to *support* and *ensure* the realization of other values, in this case personal autonomy.

Part II – Regional Level

Section 1. European Convention on Human Rights

The discussion will now turn to the system established under the European Convention on Human Rights, which grants particularly far-reaching and comprehensive protection to private interests. The system put in place by the Council of Europe (CoE) offers strong and effective protection to the private interests of individuals under the jurisdiction of Member States—in fact, more so than in other parts of the world. The protection is not only explicitly provided for in the Convention—its Article 8—but it is also given depth by the Court. The Court has interpreted and applied the provision in numerous cases, 'populating' it with specific content and therefore enhancing the general understanding of the relevant concepts it covers. This allows for the concretisation of a quite broad and abstract provision and as a result the right to privacy under the ECHR is better understood and applied than Article 12 of the UDHR or Article 17 of the ICCPR, whose scope and general conceptualization, as discussed in the first part of this chapter, are not very clear. Taking into consideration the complexity of the CoE human rights system, and the extensive nature of the case-law of the

[142] (See CCPR/C/COL/CO/7 para 32).
[143] UNHRC, 'The right to privacy in the digital age: Report of the United Nations High Commissioner for Human Rights' (3 August 2018) UN Doc A/HRC/39/29, 6. (emphasis added).
[144] It is used as a legal test to determine the applicability of the privacy protection under 4th Amendment: *Katz v. US*: See Chapter I.
[145] UNHRC, 'Right to privacy Report of the Special Rapporteur on the right to privacy' (27 February 2019) UN Doc A/HRC/40/63, paras 7-10.

Court on Article 8, this part of the chapter does not intend to be an extensive study of Article 8 of the ECHR.[146] Rather, it aims to establish the main understanding of the concept of private life and the mode of protection of the right under this instrument.
The European Convention on Human Rights[147] (ECHR) protects 'private life' in its Article 8, which reads:

> 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.

At first sight, there is an obvious difference between Article 8 and other international provisions on the right to privacy, such as Article 12 of the UDHR and Article 17 of the ICCPR, namely that the term 'privacy' is not present in the text of Article 8 but has rather been replaced by the concept of 'private life'. Another major difference is that the first paragraph of Article 8 is not framed in terms of 'protection from interference' but instead as 'a right to respect'. The second paragraph for its part specifies that interference by *public* authorities is prohibited, listing a set of exception criteria. Similarly to Articles 12 of the UDH and 17 of the ICCPR, article 8 also raises the question of what the drafters meant by 'private life' and whether 'private life' is different than the concept of 'privacy' as understood in the context of the UDHR. Once again, the analysis will turn to the drafting history of the Convention as a means of seeking some answers to these questions.

A. Drafting History

The drafting of the ECHR started in August 1949, around six months after the adoption of the UDHR by the General Assembly. The Legal Committee in charge of the ECHR drafting[148] was inspired by three main sources[149]: the UDHR,[150] the recommendations and a draft ECHR prepared by the International Committee of the Movement for European Unity[151] and its International Judicial Section. Article 8 endured many changes before reaching its final form.

---

[146] This kind of study can be found in: Council of Europe, 'Guide on Article 8 of the European Convention on Human Rights- Right to respect for private and family life, home and correspondence' (last updated 31 August 2018) <https://www.echr.coe.int/Documents/Guide_Art_8_ENG.pdf> accessed 18 September 2019. (hereinafter 'Guide on Article 8').
[147] Convention for the Protection of Human Rights and Fundamental Freedoms (adopted 4 November 1950, entered into force 3 September 1953) 213 UNTS 221. (hereinafter 'ECHR').
[148] The Committee of Ministers of the Council of Europe asked the Consultative Assembly to draw 'measures for the fulfilment of the declared aim of the Council of Europe … in regard to the maintenance and further realization of human rights and fundamental freedoms'. In order to do so, the Consultative Assembly created a Committee on Legal and Administrative Questions (hereinafter Legal Committee).
[149] Digglemann/Cleis (n 25) 452.
[150] Explicitly mentioned in the preamble.
[151] The movement was composed of different non-governmental groups that were created during the end of the second World War in order to promote a better European integration.

A first proposition protecting 'privacy' was proposed in August 1949 by Pierre-Henri Teitgen[152], referring explicitly to the UDHR: 'The Convention … will guarantee ... to every person … *inviolability of privacy*, home, correspondence and family, in accordance with Article 12 of the United Nations Declaration'.[153] During negotiations at the Legal Committee, the British Representative Lord Layton argued for the elimination of such a provision, although no explanation can be found in the records for this position. A possible explanation is that he was trying to maintain a certain coherency between the United Kingdom's different positions on the issue, since the same view was adopted during the UDHR drafting process.[154]

This proposition was however rejected by the other members of the Legal Committee and, instead, a new text was submitted by Belgian and French representatives.[155] It stated: '*Immunity* from arbitrary *interference* in his *private life*, his home, his correspondence and his family, as laid down in Article 12 of the Declaration of the United Nations'.[156] The notion of 'interference' appeared, illustrating even more the influence of the UDHR, and the concept of 'private life' was given protection- rather than 'privacy'. Whether this was on purpose or just a consequence of direct translation, no one knows. It is also worthy to point out that this proposition mentions a 'immunity' rather than a 'right'.

The Legal Committee agreed on a Draft Resolution[157], whose Article 2 read: 'In this convention, the Member States shall undertake to ensure to all persons residing within their territories […] (4) freedom from arbitrary interference in private and family life, home and correspondence, in accordance with Article 12 of the United Nations Declaration'.[158] The Consultative Assembly did not discuss this provision and included it to its recommendations to the Committee of Ministers.[159]

The Committee of Ministers subsequently decided to ask the Committee of Experts on Human Rights their opinion. The Expert Committee drew a Preliminary Draft Convention, whose provision on privacy was almost identical to Article 12 of the UDHR save for the mention of honour and reputation.[160] The Committee then provided two alternatives, each one relating to two schools of thought: the first one preferred a method of enumeration, the second one included precise definitions of the different rights and freedoms that were to be safeguarded. Only the latter included a protection of private interests.[161] The responsibility of choosing between the two options fell back on the Committee of Ministers, and the same

[152] Rapporteur of the Legal Committee and from French minister.
[153] Council of Europe, Directorate of Human Rights, *Collected Edition of the 'Travaux Preparatoires' of the European Convention on Human Rights*, vol I (Martinus Nijhoff 1975) 168 (hereinafter 'Travaux Preparatoires ECHR, vol I'). (emphasis added).
[154] Digglemann/Cleis (n 25) 453.
[155] Mr Rolin and Mr Teitgen.
[156] Travaux Preparatoires ECHR, vol I (n 153) 172.
[157] Which it submitted to the Consultative Assembly on the 5th September 1949.
[158] Travaux Preparatoires ECHR, vol I (n 153) 228.
[159] Ibid 216 ss.
[160] "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence. Everyone has the right to protection of the law against such interference." In Council of Europe, Directorate of Human Rights, Collected Edition of the 'Travaux Preparatoires' of the European Convention on Human Rights, vol III (Martinus Nijhoff 1976) 236.
[161] Ibid, 312-335.

pattern as before re-emerged: the United Kingdom favoured the first alternative, justifying the absence of a specific protection for privacy by the fact that provisions on freedom of association and information 'covered the content' of a provision on privacy.[162] The two alternatives were then merged into a New Draft Alternative B, which retained the approach of precise definition, but left a blank space for an 'Article on privacy'.[163] The British representatives proposed to fill this blank with the following provision: 'Everyone shall have the right to freedom from governmental interference with his *privacy*, family, *house* or correspondence.'[164] This way the concept of 'privacy' resurfaced as a general concept to be protected from interference, while notably 'home' was replaced by 'house'.

The tide changed again when the Conference of Senior Officials brought on the table a brand new provision, protecting this time only certain private aspects: 'The right to privacy in respect of family, home and correspondence shall be recognized.' But once again, the provision was abandoned and replaced by: 'Everyone's right to respect for his private and family life, his home and his correspondence shall be recognized.'[165] In this version, the notion of 'private life' is (re) introduced, replacing 'privacy', offering a general protection to private interests. Also, 'freedom from interference' was substituted by 'a right to respect'. Again, no explanation can be found in the travaux preparatoires for these changes. Eventually, the Committee of Ministers finally agreed on this provision, changing it very slightly to reach the final version of the Article as we know it.

In conclusion, similarities between the drafting process of the ECHR and that of the UDHR are clear. Article 8 of the ECHR underwent many changes, from being completely omitted to being framed as a protection from interference and subsequently a right to respect, from protection of 'privacy' to 'private life'. There is no explanation available for the decisions and positions taken. The shift from 'privacy' to 'private life', for example, might be the simple result of a 'direct' translation, with no intent to change the object of protection. Still-the difference exists, and it is worth highlighting that it does not appear to have raised any questions at the time of drafting.

B. European Court of Human Rights

The Court plays an important role in interpreting and concretising the obligations of States under the Convention.[166] This is also true for the scope of the right to privacy under Article 8 of the ECHR, including the concept of 'private life'. The Court is deemed as generally recognizing a wide scope of the right to respect of private life.[167]

[162] Council of Europe, Directorate of Human Rights, *Collected Edition of the 'Travaux Preparatoires' of the European Convention on Human Rights*, vol IV (Martinus Nijhoff, 1977) 110.
[163] Ibid, 182 ss.
[164] Ibid, 202 (emphasis added).
[165] Ibid, 278.
[166] Eva Brems/Janneke Gerards (eds), *Shaping Rights in the ECHR: The Role of the European Court of Human Rights in Determining the Scope of Human Rights* (CUP 2013).
[167] 'Global Survey on Internet Privacy' (n 3) 55.

According to the Court in the case *Niemietz v. Germany* the notion of 'private life' cannot be exhaustively defined under Article 8 of the ECHR,[168] as it is a very broad term.[169] In its own words, 'the Court does not consider it possible or necessary to attempt an exhaustive definition of the notion of 'private life'[170]. While interpreting the notion of private life, the Court distinguished several actions done by States that could amount to a violation of the right to respect the private life of individuals, falling thus under the scope of 'private life': intercepting/surveying communications (private or not) or telephone tapping[171], certain searches and seizures[172], gathering of files or information by States agents[173], refusing access to such information[174],... This enumeration is not exhaustive, but reference is made to these particular aspects here as they are the focus of the present study. Other matters, relating to what has been called in the United States as 'decisional privacy'[175], are also included in the scope of 'private life'.

To provide some guidance and illuminate the content of the right to privacy, the Court issued a 'Guide on Article 8' to 'inform legal practitioners about the fundamental judgments and decisions delivered by the Strasbourg Court'.[176] In addition to being a very useful document gathering all relevant caselaw on Article 8, the way the document is organised is itself noteworthy. It is divided in five parts. First, there is a section on the structure of Article 8. The four other sections are allocated to the four different interests protected under Article 8: 'private life', 'family life', 'home' and 'correspondence'. More importantly, for the purpose of the present thesis, the section on 'private life' divides cases in three main categories: 'physical, psychological or moral integrity', 'privacy' and 'identity and autonomy'. It appears from this document's structure that the Court considers there is a 'core of privacy' issues within the notion of 'private life'. One a side note, the French translation of the document translates the section 'privacy' by 'vie privee'. Thus, in the French document the notion of 'vie privée' is understood as covering the areas of 'integrité physique, psychologique et morale, 'vie privée' (again) and 'identité et autonomie'.

More specifically, the section on 'privacy' includes cases relating to: 'a) right to one's image and photographs; the publishing of photos, images; b) protection of individual reputation, defamation; c) data protection; d) right to access personal information; e) information about

[168] *Niemietz v Germany*, App no 13710/88 (16 December 1992) para 29; *Costello-Roberts v the United Kingdom*, App no 13134/87 (Judgment) (25 March 1993) para 36.
[169] *Peck v United Kindom,* App no 44647/98 (Judgment) (28 January 2003) para 57; *Perry v United Kingdom,* Merits, App no 63737/00 (Judgment) *(*17 July 2003) para 61.
[170] *Niemietz* (n 168) para 29.
[171] For example: *Iordachi and Others v Moldova*, App no 25198/02 (Judgment) (10 February 2009); *Halford v United Kingdom*, App no 20605/92 (Judgment) (25 June 1997) para 44; *Weber and Saravia v Germany,* App 54934/00 (Decision as to Admissibility) (29 June 2006) paras 76-9.
[172] *Funke v France,* App no 10828/84 (Judgment) (25 February 1993) para 48; *McLeod v United Kingdom*, App no 24755/94 (Judgment) (23 September 1998) para 36.
[173] *Rotaru v Romania*, App no 28341/95 (Judgment) (4 May 2000) paras 43-4; *Amann v Switzerland*, App no 27798/95 (Judgment) (16 February 2000) paras 65-7; *Leander v Sweden*, App no 9248/81 (Judgment) (26 March 1987) para 48. (more on this in Chapter V).
[174] *Gaskin v United Kingdom*, App no 1044/83 (Judgement) (7 July 1989); *Niemietz* (n 168).
[175] For example: Interference with sexual life (*Dudgeon v the United Kingdom*, App no 7525/76 (Judgment) (22 October 1981); *Mosley v the United Kingdom*, App no 48009/08 (10 May 2011); compulsory medical treatment: *Acmanne v Belgium*, App no 10435/83 (Admissibility Decision) (10 December 1984).
[176] Prepared by the Directorate of the Jurisconsult, CoE, 'Guide on Article 8 of the European Convention on Human Rights – Right to respect for private and family life, home and correspondence' (last updated on 31st August 2018) <https://www.echr.coe.int/Documents/Guide_Art_8_ENG.pdf> accessed 17 September 2018.

one's health; f) file or data gathering by security services or other organs of the State; g) police surveillance; h) stop and search police powers; i) privacy during detention.'[177] Although the Guide is not binding upon the Court, this official document is in fact unique in its usefulness and practical importance. This document really helps us understand how the Court conceives the protection granted by Article 8 of the ECHR.

In its caselaw, for example in the 2004 *Von Hannover v. Germany* case,[178] the Court has stated that '[t]he concept of private life extends to aspects relating to personal identity, such as a person's name[179] or a person's picture.[180] Furthermore, private life, in the Court's view, includes a person's physical and psychological integrity'.[181] It then added:

> The guarantee afforded by Article 8 of the Convention is primarily intended to ensure the development, without *outside* interference, of the personality of each individual in his relations with other human beings[182]. There is therefore a *zone* of interaction of a person with others, *even in a public context*, which may fall within the scope of 'private life'[183].[184]

This extract is particularly important because the Court uses the metaphor of the 'zone' when it comes to the protection of privacy. This resonates with the treatment discussed above in the context of the reports of Special Rapporteurs Scheinin and La Rue, and more generally to what we have called the paradigm of 'freedom from interference'. The Court stays with the 'traditional' vocabulary of 'zone'- a spatial approach to the concept of private life- but at the same time recognizes that the protection should apply even in a public context. The separation of 'zones' appears therefore blurred, or at least less clearly distinct than the conventional approach of a 'private space of home' vis-à-vis a 'public space of outside'. This position of the Court is in fact not novel: in 1992, in the aforementioned case of *Niemietz v Germany* the Court held:

> [I]t would be too restrictive to limit the notion to an 'inner circle' in which the individual may live his own personal life as he chooses and to exclude therefrom entirely the outside world not encompassed within that circle. Respect for private life must also comprise to a certain degree the right to establish and develop relationships with other human beings.[185]

---

[177] Ibid, 3-4. The category of 'physical, psychological or moral integrity' includes 'victims of violence, reproductive rights, forced medical treatment and compulsory medical procedures, mental illness, health care treatment, end of life issues, disability issues, issues concerning burial, environmental issues, sexual orientation and sexual life, professional or business activities' 3 and the 'Identity and Autonomy' category covers cases relating to "right to personal development and autonomy, right to discover one's origins, religious and philosophical convictions, desired appearance, right to a name/identity documents, gender identity, right to ethnic identity, statelessness, citizenship and residence, marital and parental status." 4.
[178] App no 59320/00 (Judgment) (24 June 2004).
[179] See *Burghartz v Switzerland*, App no 16213/90 (Judgment) (22 February 1994) para 24.
[180] See *Schüssel v Austria*, App no 42409/98 (Judgment) (21 February 2002).
[181] *Von Hannover* (n 178) para 50.
[182] (see, mutatis mutandis, *Niemietz* (n 167) para 29, and *Botta v Italy*, App no 21439/93 (Judgment) (24 February 1998) para 32).
[183] (see, mutatis mutandis*, P.G. and J.H. v the United Kingdom,* App no 44787/98 (Judgment) (25 September 2001) para 56; *Peck* (n 169) para 57).
[184] *Von Hannover* (n 178) para 50. (emphasis added).
[185] *Niemietz* (n 168) para 29.

In the same case, the Court stated that: 'the essential object and purpose of Article 8' is 'to protect the individual against arbitrary interference by the public authorities'.[186]
In the *Axel Springer AG v. Germany* case in 2012 the Court also clearly affirmed that the concept of private life 'covers personal information which individuals can legitimately expect should not be published without their consent',[187] as well as are private data collected and gathered by State's agents[188].

Section 2. Other Regional Instruments

The Council of Europe is not the only regional body in the world that enacted legal safeguards of private interests. Provisions protecting privacy interests can be found in many different instruments: the African Charter on the Rights and Welfare of the Child,[189] the American Convention on Human Rights,[190] the American Declaration of the Rights and Duties of Man,[191] the Arab Charter on Human Rights,[192] the ASEAN Human Rights Declaration,[193] and the Cairo Declaration on Human Rights in Islam.[194] From these instruments, the American Convention on Human Rights and African or Banjul Charter are worth detailing further. The former because its correlated bodies are currently interpreting the provision protecting private life and what it entails, while the latter does not even mention privacy.

According to Article 11 of the American Convention on Human Rights (ACHR):

1. Everyone has the right to have his honor respected and his dignity recognized.
2. No one may be the object of arbitrary or abusive *interference* with his *private life*, his family, his home, or his correspondence, or of unlawful attacks on his honor or reputation.

[186] Ibid, para 31.
[187] *Axel Springer AG v. Germany*, App nos 39954/08 and 39954/08 (Judgment) (7 February 2012) para 83.
[188] *Rotaru* (n 173) para 44.
[189] (adopted 01 July 1990, entered into force 29 November 1999) art 10: "No child shall be subject to arbitrary or unlawful interference with his privacy, family home or correspondence, or to the attacks upon his honour or reputation, provided that parents or legal guardians shall have the right to exercise reasonable supervision over the conduct of their children. The child has the right to the protection of the law against such interference or attacks."
[190] American Convention on Human Rights (adopted 22 November 1969, entered into force 18 July 1978) 1144 UNTS 123, art 11: "1. Everyone has the right to have his honor respected and his dignity recognized. 2. No one may be the object of arbitrary or abusive interference with his private life, his family, his home, or his correspondence, or of unlawful attacks on his honor or reputation. 3. Everyone has the right to the protection of the law against such interference or attacks."
[191] American Declaration of the Rights and Duties of Men (2 May 1948) art 5: "Every person has the right to the protection of the law against abusive attacks upon his honor, his reputation, and his private and family life."
[192] Arab Charter on Human Rights (15 September 1994) art 17: "Privacy shall be inviolable and any infringement thereof shall constitute an offence. This privacy includes private family affairs, the inviolability of the home and the confidentiality of correspondence and other private means of communication".
[193] ASEAN Human Rights Declaration (19 November 2012) art 21: "Every person has the right to be free from arbitrary interference with his or her privacy, family, home or correspondence including personal data, or to attacks upon that person's honour and reputation. Every person has the right to the protection of the law against such interference or attacks."
[194] Cairo Declaration on Human Rights in Islam (5 August 1999) UN Doc A/CONF.157/PC/62/Add.18, (A/45/421-S/21797), art 18: "(b) Everyone shall have the right to privacy in the conduct of his private affairs, in his home, among his family, with regard to his property and his relationships. It is not permitted to spy on him, to place him under surveillance or to besmirch his good name. The State shall protect him from arbitrary interference."

3. Everyone has the right to the protection of the law against such interference or attacks.[195]

The influence of the provisions of the ICCPR and of the ECHR in the text of Article 11 is evident, but the Article differs by stating a right to have one's *dignity* respected as well.
Both the Inter-American Commission on Human Rights (IACommHR) and the Inter-American Court (IACtHR) dealt with some cases concerning issues that fall under the notion of privacy, but they have usually been assessed under the larger 'umbrella' of the right to dignity.

The case-law of the IACtHR dealing directly with privacy issues is a little bit scarce[196]. Still, privacy has been understood by both bodies as a general concept including: searches and seizures of house/documents[197] and 'physical and moral integrity, human dignity, one's reputation in the context of freedom of expression'.[198] Interestingly, in 2012, the Court stated that:

> The scope of protection of the right to a private life has been interpreted in broad terms by the international human rights courts, when stating that it goes far beyond the right to privacy.[199]

The Court relies on the ECtHR case law to list different interests it considers as included in the notion of 'private life':

> According to the European Court of Human Rights, the right to a private life encompasses physical and social identity, an individual's personal development and personal autonomy as well as their right to establish and develop relationships with other people and their social environment.[200]

But it does not go further in explaining its understanding of the scope of 'the right to privacy', and why it considers it to be more restricted that the 'right to a private life'.
Further in its judgment, the Court reiterates that the content of Article 11 of the American Convention

---

[195] American Convention on Human Rights (n 189) art 11. (emphasis added).
[196] Global Survey on Internet Privacy (n 3) 53. See *Fontevecchia & D'Amico v. Argentina (*29 November 2011) Series C, No. 238 (the Court found that the publication of information about the former President of Argentina did not amount to violation of his right to privacy); *Tristan Donoso v Panama* (27 January 2009) Series C No. 193 (the Court found that the right to privacy of one private individual was violated when his private telephone conversations was made public by State's agents); *Escher et al. v Brazil (*6 July 2009) Series C, No. 200 (the case concerned telephone surveillance- see paras 127-28.
[197] IACommHR, *Garcia v Peru*, 11.006 (1995) Report No 1/95 OEA/Ser L/V/II.88rev.1 doc.9., 71. Facts: In 1992, former President of Peru Alan Garcia Perez's house forced by army soldiers and his private papers were seized (identification papers, passports, property deeds, tax declarations,..). The Commission found "the warrantless search of Dr. Garcia's home and the seizure of private family papers- actions committed by Peruvian Army soldiers- were committed in complete disregard of the procedural requirements stipulated in the Constitution. The violation of these requirements indicates that the Government of Peru failed to guarantee to Dr. Alan Garcia and to his family the full exercise of their right to privacy".
[198] Ziemele Ineta, 'Privacy, Right to, International Protection', *Max Planck Encyclopedia of Public International Law*, 30.
[199] Inter-Am Ct HR, *Atala Riffo and daughters v Chile* (24 February 2012) para 135.
[200] Ibid.

> includes, among others, the protection of privacy[201]. Privacy is an ample concept that is not subject to exhaustive definitions and includes, among other protected realms, the sex life and the right to establish and develop relationships with other human beings. Thus, privacy includes the way in which the individual views himself and to what extent and how he decides to project this view to others.[202]

The Court seems therefore to take the same approach as the Council of Europe in its 'Guide on Article 8'[203]: it appears that the notion of 'privacy' as such is considered as part of the bigger concept of 'private life'. The Court repeated this position in subsequent cases[204], but did not elaborate on the difference between the two concepts- and consequently neither on the difference of scope of the two rights.

There are other cases where the issue of protecting private interests rose in front of the IACmmHR, but in complicated circumstances: the judicial assessment of a potential violation of the right to privacy is usually absorbed by findings of serious violations such torture or kidnapping endangering the right to life.[205] Taken in conjunction with Article 13[206], the IACommHR recognized the existence of habeas data.

The Banjul Charter[207] for its part stands out by the absence of any provision protecting any kind of private interests. No article with a wording coming close to the vocabulary of 'privacy', 'private life' nor 'private interests' exists in its text. That said, it is deemed that certain aspects generally understood as 'falling within the concept of privacy' might actually be protected in practice by other articles, such as Article 4 which provides that human beings are inviolable and that personal integrity should be respected, Article 5 which consecrates the right to human dignity, and Article 16 that states that: 'Every individual shall have the right to enjoy the best attainable state of physical and mental health.' Taken all together, these provisions might cover certain private interests. The inviolability of one's individual and his right to respect of his dignity in particular 'contribute to the protection of one's privacy in a sense used in other human rights treaties'.[208] In that respect, the African Commission on Humans and People's Rights and the African Court on Human and People's Rights could substantially contribute in determining whether the Charter indeed protects private interest. However, so far the Commission has mainly been preoccupied with armed conflicts situations, gross violations of human rights and refugees related issues.[209]

Conclusion

[201] Case of the *Massacres of Ituango v. Colombia* (1 July 2006) Series C No. 148, para 193; Case of *Rosendo Cantú et al. v. Mexico* (31 August 2010) Series C No. 216, para 119.
[202] *Atala Riffo* (n 199) para 162.
[203] Guide to Article 8 (n 176).
[204] Inter-Am Ct HR, *Murillo v Costa Rica* (28 November 2012) para 143.
[205] Ziemele (n 198) 31.
[206] 'Freedom of Thought and Expression'
[207] (adopted 26 June 1981, entered into force 21 October 1986) OAU Doc. CAB/LEG/67/3 rev. 5, 21 I.L.M. 58.
[208] Ziemele (n 198) 33.
[209] Ibid, 34.

'Privacy' has been protected by international human rights instruments from the very beginning. At the universal level, both the UDHR, that has crystallised into customary international law, and the ICCPR contain provisions clearly granting legal protections to privacy. Their wide ratification by states and acceptance in the international community more generally have contributed to the establishment and solidification of an international right to privacy in international law. Additionally, other subject-specific human rights conventions, as well as the output of the Human Rights Council Special Procedures and treaty bodies have also contributed in strengthening the recognition of the right to privacy at the international level. Still, the content and scope of this right is very much open to debate.

The drafting histories of the UDHR and the ICCPR do not really give any indication on the reasons why their drafters thought that a legal protection of privacy was important to be included. They were also silent on the meaning of the concept of 'privacy' itself and the scope of the protection attached to it. It seems as if they almost 'took for granted' that a protection of privacy needed to be part of the International Bill of Human Rights, and no much debate around it took place. Interestingly, a general right to privacy was not at the time recognized in any of the constitutions of UN Member States. National jurisdictions protected mostly the inviolability of the home and the secrecy of correspondence.

The analysis of the drafting history of the ICCPR, UDHR and ECHR shows that there was no meaningful conversation behind the introduction of specific protections to 'privacy'. Even though no domestic systems at the time contained such a broad right, its inclusion in these major instruments was not contested. It seems like 'the creators of the UDHR, the ICCPR and the ECHR did something new when they decided to include an umbrella term in the provisions on privacy, but they made this step without being aware of the potential implications of such guarantee'[210]. To this day, the intentions of the UDHR and ICCPR's drafters are not clear, and hence not particularly useful in 'shaping' our understanding of the right to privacy at the international level. The only point that can be made is that both provisions are framed in terms of guarantee of 'freedom of interference'. This is a 'passive' conception of the right to privacy, requesting States not to interfere in individual's lives-allowing them a certain zone free, away, from unwanted interaction. This is so, even though the second paragraph of both provisions states that everyone has the right to the protection of the law against such interference, adding in practice a more 'positive obligation' on States, the conception of the right stays the same.

The second part of twentieth century did not raise major questions and the ambiguity left by the drafters did not seem to concern much the international community. Change appeared with important technology breakthroughs, offering States new tools for increased surveillance and creating new threats for individual's enjoyment of their privacy (threats coming from private and public sources). Article 12 of the UDHR and Article 17 of the ICCPR suddenly became the focus of many conversations, the protection they are granting being used to assess State's actions.
Official bodies such as the Human Rights Committee stayed silent on the question, but in 2015, after relevant issues being raised at the Human Rights Council and the UN General Assembly repeatedly, a Special Rapporteur was appointed to focus exclusively on the right

[210] Digglemann/Cleis (n 25) 457.

to privacy. The SRP has submitted several rapports to this day, but they mainly explore the issues of enforcement, applicability and limitations. No 'deep' (re) thinking about how the right to privacy is conceptualized at the international level seems to be on the agenda. The few parts of the reports exploring these questions appear to conceptually mix different issues: the concept of privacy, the right to privacy and the reasons behind protecting legally private interests. There is also a clear oscillation between the different paradigms of 'freedom of interference' and 'control'. When assessing the right to privacy the traditional discourse of 'zones' is often repeated by the UN bodies. Slowly, the influence of data protection regimes having an effect, a paradigm of 'control' is emerging as part of what is understood the right to privacy means/includes. This is the subject of the following chapter.

At the regional level, many frameworks protect private interests, under some form or the other. The European Convention of Human Rights probably grants the most comprehensive system of protection. Its Article 8 explicitly protects 'private life'; but what makes the regime so effective is the case-law of the ECtHR and its interpretation of the right to respect of private life. It effectively 'fills the provision with content'. Other instruments are not considered as granting such a 'strong' protection- mainly because of either the absence of corresponding courts in their respecting system or scarcity of the case-law on the subject.
As Frank La Rue stated before: 'the lack of explicit articulation of the content of this right has contributed to difficulties in its application and enforcement'[211]. This 'lack of explicit articulation' at the international level complexifies the discourse on online surveillance regulation and how to bring surveillance activities to comply with the international right to privacy.

[211] La Rue (n 5) 21.

CHAPTER III: Data Protection Frameworks

Introduction

Looking at the international regulation of privacy and surveillance practices in the 21st century is inevitably linked to the regime of data protection laws. One of the sources of confusion in the debate on online surveillance regulation is not only the conceptual baggage of privacy regulations, but complicated relationship between the legal regimes of privacy and data protection. To bring conceptual clarification to the surveillance debate, attention needs to be paid to data protection frameworks.

It is no coincidence that the attention of the public, policy-makers and scholars to privacy surged in the 1960s when new technologies, including computers, started to emerge and progressively became available to the general population and public authorities alike. Simultaneously to the emergence of the so-called Information Age,[1] this increase in computer usage led to concerns about how people's private interests would be best safeguarded. The emergence of cloud-based systems of data storage, involving Big Data technology, increased exponentially the possibility that the protection of individuals' data would be undermined.[2] It is quite common pattern that new technologies lead to public concern, triggering in turn legislative processes aiming to regulate the new activities that are made possible by said technological development. A pertinent illustration can be found in a 1890 article by Brandeis and Warren, where the authors expressed their concern over the appearance of amateur cameras and the risk they could pose to individuals' privacy.[3] At the end of the 19th century, the public was concerned about instantaneous photography, while at the end of the 20th century public awareness focused on computers, and later, the internet. The invention of the internet, and its far-reaching grasp in virtually everyone's everyday life, have completely transformed the way information is generally accumulated, spread, and shared, and more particularly the extent to which information on individuals may be intercepted, stored, and used. This has in turn led to Governments starting to collect big amounts of data on their citizens, which has raised concerns about the lack or deficiencies of legal protection afforded to such data. The growing ability of computers to process vast amounts of data drove the development of the law and its specialisation towards the regulation of new technologies. Hence, the emergence of the so-called 'information technology' is one of the main driving forces behind the development of data protection as

[1] Robert M Gellman, 'Can privacy be regulated effectively on a national level? Thoughts on the possible need for international privacy rules' (1996) 41 Vill. L. Rev. 129, 133. "Alan Westin refers to the 'privacy crisis on the 1960s' when new physical, psychological and data surveillance technology applications transformed privacy into an issue that affected average consumers" quoted in in Gellman 133.
[2] Rolf H Weber and Dominic Staiger, *Transatlantic Data Protection in Practice* (Springer 2017) 1.
[3] Samuel D Warren and Louis D Brandeis, 'The Right to Privacy' (1890) 4 Harvard Law Review 193, 195: "Recent inventions and business methods call attention the next step which must be taken from the protection of the person, and for securing to the individual what Judge Cooley calls the right 'to be let alone'. Instantaneous photographs and newspaper enterprise have invaded the sacred precincts of private and domestic life; and numerous mechanical devices threaten to make good the prediction that 'what is whispered in the closed shall be proclaimed from the house-tops". For more on Brandeis and Warren's article, See *supra* Chapter I.

a separate field of law.[4] As shown in two first chapters of this thesis, a general right to privacy was already recognised in certain domestic jurisdictions and at the international level in the second part of the 20th century,[5] but it was still felt that these more general provisions were not enough to protect individuals' rights from automated and mass processing.[6]

Slowly, a new specialised regime regulating data processing was created, a specific right to data protection recognised in certain instruments,[7] progressively separating itself from general privacy laws. These two fields of law, the regime on the protection of privacy and on data protection, are not similar and identifying the exact nature of their relationship is an important issue. More specifically, the two regimes might sometimes overlap and in certain occasions data protection practices might be understood as falling under the scope of 'a general right to privacy'.[8] The distinction, however, is not purely symbolic as the two rights have significant differences in scope and in their accepted limitations.[9] Data protection laws usually protect *personal* data and they are not confined on *private* data; for this reason, they cannot be 'subsumed' under the concept of privacy, or its legal protection. The ECJ, for example, has clearly explained that in comparison to the general right to privacy, the EU data protection regulations grant 'a specific and reinforced system of protection'.[10] In that respect, any processing of personal data—at least in Europe—triggers the relevant data protection frameworks, whereas the right to privacy is only at stake when a certain private interest, or 'private life' is under threat. Of course, in certain cases a given activity or conduct can compromise both rights at the same time.[11]

At this point, a terminological clarification concerning data protection regimes is also in order. The terminology of 'data protection' is usually found in European legal frameworks and instruments, while in certain other legal regimes, such as in the United States legislation, data regulation is framed under the larger 'privacy' umbrella. Data protection is understood in these jurisdictions as an 'informational subset of privacy'.[12] Terms such as 'informational privacy' are used within the relevant legal framework, while the terminology of 'data privacy' has been increasingly used by scholars in the last twenty years. This term is conceived as "an attempt to signal more accurately than the other two terms [data protection and informational privacy] the focus, thrust, and rationale of the relevant norms".[13] Such terminological differences should be kept in mind when reading and analysing legal systems

[4] Paul De Hert/Vagelis Papakonstantinou, 'Three Scenarios for International Governance of Data Privacy: Towards an International Data Privacy Organization, Preferably an UN Agency' (2013) 9 ISJLP 271, 272.
[5] See *supra* Chapter II of this thesis.
[6] De Hert/Papakonstantinou (n 4) 272.
[7] Charter of Fundamental Rights of the European Union (7 December 2000) OJ C364/1, [2007] OJ C303/1, [2012] OJ C326/391, art 8.
[8] Toby Mendel et. al., 'Global Survey on Internet Privacy and Freedom of Expression' (Unesco Series on Internet Freedom, Unesco Publishing 2012) 51. (hereinafter 'Global Survey on Internet Privacy').
[9] Juliane Kokott/Christoph Sobotta, 'The distinction between privacy and data protection in the jurisprudence of the CJEU and the ECtHR' (2013) 3 International Data Privacy Law 222, 222.
[10] Case C-28/08 P *Commission/Bavarian Lager* [2010] ECR I-6055, 60. (and this finding was based on EU secondary law and not even considering the EU Charter that in the meantime has become EU primary law).
[11] For example: in the Digital Rights Ireland case, the CJEU found that the EU Data Retention Directive 2006/24/EC violated both the fundamental right to personal data protection (para 36) and the right to respect of private life (para 32-35). Joint Cases C-293/12 and C-594/12 [2014].
[12] Monika Zalnieriute, 'An International Constitutional Moment for Data Privacy in the Times of Mass-Surveillance' (2015) 23 International Journal of Law and Information Technology 99, 104.
[13] Lee A Bygrave, *Data Privacy Law: An International Perspective* (OUP 2014) 26.

and literature on the subject, especially since major actors such as the United States and European States use two different sets of vocabulary. This not only does little to clarify an already muddled field but also reveals two different conceptual views on the subject, or at least two different focuses. In Europe, the vocabulary of 'data protection' is commonly used denoting a clear(er) separation between the legal protection over data and the protection over private interests (i.e. of the right to privacy).[14] Private or not, personal data receives the same legal protection under data protection regulations. Certain safeguards are further enhanced when the data in question is considered 'sensitive',[15] and this 'sensitivity' is linked to the private character of the information concerned. Nonetheless, certain data do not concern in any way private aspects of individuals' lives and still benefit from the protection of the respective legal framework. Contrariwise, this distinction is muddled in jurisdictions like the United States which use the terminology of 'information privacy', or 'data privacy'. Overall, data protection terminology focuses on 'data', whereas 'informational privacy' shifts the attention to 'privacy', granting legal protection exactly because of the private character of the data concerned.

In this thesis, the terminology of 'data protection' is mainly used as it seems to offer a clearer view on the separate objectives of the two regimes and also avoids unnecessary confusion. The right to privacy is a human right, protected under the relevant human rights instruments and the constitutional frameworks of the various states, whose scope includes private data processing; data protection laws regulate data processing activities, irrespective of whether these involve private data or not. Part I of this chapter then looks at the existing international and regional regulatory frameworks on data protection. After discussing the main instruments at play (section 1), the general patterns and principles that underpin these frameworks are teased out (section 2). Following that, the theoretical relationship between the right to privacy and data protection is analysed in more detail (section 3). The second part of this chapter offers a comparative analysis between the data protection systems found in Europe and the United States. The first part looks at the European system (section 1), the second at the United States (section 2), while the third contains a comparative analysis of the two, highlighting their differences and the problems such disparities raise (section 3).

Part I. International and Regional Data Protection Frameworks

When discussing the legal protection of data and the debates surrounding it, it is important to clarify the different aspects of the question. There are several sides to the issue, with each including a different 'international component'. One side is the regulation of data processing activities, ranging from collection, to storage, usage and destruction. Different countries

[14] For example, the EU Charter (n 7) has established two different provisions, one protecting privacy (Article 7) and the other personal data (Article 8).

[15] Eg, 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 (24 October 1995) OJ L 281, 23 November 1995, p. 0031-0050, (70) (hereinafter 'Directive 1995'); Regulation (EU) 2016/679 of the European Parliament and 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), 2016 O.J. (L. 119) 1 (EU), art 9, Recitals 51, 53, 54. (hereinafter GDPR).

have different views on how best to do all this,[16] and this aspect of data protection is considered as a domestic matter. Certain international and regional treaties set standards on the topic, but there is no international element 'per se' in the processing. The international element ensues from the nature of the instruments regulating data processing instead.

Another aspect of the data protection discourse is the regulation of transborder flows of data. Because practices of data transfers and data processing regularly happen across borders, complex situations arise where several data protection laws might apply simultaneously to one single operation.[17] This has created difficulties for many private companies and multinational corporations, which quickly 'actively demanded' clarification of the rules at play. Hence, a clear economic incentive existed for States to find concrete solutions to facilitate information flows between countries and make it easier for private companies to engage in international business. That was a driving force behind the internationalization of data protection regulations early on.[18] From this perspective, the international element is at the core of the subject. States regulate the transborder flow of data to achieve different goals, including building stronger mutual cooperation and removing obstacles that make it difficult to share data. Their motives can vary from ensuring the respect of their own citizens' rights to facilitating trade; often they are a mixture of these two and other objectives too.[19] To achieve this, States may engage in traditional treaty-making, as for example is the case with the EU-US and EU-Swiss Privacy Shield Frameworks. In this instance, the international element is clear. Sometimes, however, even 'strictly' domestic or regional standards have international repercussions. For example, when the EU imposed an adequacy requirement in 1995,[20] the effect rippled through worldwide with many States having to adapt (or even enact for the first time) their own legislations in order to be able to keep exchanging data with a significant player as the EU. This makes evident that the international aspects of transborder data flow regulation are multiple. These two aspects, namely regulating data processing activities and regulating transborder flows of data, despite being obviously interlinked, remain different, and it is useful to keep that in mind when analysing the field of data protection.

One factor obfuscating the data protection field is the multitude of frameworks existing. It is not just the impressive amount of the different instruments that makes the topic complex, but also the very wide range of legal framework. The various instruments and legislations provide from restricted rights targeted exclusively to specific fields (e.g., typically the ones found in the legal regime of the United States) to comprehensive omnibus laws (typically

[16] For example, in Europe, 'omnibus' laws are preferred: they regulate the processing of data in general, and certain additional safeguards are granted for specific data. In the United States, sectorial regulations are enacted according to the field in which the processing takes place; more on this *infra:* Section 2.
[17] Joel R Reidenberg, 'The simplification of international data privacy rules' (2006) 29 Fordham Int'l L.J. 1128, 1128.
[18] De Hert/Papakonstantinou (n 4) 276.
[19] See for example the preface of the OECD Guidelines.
[20] The "adequacy requirement" was originally established by the 1995 Directive (art 25.1) and is now found in the GPDR. It only allows data transfers to a third-party country if the latter warrants an 'adequate level of protection: "*A transfer of personal data to a third country* or an international organisation may take place where the Commission has decided that the third country (…) or the international organisation in question *ensures an adequate level of protection*". (GDPR art 45).

found in Europe) and general fair information principles (e.g. the UN Guidelines[21] or OECD Guidelines[22]). It is thus fair to say that data protection frameworks can take extremely varied forms, and vary in scope and the regulatory tools and principles they use: laws, principles, self-regulatory mechanisms, technical standards, binding or non-binding, of national, regional, or international scope, targeting public and/or private actors. It is easy to get lost in the legion of instruments.

The purpose of the following sections is to clarify the heavily-regulated field of data protection: firstly by sketching the main regulatory frameworks at play[23], secondly by exposing the core principles in data protection and finally by exploring their relation with the right to privacy and the different conceptual paradigms they imply.

Section 1. Regulatory Actors

Domestically, the very first data protection law appeared in the State of Hesse in Germany in 1970.[24] It was followed at the national level by Sweden (1973),[25] the United States (1974),[26] Germany (1977),[27] and France (1978).[28] Data protection laws have been enacted at the international and regional levels for – roughly – the past forty years.

A. OECD

In 1980, the Organization for Economic Co-operation and Development (OECD) drew the very first guidelines on data protection at the international level: the Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.[29] The preparatory work for these Guidelines started in 1968, which shows how pioneering the OECD was with regard to this topic. These Guidelines enjoy wide consensus from OECD Members which, at the domestic level, have very different attitudes towards data protection, in particular when it comes to Germany, the United Kingdom, the United States and Japan.[30] The main principles found in this instruments will be detailed in the following section.
One of the main objectives of the Guidelines was to increase and facilitate international cooperation, rather than to directly harmonize the respective national frameworks. To do so, it formulated very broad and basic principles that States could then implement easily in their domestic jurisdictions,[31] avoiding the more complicated, model-law approach with

[21] UNGA Res 45/95, 'UN Guidelines for the Regulation of Computerized Personal Data Files' (14 December 1990). (hereinafter 'UN Guidelines').
[22] OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (adopted 23 September 1980, updated in 2013). 'hereinafter OECD Guidelines'.
[23] To read a comprehensive analysis of all international instruments regulating data protection, See Bygrave (n 13); Christopher Kuner, *Transborder Data Flows and Data Privacy Law* (OUP 2013).
[24] Hessian Data Protection Act (7 October 1970) GESETZUNO VERORONUNGSBLATT [GVBI] 625.
[25] The Data Act of 1973, SFS 1973:289, amended at SFS 1982:446 (Swedish Code of Statutes).
[26] The Privacy Act of 1974, P.L. 93-579, 5 USC §552a.
[27] The Federal Data Protection Act (BDGS).
[28] Loi No. 78-17 du 6 Janvier 1978 relative à l'information, aux fichiers et aux libertés, *Journal Officiel de La République Française* (7 January 1978).
[29] adopted by OECD Council Recommendation on 23 September 1980 (updated in 2013).
[30] De Hert/Papakonstantinou (n 4) 277.
[31] Preface of the Guidelines states that the Guidelines "would help to harmonise national privacy legislation and, while upholding such human rights, would at the same time prevent interruptions in international flows of data. They represent a consensus on basic principles which can be built into existing national legislation,

comprehensive provisions that would have had to be integrated in its entirety. The Guidelines established a voluntary common basis, leaving specific implementation to be done at the national level.[32] This type of framework has subsequently been copied by numerous other organizations enacting their own regulatory standards on data management.

B. Council of Europe

Almost simultaneously, in 1981, the Council of Europe adopted Convention No 108 for the Protection of Individuals with Regard to the Automatic Processing of Personal Data,[33] which was later amended in 2001[34] and in 2018[35] with additional protocols. The 2018 Protocol modernised the Convention regime, 'to ensure that the transfer of personal data across borders is done with appropriate safeguards', also providing for the possibility of the EU and other international organizations becoming parties to the Convention.[36] The Convention as an international treaty is legally binding upon the parties— not frequently the case in data protection regulation, which tend to take more soft-law forms. It is also open for signature to countries that are not members of the Council of Europe,[37] a fact that elevates this instrument above the regional context. Convention No. 108 was also the first instrument to set an 'adequacy requirement',[38] which apart from enhancing strong cooperation between States, also created a strong incentive for States without data protection laws to establish one.

This discussion shows that from the 1960s, the OECD and the Council of Europe provided States involved in information processing and exchange with platforms to discuss new issues that they were facing, while in the early 1980s they set up the first international frameworks regulating these activities. They also influenced upcoming new domestic regulations, which drew inspiration from these international frameworks, and which consequently led to similarities between regimes.

C. United Nations

---

or serve as a basis for legislation in those countries which do not yet have it"; and that the purpose of the guidelines is "to advance the free flow of information between Member countries and to avoid the creation of unjustified obstacles to the development of economic and social relations among Member States".

[32] De Hert/Papakonstantinou (n 4) 277.

[33] (adopted on 28 January 1981, entered into force 1 October 1985) ETS No. 108. (hereinafter Convention No 108).

[34] Additional Protocol to the Convention for the Protection of Individuals with Regard to the Automatic Processing of Personal Data, Regarding Supervisory Authorities and Transborder Data Flows (adopted 8 November 2001, entered into force 1 July 2004) ETS No. 181.

[35] Protocol amending the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (adopted 10 October 2018, not yet entered into force) ETS No. 223.

[36] See 'Council of Europe treaty bolstering data protection opened for signature' <https://search.coe.int/directorate_of_communications/Pages/result_details.aspx?ObjectId=09000016808e4d8a> accessed 12 September 2019.

[37] Council of Europe, Committee of Ministers of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108) (T-PD), 'Abridged report of the 24th plenary meeting (Strasbourg, 13-14 March 2008)' (2 July 2008) (CM(2008)81) Decision, Item 10.2. <https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=09000016805d3576> accessed 10 September 2019.

[38] Convention No 108 (n 33) art 12. More on this *infra.*

Almost ten years later, in 1990, the United Nations adopted the UN Guidelines for the Regulation of Computerized Personal Data Files.[39] The principles contained in the Guidelines apply to national legislations, but also to inter-governmental organizations, targeting publicly and privately stored computerized files on individuals and manual files on legal persons.[40] The UN Guidelines did not receive a particularly warm welcome from States and scholars alike[41]: they are not legally binding, and they did not bring anything new in comparison to the OECD Guidelines and the Convention No. 108, which were already firmly set and accepted as regulating the field since they were adopted. Still, even if non-binding, this is the only truly global instrument on data protection.

In 2006, the International Law Commission addressed the issue of 'protection of personal data in transborder flow of information' in its fifty-eight session.[42] The objective of the proposal was to

> elaborate general principles that are attendant in the protection of personal data. (…) The elaboration of a 'third generation' of privacy principles would augur well with increasing calls for an international response on this matter. (…) The Commission may be able to identify emerging trends in legal opinion and practice which are likely to shape any global legal regime which would finally emerge.[43]

Data protection concerns have started to appear in UN discourse in the context of human rights, too. In 2009, Martin Scheinin, UN Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism wrote that 'data protection is also emerging as a distinct human or fundamental right'.[44] In 2011, Frank Larue, the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, underscored the obligation of States to adopt effective privacy and data protection laws in accordance with human rights standards.[45] As already mentioned in Chapter II, in March 2015, a Special Rapporteur on the right to privacy (SRP) was established by the Human Rights Council.[46] Among his other activities, he also set up a Task

[39] UNGA Res 45/95 (14 December 1990).
[40] Global Survey on Internet Privacy (n 8) 63.
[41] For example, they are often referred as of "limited practical relevance" in Christopher Kuner, 'An International Framework for Data Protection: Issues and Prospects' (2009) 25 Computer L. & Security Rev. 314.
[42] ILC Secretariat, 'Annex IV. Protection of Personal Data in Transborder Flow of Information' in Report of the International Law Commission on the work of its fifty-eight session (1 May to 9 June to 11 August 2006) UN Doc A/61/10, 217-228. (hereinafter 'ILC Report').
[43] Ibid, para 12.
[44] UNHRC, 'Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Martin Scheinin' (28 December 2009) UN Doc A/HRC/13/37, para 12.
[45] UNHRC, 'Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue' (16 May 2011) A/HRC/17/27: "The Special Rapporteur underscores the obligation of States to adopt effective privacy and data protection laws in accordance with article 17 of the International Covenant on Civil and Political Rights and the Human Rights Committee's general comment No. 16. This includes laws that clearly guarantee the right of all individuals to ascertain in an intelligible form whether, and if so what, personal data is stored in automatic data files, and for what purposes, and which public authorities or private individuals or bodies control or may control their files." para 83.
[46] UNHRC, 'Resolution: The right to privacy in the digital age' (24 March 2015) UN Doc A/HRC/28/L.27, 4.

Force specifically dedicated on Big Data and Open Data.[47]Its first report was presented at the General Assembly in October 2017.[48]

D. Other Regional Frameworks

At the regional level, frameworks safeguarding individuals' data have emerged in all continents. In Europe, as mentioned above, the Council of Europe adopted Convention No 108 in 1980. The European Union for itself has enacted several Directives and Regulations on the subject,[49] the main one being the Data Protection Directive of 1995,[50] which was replaced in 2018 by the General Data Protection Regulation (GDPR).[51] The European Union also included a specific provision on data protection in the European Union Charter of Fundamental Rights (Article 8) and in the Treaty of the Functioning of the European Union (Article 16).

In Asia, the Asia-Pacific Economic Cooperation (APEC) adopted its Privacy Framework in 2004.[52] This is a non-binding instrument, establishing more flexible standards of protection than those found in Europe. However, it does still create a common ground for data protection in a region where such regulations are less frequent.[53] The Framework was updated in 2015.[54] It is accompanied by the Cross-Border Privacy Rules (CBPR), which is a system set up by APEC economies that 'requires participating businesses to implement data privacy policies consistent with the APEC Privacy Framework'.[55]
The Association of Southeast Asian Nations (ASEAN) adopted the ASEAN Human Rights Declaration in November 2012.[56] Its Article 21 reads:

---

[47] The Task Force looks in details into the issues of Data, Big Data, advanced analytics, algorithms, open data, open government,… UNGA, 'Right to Privacy: Note by the Secretary General transmitting the Report of the Special Rapporteur of the Human Rights Council on the Right to Privacy, Joseph A Cannataci' (19 October 2017) UN Doc A/72/540, paras 5-25.
[48] UNGA, 'Report of the Special Rapporteur on the right to privacy: Note by the Secretary-General' (19 October 2017) UN Doc A/72/43103.
[49] Eg: Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector ("ePrivacy Directive") but it will be replaced by the "ePrivacy Regulation" (Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications); Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services; Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws; Regulation (EC) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/ECText with EEA relevance.
[50] Directive 1995 (n 15).
[51] GDPR (n 15).
[52] APEC Privacy Framework (December 2005) APEC#205-SO-01.2
[53] De Hert/Papakonstantinou (n 4) 288.
[54] APEC Privacy Framework (2015) APEC#217-CT-01.9 (published in 2017).
[55] Cross Border Privacy Rules Official Website <http://cbprs.org/> accessed 20 May 2019.
[56] ASEAN Human Rights Declaration (19 November 2012) <http://www.europarl.europa.eu/meetdocs/2009_2014/documents/droi/dv/42_aseanhrdecl_/42_aseanhrdecl_en.pdf> accessed 10 September 2019.

> Every person has the right to be free from arbitrary interference with his or her privacy, family, home or correspondence *including personal data*, or to attacks upon that person's honour and reputation.
>
> Every person has the right to protection of the law against such interference or attacks.[57]

The vocabulary used in this provision is clearly influenced from the Universal Declaration of Human Rights, and even though the ASEAN Declaration has undergone criticism by many human rights organisations and the UN as falling short in establishing effective human rights standards,[58] the special reference to personal data is something to highlight. Indeed, it illustrates not only the growing attention around the issue of data protection, but has also pushed ASEAN members to implement domestic frameworks regulating the processing of personal data.[59]

In Africa, the Economic Community of West African States (ECOWAS) has adopted a Supplementary Act A/SA.1/01/10 on Personal Data Protection.[60] The Act was undoubtedly influenced by the Data Protection Directive of the European Union: it sets the standards of data protection that each State needs to implement,[61] and it also requires the establishment of data protection authorities at the domestic level.[62] For its part, the African Union adopted a Convention on Cyber Security and Personal Data Protection (Malabo Convention) in 2014.[63]

The General Assembly of the Organization of American States (OAS) has passed several Resolutions on 'Access to Public Information and Protection of Personal Data'.[64] In 2012, the OAS Inter-American Juridical Committee proposed to the General Assembly to adopt twelve principles.[65] These are 'intended to prevent harm to individuals from the wrongful or unnecessary collection or use of personal data and information'[66], though without explicitly detailing the kind of harms that they concern. The Inter-American Juridical Committee was also instructed by the OAS General Assembly in June 2014 'to prepare proposals (…) on the different ways in which the protection of personal data can be regulated, including a

---

[57] (emphasis added).
[58] Graham Greenleaf, 'Sheherezade and the 101 Data Privacy Laws: Origins, Significance and Global Trajectories' (2014) 23(1) Journal of Law, Information & Science, 26; UN News, 'UN official welcomes ASEAN commitment to human rights, but concerned over declaration wording' (19 November 2012) <https://news.un.org/en/story/2012/11/426012> (accessed 20 May 2019)
[59] Greenleaf (n 58) 25-26.
[60] ECOWAS, Supplementary Act on Personal Data Protection (adopted on 16 February 2010) A/SA.1/01/10.
[61] Ibid, arts 2, 3, and 4.
[62] Ibid, art 14.
[63] African Union, Convention on Cyber Security and Personal Data Protection (adopted 27 June 2014, still not into effect) EX.CL/846(XXV).
[64] Resolution 2661 'Access to Public Information and Protection of Personal Data' (7 July 2004) AG/RES.2661 (XLI-O/11); Resolution 2727 'Access to Public Information and Protection of Personal Data' (4 June 2012) AG/RES. 2727 (XLII-O/12); Resolution 2811 'Access to Public Information and Protection of Personal Data' (6 June 2013) AG/RES. 2811 (XLIII-O/13); Resolution 2842 'Access to Public Information and Protection of Personal Data' (4 June 2015) AG/RES. 2842 (XLIV-O/14).
[65] Inter-American Juridical Committee 'Proposed Statement of Principles for Privacy and Personal Data Protection in the Americas' (9 March 2012) CJI/RES. 186 (LXXX-O/12). The principles roughly following the general FIPs: Lawful and Fair Purposes; Clarity and Consent; Relevant and Necessary; Limited Use and Retention; Duty of Confidentiality; Protection and Security; Accuracy of Information; Access and Correction; Sensitive Information; Accountability; Trans-border Flow of Information and Accountability; Disclosing Exceptions. – more on this in the next section.
[66] Ibid, 1.

model law on personal data protection, taking into account international standards in that area'.[67] After several short reports,[68] the OAS Principles on Privacy and Personal Data Protection (With Annotations)[69] were presented in March 2015. The stated purpose of the principles is to 'establish a framework for safeguarding the rights of the individual to personal data protection and informational self-determination (…) They are intended to protect individuals from wrongful or unnecessary collection, use, retention and disclosure of personal data'.[70] In their drafter's opinion, the best option was to flesh out the content of the previously adopted twelve principles in 2012[71] (with few minor changes). These could then serve as legislative guidelines for Member States, instead of trying to work towards the enactment of a specific law with all the difficulties in reaching agreement that this would entail.[72] The OAS has also established a fundamental right 'to access to information',[73] which became a cornerstone of the system.[74]

The Organisation of Eastern Caribbean States (OECS) has also its own a Data Protection Bill,[75] which follows the main Fair Information Principles,[76] grants individuals some rights and sets enforcement measures. Finally, another major source of data protection norms is the Associations of Data Protection Authorities around the world. These exist and operate at the international,[77] regional,[78] and domestic levels. They produce a massive amount of work, but they fall outside the scope of this study.

---

[67] Resolution AG/RES 2811 (XLIII-O/13).
[68] Inter-American Juridical Committee, 'Report by David P. Stewart: Privacy and Data Protection' (25 February 2014) CJI/doc. 450/14; Inter-American Juridical Committee, 'Report by David P. Stewart: Privacy and Data Protection' (26 July 2014) CJI/doc. 465/14.
[69] Inter-American Juridical Committee, 'Privacy and Data Protection' (26 March 2016) CJI/doc. 474/15 rev.2. 3.
[70] 'Privacy and Data Protection' (26 March 2016) 3. (emphasis added).
[71] CJI/RES. 186 (LXXX-O/12).
[72] 'Privacy and Data Protection' (n 69) 1.
[73] "Access to information is a *fundamental human right* which establishes that everyone can access information from public bodies, subject only to a limited regime of exceptions in keeping with a democratic society and proportionate to the interest that justifies them. States should ensure full respect for the right to access to information through adopting appropriate legislation and putting in place the necessary implementation measures." In Inter-American Juridical Committee 'Principles on the Right of Access to Information' (7 August 2008) CJI/RES.147 (LXXIII-O/08) 1. (emphasis added). See also Inter-American Juridical Committee 'Right to Information: Access to and Protection of Information and Personal Data in Electronic Form' (27 February 2007) CJI/doc.25/00 and Committee on Juridical and Political Affairs, 'Recommendations on Access to Information' (21 April 2008) CP/CAJP-2599/08.
[74] AG/RES. 2842 (XLIV-O/14) 'Access to Public Information and Protection of Personal Data'; AG/RES. 1932 (XXXIII-O/03) 'Access to Public Information: Strengthening Democracy'; AG/RES. 2057 (XXXIV-O/04) 'Access to Public Information: Strengthening Democracy'; AG/RES. 2121 (XXXV-O/05) 'Access to Public Information: Strengthening Democracy'; AG/RES. 2252 (XXXVI-O/06) 'Access to Public Information: Strengthening Democracy'; AG/RES. 2288 (XXXVII-O/07) 'Access to Public Information: Strengthening Democracy'; AG/RES. 2418 (XXXVIII-O/08) 'Access to Public Information: Strengthening Democracy'; AG/RES. 2514 (XXXIX-O/09) 'Access to Public Information: Strengthening Democracy'; AG/RES. 2607 (XL-O/10) 'Model Inter-American Law on Access to Public. Information'.
[75] Organisation of Eastern Caribbean States, 'Data Protection Bill' (6 October 2011).
[76] More on this in the next section.
[77] International Conference of Data Protection and Privacy Commissioners (ICDPPC); Global Privacy Enforcement Network (GPEN).
[78] EU Article 29 Working Party; European Data Protection Authorities (EDPA), Asia Pacific Privacy Authorities (APPA; Central and Eastern Europe Data Protection Authorities (CEEDPA); Nordic Data Protection Authorities (NDPA), British, Irish and Islands Data Protection Authorities (BIDPA), Association of Francophone Data Protection Authorities (AFAPDP), La Red Iberoamericana de Proteccion de Datos (Latin American Network) (RIPD), Committee associated to Convention 108. To read more on the work of the EU 29 Working Party: See Y Poullet and Serge Gutwirth, 'The Contribution of the Article 29 Working Party to

All these regional and international organisations have produced an incredible volume of work on data protection, which has enriched data protection regimes worldwide. However, 'one cannot help but note that these efforts are sometimes duplicative and largely advance in parallel, [and that] missing from this framework is formal and institutional trans-organisational cooperation aimed at the formulation of a common regulative framework.'[79] The next section will try to see past through this fragmentary framework and bring together the various instruments by fleshing out the core principles of data protection. This intends to deepen our understanding with regard to the fundamental normative elements of the field as a whole.

Section 2. Core Principles of Data Protection

As a general rule, most data protection frameworks are constructed so as to attain three goals. The first is to regulate the actions of 'data controllers', meaning they determine the modalities of data processing from collection, storage, use, transfer to destruction.[80] The second is to grant individuals (often referred to as 'data subjects') certain specific rights on their data, such as having access to it or having it rectified. Finally, some regimes set an oversight system to supervise the enforcement of the rules in place.[81] Additionally, data protection frameworks (both at the domestic and the international levels) are usually built around certain key principles. These principles are sometimes named or branded differently in the various instruments (depending on the organisation that has adopted them), but they all aim towards achieving these three main goals.[82]

The data protection field is riddled with multiple regulatory schemes (national, regional, international) of a different nature (from binding conventions to advisory guidelines), different scope of application (omnibus approach or sectorial regulations), and different objectives. But in the midst of all this complexity, all the relevant frameworks are built around the same core principles, often referred as 'Fair Information Principles' (FIPs).[83] Even though the main overall principles are similar across regions of the world, similitude and agreement is usually only found at the abstract level. In the words of the ILC there is 'commonality of interests in a number of core principles'.[84] Beyond this, there are clear disparities in the details of how these principles are understood and applied in practice,

---

the Construciton of a Harmonised European Data Protecitonk System: An Illustration of 'Reflexive Governance'?' in Marie Pérz-Asinari and Pablo Palazzi (eds), *Challenges of Privacy and Data Protection Law* (Bruylant 2008).

[79] De Hert/Papakonstantinou (n 4) 285.

[80] Jeffrey B Ritter, Benjamin S Hayes, and Henry L Judy, 'Emerging Trends in International Privacy Law' (2001) 15 Emory Int'l L. Rv. 87, 91.

[81] Global Survey on Internet Privacy (n 8) 63.

[82] ILC Report (n 42) para 11: "The international binding and non-binding instruments, as well as the national legislations adopted by States, and judicial decision reveal a number of core principles including: (a) lawful and fair data collection and processing; (b) accuracy; (c) purpose specification and limitation; (d) proportionality; (e) transparency; (f) individual participation in particular the right to access; (g) non-discrimination; (h) responsibility; (i) supervision and legal sanction; (j) data equivalency in the case of transborder flow of personal data; and (k) the principle of derogability". These principles are developed in the same report at para 23.

[83] This terminology was originally mainly used in US privacy law, but is now accepted and used by other legal systems around the globe. Ibid.

[84] ILC Report (n 42) para 12.

depending on cultural, historical and legal approaches to information regulation. This makes the subject simple and complex, at the same time.[85]

The following core principles can be found in most data protection regulatory schemes:

- Collection Limitation/Fair Collection: collection must be limited, lawful and fair;
- Purpose Specification: the purpose and disclosure of the collection must be specified;
- Use Limitation: data can only be used for the specific purpose for which it has been collected;
- Security: data should be protected by certain standards to avoid unintended or unauthorized disclosure;
- Data Quality: data must be accurate, complete, and relevant to the purpose of collection;
- Openness: data processing activities should be transparent;
- Access and correction: individuals should be able to access their personal data and have it rectified if inaccurate or misleading;
- Accountability/Enforcement: data controllers/processors must comply with the above principles and be held accountable in case they do not.

It has to be born in mind that these core principles are not found in all instruments and/or sometimes appear under other names. The table below illustrates the (unnecessary) confusion that often arises from an inconsistent terminology in the field of data protection:

Goals	**UN Guidelines[86]**	**OECD Guidelines 2013[87]**	**EU Charter (Art. 8)**
Regulate Data Processers actions	• Lawfulness and Fairness[88] • Accuracy[89] • Purpose Specification[90] • Security[91] • Non-discrimination[92]	• Collection Limitation[94] • Data Quality[95] • Purpose Specification[96] • Use Limitation[97] • Security[98]	• Requirement Consent/Basis in Law • Specified Purposes • Fair processing

[85] Ritter/Hayes/Judy (n 80) 88-89.
[86] UN Guidelines (n 21).
[87] OECD Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data (2013) [C(80)58/FINAL, as amended on 11 July 2013 by C(2013)79]. (hereinafter 'OECD Guidelines 2013')
[88] UN Guidelines (n 21) 1.
[89] Ibid, 2.
[90] Ibid, 3.
[91] Ibid, 7.
[92] Ibid, 5.
[94] OECD Guidelines 2013 (n 87) 7:
[95] Ibid, 8.
[96] Ibid, 9.
[97] Ibid, 10.
[98] Ibid, 11.

	• Power to make exceptions[93]	• Openness[99]	
Grant Individuals Rights over their Data	• Interested Person Access[100]	• Individual Participation[101]	• Right to Access to Data • Right to Have Data Rectified
Enforcement	• Supervision and Sanctions[102]	• Accountability[103]	• Independent Authority Requirement

The table illustrates how different frameworks convey the same principle under different terminologies. For example, the 'Lawfulness and Fairness Principle'[104] in the UN Guidelines is called 'Collection Limitation'[105] in the OECD Guidelines, and is also present in the EU Charter under the requirements of consent and legal basis.[106] These all mean that the collection of data should be limited, lawful, and fair. Overall, Fair Information Principles came about to compensate for the fact that the 'generic' right to privacy was not able to respond to the challenges raised by modern technologies, especially when it came to mass automated data processing.[107] The relationship between the right to privacy and data regulatory schemes is hence the subject of the next section.

Section 3. Relationship between the Right to Privacy and Data Protection

A. Data Protection Under Human Rights Treaties

Data processing activities sometimes fall under the scope of the right to privacy enshrined in international human rights treaties. Both the ICCPR and the ECHR have provisions protecting 'privacy' or 'private life',[108] and such provisions have been interpreted so as to provide the normative basis for certain data protection principles.

---

[93] Ibid, 6.
[99] Ibid, 12.
[100] UN Guidelines (n 21) 4.
[101] OECD Privacy Guidelines 2013 (n 87) 13.
[102] UN Guidelines (n 21) 8.
[103] OECD Privacy Guidelines 2013 (n 87) 14.
[104] UN Guidelines (n 21) 1: "Information about persons should *not* be collected or processed in *unfair or unlawful ways*, nor should it be used for ends contrary to the purposes and principles of the Charter of the United Nations" (emphasis added).
[105] OECD Privacy Guidelines 2013 (n 87) 7: "There should be limits to the collection of personal data and any such data should be *obtained by lawful and fair means* and, where appropriate, with the knowledge or consent of the data subject." (emphasis added).
[106] EU Charter (n 7) art 8(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." (emphasis added).
[107] Bart van der Sloot, 'Legal Fundamentalism: Is Data Protection Really a Fundamental Right?' in Ronald Leenes et al. (eds), *Data Protection and Privacy: (In)visibilities and Infrastructures* (Springer 2017) 5.
[108] International Covenant on Civil and Political Rights (adopted 16 December 1966, entered into force 23 March 1976) 999 UNTS 171, art 17 (hereinafter ICCPR) and the Convention for the Protection of Human

According to HRC General Comment No 16 on Article 17 of the ICCPR, data processing activities should be regulated in both the public and private sectors: 'The gathering and holding of personal information on computers, data banks and other devices, whether by public authorities or private individuals or bodies, must be regulated by law.'[109] With this in mind, the Committee then proceeded to enumerate certain core principles of data protection regimes:

> Effective measures have to be taken by States *to ensure* that information concerning a person's private life does not reach the *hands of persons who are not authorized* by law to receive, process and use it, and is never used for *purposes incompatible* with the Covenant. In order to have the most effective protection of his private life, every individual should have *the right to ascertain* in an intelligible form, whether, and if so, what *personal* data is stored in automatic data files, and for what purposes. Every individual *should also be able to ascertain* which public authorities or private individuals or bodies control or may control their files. If such files contain incorrect *personal* data or have been collected or processed contrary to the provisions of the law, every individual should have the *right to request rectification or elimination*.[110]

Notably, the Committee refers mostly to 'personal data', and not exclusively to 'private' ones. This is important because it implies that processing practices involving personal data are understood as falling under the scope of Article 17 of the ICCPR, potentially even when the data in question are not of a private nature.

These standards and rights recognised by the Committee as encompassed in the scope of Article 17 are clearly inspired by the FIPs found in international legal instruments on data protection and discussed in the previous section. Still, not all the 'usual core principles' are listed in the General Comment. In particular, no requirement for the collection to be done in a fair manner is mentioned, and no 'security' or 'data quality' principle is included. Additionally, there is no mention of special categories of data deserving additional protection. The principle of purpose specification is also not as strict as in other instruments, such as in the CoE Convention No 108. In that respect, it is not clear whether the list of principles provided for in General Comment No 16 is exhaustive or it only addresses some, and not all, of the standards that could be drawn from Article 17.[111] From a conceptual perspective, the first standards enumerated by the Committee reflect a conception of privacy as a sphere that should be free from any interference; that people should be able to keep their private information out of the hands of other people if they wish so. However, the rights to request rectification or elimination indicate a form of control over personal information, too.[112] That points to broader conception beyond one that simply views privacy as a sphere

---

Rights and Fundamental Freedoms (adopted 4 November 1950, entered into force 3 September 1953) 213 UNTS 221, art 8 (emphasis added). (hereinafter ECHR).

[109] UNHRC, 'General Comment No. 16: Article 17 (Right to Privacy): The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation' (8 April 1988) UN Doc HRI/GEN/1/Rev.9, para 10.

[110] Ibid, para 10. (emphasis added).

[111] Lee A Bygrave, 'Data Protection Pursuant to the Right to Privacy in Human Rights Treaties' (1998) 6 International Journal of Law and Information Technology 247, 253.

[112] Ibid, 253-4.

free from interference. Arguably, this list in General Comment No 16 is not exhaustive, only enumerating some of the 'guarantees capable of specification pursuant to Article 17'.[113]

Although the ECHR does not contain a specific provision on data protection,[114] the European Court of Human Rights has interpreted Article 8 as providing protection to personal data.[115] In the case of *Rotaru v Romania*, the Court held that storing information about a person's private life by a public body came under the scope of Article 8 and that 'such information[116], when systematically collected and stored in a file held by agents of the State, falls within the scope of "private life".[117] The mere fact of storing data about the private life of a person amounts to an interference of Article 8,[118] and the ensuing use of the stored information does not have any consequence on that finding.[119] To determine whether personal information relates to private life of an individuals, the Court will have "due regard to the specific context in which the information at issue has been recorded and retained, the nature of the records, the way in which these records are used and processed and the results that may be obtained".[120] The Court held in *Satakunnan Markkinaporssi Oy and Satamedia Oy v. Finland* that "in this connection that the term 'private life' must not be interpreted restrictively".

The Court recognized that:

> The protection of personal data is of fundamental importance to a person's enjoyment of his or her right to respect for private and family life, as guaranteed by Article 8 of the Convention. The domestic law must afford appropriate safeguards to prevent any such use of personal data as may be inconsistent with the guarantees of this Article.[121] Article 8 of the Convention thus provides for the right to a *form of informational self-determination,* allowing individuals to rely on their right to privacy as regards data which, albeit neutral, are collected, processed and disseminated collectively and in such a form or manner that their Article 8 rights may be engaged.[122]

Often, the ECtHR has interpreted the scope of the right under Article 8 quite broadly.[123] In order to assess if a certain type of processing involves an individual's privacy, the European Court of Human Rights uses two criteria: it first examines the type of data at stake, and then

---

[113] Ibid, (n)254.
[114] Contrary to the Charter of Fundamental Rights of the European Union.
[115] For the case-law by the ECtHR on the protection of personal data: See CoE, 'Case Law of the European Court of Human Rights Concerning the Protection of Personal Data' (15 November 2017) <https://rm.coe.int/case-law-on-data-protection/1680766992> accessed 18 September 2019.
[116] [in this specific case "various pieces of information about the applicant's life, in particular his studies, his political activities and his criminal record, some of which had been gathered more than fifty years earlier." same para]
[117] *Rotaru v Romania*, App no 28341/95 (Judgment) (4 May 2000) para 43-44.
[118] *Leander v Sweden*, App no 9248/81 (Judgment) (26 March 1987) para 48; *S and Marper v United Kingdom*, App nos 30562/04 and 30566/04 (Judgment) (4 December 2008) para 67.
[119] *S and Marper* (n 118) para 67; *Amann v Switzerland*, App no 27798/95 (Judgment) (16 February 2000) para 69*; Leander* (n 118) para 48; *Kopp v Switzerland*, App no 13/1997/797/1000 (Judgment) (25 March 1998) para 53.
[120] *S and Marper* (n 118) para 67.
[121] (see *S. and Marper* (n 118) para 103).
[122]*Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland*, App no 931/13 (Judgment) (27 June 2017) para 137. (emphasis added).
[123] Global Survey on Internet Privacy (n 8) 55.

the extent of the processing activities. According to the Court's caselaw, Article 8 will automatically apply to any data inherently relating to private life. If the nature of the data is not in essence private, the Court will analyse the extent of the processing. If the processing is systematic, it is then inquired whether there is a certain focus on the data subject and whether the latter could expect that processing of his or her personal information would take place.[124] When the processing activity is indeed found as interfering with the right to privacy, the Court has in the past recognised the applicability of certain guarantees that are usually found in data protection regulations:[125] it has approved the 'purpose limitation' principle,[126] it has recognised a right of access to personal files,[127] and the right to economic redress in case of violation of Article 8.[128] It has also agreed to requests to delete personal data stored in public files,[129] and has decided in favour of independent supervisory bodies to overview personal data processing practices.[130] These guarantees have been developed incrementally and have been granted on a case-by-case basis, so, contrary to HRC General Comment No 16, it is hard to draw any general patterns from them.

It is still quite telling of how dynamically the Court reads the provision. It implies a vision of control for the individual over his personal information and his private life. It is not exclusively about letting private parties having a 'space' free from interferences from public authorities interferences, or the necessity to let people establish relationships between themselves (both having a more 'passive' dimension), but it also gives a right to *choose* how information about one' self are collected, processed, stored, used and released. This, in turn, shows how a provision as broad as Article 8, protecting a concept as wide and abstract as 'private life' can be dynamically interpreted in granting individuals different prerogatives in practice. It illustrates how 'creative' courts might be in trying to keep legal protections relevant to modern contexts. Article 8 had to be understood progressively in order to keep offering an effective protection in front of new threats.[131] The Court could not find a specific basis for data protection on the law and so it interpreted and 'shaped' the right to privacy to include the necessary elements. As this passage illustrates, including 'data' as in the scope of legal protection granted by Article 8, the Court does not only increase the scope of the right in practice, but it also changes our theoretical understanding of what the right to privacy means.

B. Relationship between the two legal regimes

---

[124] Raphaël Gellert/Serge Gutwirth, 'The Legal Construction of Privacy and Data Protection' (2013) 29 CLSR 522, 525.
[125] Ibid, 525.
[126] *Peck v United Kindom,* App no 44647/98 (Judgment) (28 January 2003) para 62; *Perry v United Kingdom,* Merits, App no 63737/00 (Judgment) *(*17 July 2003) para 40; *P.G. and J.H. v the United Kingdom,* App no 44787/98 (Judgment) (25 September 2001) para 59.
[127] *Gaskin v United Kingdom*, App no 1044/83, (Judgement) (7 July 1989); *Antony and Margaret McMichael v United Kingdom*, App no 16424/90 (Judgment) (24 February 1995); *Guerra v Italy*, App no 14967/89 (Judgement) (19 February 1998); *McGinley & Egan v United Kingdom*, Applications nos. 21825/93 and 23414/94 (Judgment) (28 January 2000).
[128] *Rotaru* (n 117) para 83.
[129] *Leander* (n 118); *Segerstedt-Wiberg and others v Sweden*, App no 62332/00 (6 June 2006).
[130] *Klass and others v Germany*, App no 5029/71 (Judgment) (6 September 1978) para 55; *Leander* (n 118) paras 65–67; *Rotaru* (n 117) paras 59–60. See in detail: *Gaskin (*n 127); *Z. v Finland*, App no 22009/93 (Judgment) (25 February 1997).
[131] (such as the increased scope of data processing/storing by States).

At the end of the 20th century, new rules needed to be enacted and 'a new concept of privacy emerged known in some jurisdictions as "informational privacy"[132] and in others as the "right to informational self-determination". This concept led to the development of special legal regulations that provide personal data protection.'[133] Privacy concerns might have been where the development of the data protection field originated, but data protection acquired gradually a separate existence, becoming an interest worth of independent legal protection. The scope of data protection regimes has been said to be both broader and narrower than that of the right to privacy. It is narrower in the sense that it only concerns personal data processing; it is broader as it regulates processing of all personal data, rather than being restricted to private ones, and it applies even where the activity concerned does not interfere with the individual's privacy. At the same time, legal protections of privacy can also be framed as broader and narrower than data protection frameworks: their scope includes the processing of any kind of data that threaten privacy (not just personal ones), but again, only if the processing does infringe upon privacy.[134]

The right to privacy is meant to protect 'privacy' or 'private life'—the meaning of these two concepts being the subject of many debates, as has already been explained in Chapters I and II. When conducting a comparative analysis of the French and American systems in Chapter I, two different paradigms were highlighted behind 'the right to privacy': a freedom from interreference or a right to control. Traditionally and at first sight, in most human rights treaties the right to privacy has been understood as consisting of a general prohibition of unwarranted interference. However, closer examination reveals that the individual's 'ability to control' his private interests paradigm is also present.[135] These considerations raise the question what are the 'primary interests' underpinning data protection regimes and on which paradigms regulation of data processing practices has been based.

The core value protected by the right to privacy is 'privacy', which has been tied to other values, such as personhood, dignity or autonomy. These concepts are often invoked to justify the need to protect under the law various private interests. From this perspective, an individual's privacy should be protected because it enables personhood and autonomy. Privacy is therefore what could be called 'the primary interest' behind the right to privacy, while other values, even though linked, would qualify as 'secondary interests'. These additional values benefit from the legal protection of private interests, but they are not at the core of the right to privacy. The right to data protection may be understood as 'the regulation and organisation of the conditions under which personal data can be lawfully processed'.[136] The goal behind data protection frameworks is to regulate a specific activity: data processing. However, it is not very obvious why we want to regulate data processing and which values we are trying to protect through such regulation. The two main reasons behind most data protection regulations are 'to protect fundamental rights' and 'facilitate data

[132] German Federal Constitutional Court, *Volkszahlungsurteil*, BverfGE Bd. 65, S. 1ff.
[133] EU Agency for Fundamental Rights (FRA), Council of Europe, Registry of the European Court of Human Rights, and the European Data Protection Supervisor, *Handbook on European Data Protection Law* (2018) 18.
[134] Gellert/Gutwirth (n 124) 525.
[135] See relevant chapters.
[136] Gellert/Gutwirth (n 124) 524.

transborder flows'.[137] These two aspirations are very different from one another and will be analysed in turn.

Unregulated data processing is perceived as a threat to 'fundamental rights'. But which ones? The right to privacy comes first to mind. The first data protection regulations were enacted to strengthen the right to privacy to face the challenges posed by new technologies. The risks that unchecked data processing activities would pose on the privacy of individuals are obvious. Hence, data protection was initially conceived as a subset of the right to privacy- and in certain legal systems it is still understood that way.[138] As the ILC stated in its Report on Protection of Personal Data in 2006:

> There is a link between privacy and data protection. (…) From a philosophical and analytical perspectives, privacy conjures a variety of possibilities and ideas which may fall into one or cross-cut any of the following clusters: (a) spatial; (b) decisional; (c) informational and (d) privacy of communications.[139]

It then continued:

> The main focus [of the present proposal] is on the third cluster: the *informational subset of privacy*, which is concerned with the individual's *control* over the processing of personal information- its acquisition, disclosure and use, a concept usually referred to as 'fair record management'. It would be necessary to consider the rights that the data subject and users possess"[140]. "It [the present proposal] would address the protection to be afforded to the means of communication, that is to say, those aspects of the fourth cluster concerning privacy of communications *insofar as there is a connection in securing informational privacy*: the security and privacy of mail, telephony, email and other forms of ICTs.[141]

For the ILC, data protection issues therefore fall under a 'privacy cluster', more specifically informational privacy. This is the approach also adopted by the United States. The US legal system does not differentiate conceptually between 'protection of privacy' and 'data protection'. It regulates specific data processing practices under 'informational privacy laws'.

Privacy is therefore clearly a value behind data protection. However, not all data processing involves private data. There is an argument to be made that even if the data concerned is not intrinsically private, certain kinds of processing may still pose a threat to privacy.[142] Beyond that, however, certain data processing activities might not relate to privacy or private life at all. In this case, the question arises whether data protection frameworks are meant to protect values other than privacy and what are the types of harm that these regulations try to protect individuals from. First, non-discrimination is one of the values protected by data processing

[137] Eg. OECD Guidelines (n 22) Preface, GDPR (n 15) art 1.
[138] Eg. The United States.
[139] ILC Report (n 42) para 13.
[140] Ibid, para 15.
[141] Ibid, para 16. (emphasis added).
[142] Position taken by the ECtHR.

regulations- either directly by specific provisions,[143] or as a result of other principles. Liberty is another value, forming the legal basis, for example, of the French data protection regime.[144] It has also been referred to by scholars as such.[145] For some other scholars, the individual's personhood[146] is at risk, and in the EU 'data protection is a fundamental right anchored in interests of dignity, personality, and self-determination'.[147] These statements seem to indicate that data protection regimes pursue different 'primary values', not only privacy but also human dignity and personhood. According to the Handbook on European Data Protection, prepared by the Council of Europe, the European Data Protection Supervisor and EU Agency for Fundamental Rights, the right to privacy and the right to data protection "both strive to protect similar values, i.e. the autonomy and human dignity of individuals"[148]. This statement is not wrong per se, but one needs to be mindful that the values have different places depending on each right. When it comes to data protection regimes they are at their core; but with respect to the right to privacy (as explained above) they are only secondary. They may be bolstered by the respect of privacy, but they are not the primary objective pursued by the right to privacy.

The second reason behind data processing regulation is the need to facilitate transborder data flows. In this respect, the rationale for legal regulation, being market-driven, is completely different from the desire to protect fundamental human rights.[149]

Having inquired about the values pursued by data processing regulation, the analysis now turns to the conceptual paradigms underpinning such regulation. As mentioned, according to the European Handbook both the right to privacy and the right to data protection protect the same values (which we only partly agreed with) "by granting them a *personal sphere* in which they can freely develop their personalities, think and shape their opinions".[150] This vocabulary of a 'sphere' in which individuals can be 'free' points to the paradigm of 'freedom from interference', which was discussed in Chapters I and II.

However, closer examination of data protection regimes reveals that these are not framed under this paradigm of 'freedom from interference' but are rather based on the paradigm of control over one's own data. Many of the FIPs, such as the right to access personal data and the right to request rectification, clearly grant individuals control over their personal data. Additionally, other common principles such as 'Lawfulness and Fairness', 'Openness, 'Purpose Specification' or 'Security' seem to illustrate the paradigm of control. The requirements for data processors to process information in a fair and lawful way, to be transparent about their activities, to specify their purposes and not deviate from it do not resonate with the conception of 'a sphere of freedom'. Rather, they allow individuals to

[143] Eg, UN Guidelines (n 21) 5.
[144] Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés**,** repealed by Loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles**.**
[145] Gellert/Gutwirth (n 124) 524: "Aware of the sensitive and potentially threating nature of such a process [processing of personal data], it [data protection] has put in place a number of qualitative thresholds (…) and procedural safeguards (..) which are deemed sufficient to protecting the individual's *liberty* when data about him/her are processed". (emphasis added).
[146] Paul Schwartz/Karl-Nikolaus Peifer, 'Transatlantic Data Privacy Law' (2017) 106 Geo. L. J. 115, 127.
[147] Ibid, 123.
[148] Handbook on European Data Protection Law (n 133) 19. (emphasis added).
[149] To read about the difference between fundamental and human rights See Van der Sloot (n 107) 12-19.
[150] Handbook on European Data Protection Law (n 133) 19. (emphasis added).

manage their personal information, or at least to know how their data is being processed and what is to be expected from such processing. In that respect, data processing practices should not conflict with the data subject's expectations.[151] In terms of formulation, data protection frameworks are not prohibitive in nature. If anything, they accept the existence of data processing activities. Rather than forbidding such practices, they seek to regulate them. Checks and balances are put in place,[152] which empower the individual to know the modalities under which his/her personal data is being processed and grant him/her the ability to manage it. The three goals behind data protection mentioned above, namely to regulate data processors actions, to grant data subjects rights over their data, and put in place enforcement mechanisms, show a pattern of 'control' or at least of 'individual empowering' when it comes to personal data, and do not seek to delimit a sphere 'free from interference'.

Chapter I of this dissertation developed the different conceptual approaches the United States and France took on regulating privacy. The following section will also proceed to a comparative analysis, but this time between European and US data protection legal systems.

Part II. Comparative Analysis between the European and US systems

This section looks at the European and the US system on data protection in more details. It also compares and contrasts the two, highlighting the different approaches these two main actors take on regulating data processing practices. One might wonder why special attention is granted specifically to these two Western legal systems, as data protection regulations are of course found beyond these two systems.[153] There are several reasons behind this choice. First, European legislators have been at the forefront of developing the data protection field, both timewise, as one of the first regions to start developing this new legal field (CoE adopted Convention No 108 in 1981), and as they have established rather comprehensive and robust legal standards since then. These 'European standards' have in turn influenced considerably many domestic systems around the world. The globalisation of Convention No 108 exported these 'European principles' outside European borders,[154] while legal standards set by the European Union have also been used as a starting point for the development of many data privacy regimes around the globe.[155] According to Schwartz and Peifer, the regime of the EU on data protection has been 'stunningly influential, most of the rest of the world follows it',[156] European standards becoming 'the norm in most parts of the world with data privacy laws'.[157] The 'adequacy requirement' is a good example of the influence the European framework on data protection has had on other domestic regimes. Even though the same principle can be found in other instruments such as Convention No 108[158] and the UN

[151] Ritter/Hayes/Judy (n 80) 88.
[152] Handbook on European Data Protection Law (n 133) 19.
[153] See: Graham Greenleaf, *Asian Data Privacy Laws* (2014).
[154] Greenleaf, 'Shererezade' (n 58) 36.
[155] LA Bygrave, *Data Privacy Law* (n 26) xxvi.
[156] Schwartz/Peifer (n 146) 122.
[157] Graham Greenleaf, *Asian Data Privacy Laws* (n 153) 52.
[158] art 12.

Guidelines[159], the EU is the only one implementing it in practice.[160] This has strongly encouraged (not to say, coerce) other countries wanting to exchange data with Europe to adapt and update their own legislations to become compatible with European standards and meet the adequacy requirement.

The United States, on the other hand, does not have the same kind of influence outside its borders. Still, it does hold a major place in both the world economy and in security matters, while inquiring into its legal framework is useful as it takes a completely different approach to the European one in regulating data processing. In that respect, and exactly because of their technological, economic and political dominance, the US government and US corporations have been able to resist adapting their approach in data regulation to different ones for a long time.[161] Hence, comparing the two systems and understanding their differences and the distinctive approaches they take on the same issues is instrumental in understanding the international legal discourse on data processing. This will not only clarify the debate and help find a way forward,[162] but is also essential in any conversation about international regulation of surveillance activities and privacy concerns.

Section 1. Data Protection in Europe

Both the right to privacy and the right to data protection are recognized as fundamental rights in Europe, enshrined in the European Convention on Human Rights[163] and the EU Charter of Fundamental Rights.[164] These two instruments are the two pillars of fundamental rights protection in Europe. They have adopted an 'omnibus approach' to regulating data processing. This means that the scope of such laws is very broad. They tend to cover all kinds of personal data, processed by private and/or public actors, no matter the area of the economy this takes place in. Specific sectorial regulations do exist, but these come as additional protection for certain types of data[165] or in certain fields[166], and they do not constitute the very basis of protection (like, for example, in the United States system)[167]. Absent any specific, sectorial regulation, a general omnibus regime is already in place 'by default', as a safety net.

A. Regulatory Actors

A.1. Council of Europe

[159] art 9.
[160] De Hert/Papakonstantinou (n 4) 286, footnote 41.
[161] Greenleaf, 'Shererezade' (n 58) 38-39. (even though "the international legal environment for their continuing to do so is slowly becoming more hostile and complex to navigate" ibid).
[162] Schwartz/Peifer (n 146) 157. (about EU and US systems)
[163] ECHR (n 108) art 8.
[164] EU Charter (n 7) art 7 and 8.
[165] Eg: GDPR (n 15) art 9: "Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited."
[166] For example, the field of telecommunications is often the object of additional specific regulation: "Article 1 subs 2 with Recital 4 of Directive 2002/58/EC of 12 July 2002, 12 July 2002, 2002 OJ (L 201) 37; GDPR (n 15) art 95 with Recital 173."
[167] More on infra.

As discussed in Section 1 of this chapter, the Council of Europe is an important actor in the data protection field through the regime established under Convention No 108 and its Additional Protocols, as well as in the context of the dynamic interpretation of Article 8 of the ECHR by the European Court on Human Rights, extending the scope of protection of this provision to personal data.[168] The Convention No 108 and its Protocols have now been signed and ratified by 55 countries, including by many non-European states.[169] This opening of the Convention to States outside the European borders transformed it to a global agreement. It only regulates processing of personal data, but it is binding upon all the countries that have ratified it- which is rare in data protection.[170]

A.2. European Union

Contrary to the ECHR, the European Union regime draws a clear distinction between privacy and data protection regimes. The 2000 Charter of Fundamental Rights contains a provision specific to data protection, additional to the 'traditional protection of privacy'.[171] The Charter is a binding constitutional document of the EU[172] and its Article 8 states:

> 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.

The establishment of a 'constitutional' right to data protection in the EU Charter is crucial. Firstly, it specifically details what a 'right to data protection' entails in practice: it grants precise rights to individuals (right of access to their personal data and right to have it rectified) and sets clear standards that have to followed by data processors (both in the public and private sectors). Also, as mentioned in the previous section, data protection laws often protect data other than private ones.

The Treaty on the Functioning of the European Union (TFEU) also recognizes the right to personal data protection.[173] The European Court of Justice (ECJ), in *Volker under Markus Schecke and Eifert*, held that personal data – defined as any information relating to an

[168] For the case-law by the ECtHR on the protection of personal data in its entirety: See CoE, 'Case Law of the European Court of Human Rights Concerning the Protection of Personal Data' (15 November 2017) <https://rm.coe.int/case-law-on-data-protection/1680766992> accessed 12 September 2019. See also Chapter II.
[169] Uruguay (2013), Senegal (2016), Mauritius (2016), Tunisia (2017), Cabo Verde (2018), Mexico (2018), Morocco (2019), Argentina (2019). <https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108/signatures?p_auth=cN6J4BCa> accessed 20 June 2019.
[170] Gellman (n 1) 154. For example: the OECD Guidelines are not limited to personal data, but on the other hand they are not binding.
[171] art 7.
[172] Since the Treaty of Lisbon amending the Treaty on European Union and the Treaty establishing the European Community (signed 13 December 2007, entered into force 1 December 2009).
[173] Consolidated version of the Treaty on the Functioning of the European Union, Official Journal C 326, 26/10/2012 P. 0001 – 0390, art 16.

identified or identifiable individual[174] – fall under the concept of 'private life'.[175] The Court made clear that individuals are protected under this regime even in the absence of harm[176] and even if the data being processed is not sensitive.[177] Contrary to the protection offered by the ECtHR through the interpretation of Article 8 of the ECHR, any personal data (and not exclusively private ones) is protected under the Charter. The ECJ's opinion is that the mere fact of processing personal data poses a risk to the rights of individuals, and therefore it should only be done if it is allowed by law, and if the process is regulated.[178] This neat separation between a 'right to data protection' and a 'right to privacy' reflects, and respects, the different approaches taken by different EU Member States. While Belgium has always linked data protection to questions of privacy,[179] other countries like France or Germany have not done so.[180] Lacking specific privacy guarantees in their constitutional apparatus, these countries have had to ground data protection standards in other principles, such as the right to liberty[181] or human dignity.[182]

One of the main points of reference when it to comes to the European data protection framework is the General Data Protection Regulation (GDPR),[183] which replaced the renowned Data Protection Directive of 1995.[184] The GDPR is centred around the Fair Information Practices principles. The 1995 Directive was one of the pillars of data protection in Europe. It had a huge influence on other systems around the world, because of how detailed the standards of protection were and because (as already discussed) of its 'adequacy requirement'. One of the objectives of the Directive was to ensure the same legal protection over personal data for individuals, regardless of their national citizenship.[185] Another major goal was to do away with obstacles to data flows between the EU Member States. That goes directly to the overarching aim of the European Union which was to create an economic and monetary union, in which internal borders would not be considered as hurdles. The discrepancy between different national data protection regulations constituted a complication to the transborder flow of data,[186] and therefore the different national

[174] Directive 1995 (n 15) art 2(a); GDPR, art 4(1).
[175] CJEU, Joined Cases C-92/09 and C93/09, *Volker under Markus Schecke and Eifert* [2010] ECR I-11063, para 52.
[176] The protection does not depend on whether "the inclusion of the information in question (…) causes prejudice to the data subject" in Case C-131/12, *Google Spain v AEDP* [2014] ECR 317, para 96.
[177] ECJ: "to establish the existence of an interference with the fundamental right to respect for private life, it does not matter whether the information in question (…) is sensitive or whether the persons concerned have suffered any adverse consequences on account of that interference" in C-362/14, *Schrems v Data Prot. Comm'r* [2015] ECR 650, para 87.
[178] Schwartz/Peifer (n 146) 127.
[179] Eg. Until 2018, the 'Privacy Act of 1992' (8 December 1992 : Loi relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel) regulated data processing activities. It has now been repealed by 'The Act of 30 July 2018 on the protection of natural persons with regards to processing of their personal data'.
[180] Paul de Hert/Serge Gutwirth, "Privacy, Data Protection and Law Enforcement. Opacity of the Individual and Transparency of the Power" in Erik Claes, Antony Duff and Serge Gutwirth (eds), *Privacy and the Criminal Law*, Intesentia 2006, 61, 82.
[181] France: Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés**,** repealed by Loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles**.**
[182] Germany : Grundgesetz für die Bundesrepublik Deutschland [GG] [Basic Law] May 23, 1949, BGBL. 1, arts. 1(1), 2(1).
[183] GDPR (n 15).
[184] Directive 1995 (n 15).
[185] Ibid, op (8).
[186] Gellman (n 1) 156.

regulatory schemes needed to be harmonized.[187] This led the European Commission to propose the enactment of the 1995 Directive. These two main objectives reflect the two aspects of data protection discourse mentioned before: one is about regulating domestic data processing activities by private and/or public data processors and their impact on individuals' rights; the other concerns transborder data flows and how to make them smoother. The difficult exercise of balancing these two interests is at the core of the legal debate surrounding data regulation. The 1995 Directive includes roughly the same 'Fair Information Principles" found in the CoE Convention No 108 and the OECD Guidelines. It contains rules applying to personal data in general and does not set different protection levels or rules depending on the industry in which the processing takes place.[188] Additional safeguards regarding the processing and use of sensitive data are included,[189] as well as for data collected for direct marketing.[190] This is a typical illustration of the kind of 'omnibus architecture' that characterizes the European data protection system.

In January 2012, the European Commission announced that a reform of the Directive was underway in order 'to strengthen online privacy rights and boost Europe's digital economy'.[191] The goals were to increase private companies' responsibilities in processing data, to grant more rights to citizens[192] and therefore offer a clearer and harmonised approach to data protection.[193] After long and difficult negotiations,[194] a political agreement was finally reached in December 2015 and voted in by the Council and Parliament in the beginning of 2016. In terms of content, the GDPR is centred around the Fair Information Practices principles. It grants very detailed protection to personal data and to data subjects.[195] The reform aims to provide tools for 'gaining control of one's personal data'.[196] It intends to do so through a right to be forgotten, an easier access to one's data, a right to data portability, the right to know when one's data has been hacked, stronger enforcement of the rules and through embedding data protection by design and by default.[197] The GDPR reiterates that 'the protection of natural persons in relation to the processing of personal data is a

[187] Directive 1995 (n 15) art 4. Side note: Harmonization of standards is different than 'uniformity of laws'- it "calls for an increased standardization" *in* Gellman (n 1) 156. Harmonization does not eradicate 'national diversity', it sets "minimum standards around which each Member State must enact enabling legislation" *in* Ritter/Hayes/Judy (n 80) 94.
[188] Ritter/Hayes/Judy (n 80) 94.
[189] Directive 1995 (n 15) at (34) and (70).
[190] Ibid, (30) and art 14(b): Right for individuals to "object, on request and free of charge, to the processing of personal data relating to him which the controller anticipates being processed for the purposes of direct marketing".
[191] European Commission, Press Release 'Commission proposes a comprehensive reform of data protection rules to increase users' control of their data and to cut costs for businesses' (25 January 2012) <http://europa.eu/rapid/press-release_IP-12-46_en.htm> accessed 4 July 2019.
[192] Edward R Alo, 'EU Privacy: A Step Towards Global Privacy" (2014) 22 Mich. St. Int'l L. Rev. 1095, 1117.
[193] Ariadna Ripoll Servent, 'Protecting or Processing? Recasting EU Data Protection Norms' in W.J. Schunemann and M-O Baumann (eds), *Privacy, Data Protection and Cybersecurity in Europe* (Springer 2017) 119.
[194] For more details on this See: Ibid, 120-124.
[195] Alo (n 192) 1119.
[196] European Commission, Fact Sheets (21 December 2015) <http://europa.eu/rapid/press-release_MEMO-15-6385_en.htm> accessed 6 July 2019.
[197] Ibid. For a detailed analysis of the GDPR see: Paul Voigt and Axel von dem Bussche, *The EU General Data Protection Regulation – A Practical Guide* (Springer 2017).

fundamental right'.[198] The most common 'Fair Information Principles' can be found in its Article 5.[199]

One of the main changes of the GDPR as compared to the 1995 Directive is the definition of what constitutes 'personal data'. It still defines personal data as 'any information relating to an identified or identifiable natural person',[200] but the list of what constitutes an 'identifiable person' has now increased.[201] The other big change is the requirement to have the consent of the individual concerned before processing any of his personal data. This 'opt-in' requirement had a major impact on businesses.[202] The move from a Directive to a Regulation illustrates the increased focus on data protection and privacy issues online. A Directive as a legislative tool in EU law has a harmonizing goal and it is not directly binding as it first needs to be transposed and implemented in domestic legislations. That is not the case for EU regulations, which are directly binding and impose directly enforceable obligations.[203] For the EU institutions to purposefully move from a Directive format to a Regulation shows a desire to regulate more strongly data processing and to better protect data subjects, especially in the field of consumer protection which is usually only regulated through directives.[204] This change emphasises how fundamental data protection became as a right.

One important factor to highlight, in the context of this study, is that the GDPR does not apply to national security activities. Its Recital 16 states that:

> This Regulation does not apply to issues of protection of fundamental rights and freedoms or the free flow of personal data related to activities with fall outside of the scope of Union law, such as activities concerning national security.
> This Regulation does not apply to processing of personal data by the Member States when carrying out activities in relation to the common foreign and security policy of the Union.[205]

It is still vital to look into the GDPR. It is a significant piece of legislation, which is now 'widely regarded as a privacy law not just for the EU, but for the world'[206] and the standards it enshrines are the embodiment of the European understanding of legal data protection. Because of its adequacy requirement and its transnational reach, the GDPR massively

---

[198] Recital 1.
[199] GDPR (n 15) art 5(a) 'lawfulness, fairness and transparency'; 5(b) 'purpose limitation; 5(c) 'data minimisation'; 5(d) 'accuracy'; 5(e) 'storage limitation'; 5(f) 'integrity and confidentiality'; Article 5(2): 'Accountability' and Recital 39.
[200] GDPR (n 15) art 4(1).
[201] According to the GDPR: "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" in art 4(1) (emphasis added).
[202] We won't go in more details in here because it not necessary for the purpose of this study but, as a side note, this fits with a bigger trend to broaden the scope of the definition of personal data- since the very first frameworks in the 70s: See van der Sloot (n 107) 8.
[203] In this case, GDPR imposes for the first time enforceable standards directly on data processors.
[204] Schwartz/Peifer (n 146) 129.
[205] (emphasis added).
[206] Paul Schwartz, 'Global Data Privacy: the EU Way' (forthcoming 2019) 94 NYU Law Review, 3.

influences not only the development of the field in general, but its overall standardization. As Cunningham writes: "notwithstanding international treaties or conventions, the EU endeavors to maintain its prominence as the tip of the data protection spear".[207]
In 2016, the Police and Criminal Justice Data Protection Directive[208] was enacted. This Directive solely regulate processing related to security issues and is another part of the EU "data protection reform package" undertaken by the Commission in 2016.[209]

B. Analysis

The importance granted to data protection is illustrated by the fact that it is recognised as a fundamental right by the EU Charter and is now regulated by a Regulation.[210] Individuals are at the core of the European system on data protection. Schwartz and Peifer refer to a 'rights-focused legal discourse centred on the individual whose data is processed'.[211] The main goal of the European data protection framework is to protect data subjects, by regulating data processing and granting them specific rights. The whole protection is framed in the language of human rights.[212] In the words of the European Commission, 'the EU data protection legislative framework is a cornerstone of the European *human-centric* approach to innovation'.[213] This conception of data protection again raises a question about how the link between the right to privacy and data protection is understood in Europe.
The Council of Europe initially tied the two matters together.[214] Convention No 108, for example, has clear references to the right to privacy in its preamble[215] and its Article 1.[216] As explained *supra*, Article 8 of the ECHR has been interpreted by the ECtHR as including

[207] McKay Cunningham, 'Complying with International Data Protection Law' (2016) 84 U. Cin. L. Rev. 421, 428.
[208] Directive (EU) 2016/680 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 by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, *OJ L 119, 4.5.2016, 89–131.*
[209] The EU Data Protection Landscape is composed of the GPDR, the Data Protection Law Enforcement Directive and the Data Protection Regulation for EU Institutions and Bodies (Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC, OJ L 295, 21.11.2018, p. 39-98. It became applicable on 11 December 2018).
[210] For a detailed study on the 'fundamentalisation of data protection' See van der Sloot (n 107) and Stefano Rodotà, 'Data Protection as a fundamental right' in Serge Gutwirth et al., *Reinventing Data Protection?* (Springer 2009).
[211] Schwartz/Peifer (n 146) 122.
[212] Ibid, 127.
[213] European Commission, 'Communication from the Commission to the European parliament and the Council: Data protection rules as a trust-enabler in the EU and beyond – taking stock' (24 July 2019) COM (2019) 374 final, 2 (emphasis added).
[214] The very first frameworks on data processing in Europe were both looking to protect privacy of individuals: Council of Europe, Committee of Ministers, Resolution 73(22) on the protection of the *privacy of individuals* vis-à-vis electronic data banks in the private sector (adopted 26 September 1973) and Council of Europe, Committee of Ministers, Resolution 74(29) on the protection of the *privacy of individuals* vis-à-vis data banks in the public sector (adopted 20 September 1974).
[215] "Considering that it is desirable to extend the safeguards for everyone's rights and fundamental freedoms, and in particular the *right to the respect for privacy*, taking account of the increasing flow across frontiers of personal data undergoing automatic processing" (emphasis added)
[216] "The purpose of this Convention is to secure (…) for every individual (…) respect for his rights and fundamental freedoms, and in *particular his right to privacy*, with regard to automatic processing of personal data relating to him ('data protection')." (emphasis added).

protection of *private* personal data. However, this attitude evolved over time and they are now considered two related, but distinct rights.[217] There is still a debate, though, on the position of the EU on this question. Certain scholars believe that the EU initially linked data protection to the right to privacy and only gradually separated the two fields, while others argue that they have always been conceptualized as different matters.[218] Where the 1995 Directive mentions the right to privacy several times, including in defining its object,[219] the GDPR does not mention it even once. In 2000, when the Charter of Fundamentals Rights was enacted, the choice was made to include two separate provisions.[220] It therefore seems that- whatever the initial position was- the EU legal framework now considers data protection and the right to privacy as distinct matters, independent from each other.[221] The main focus of data protection regimes in Europe (both in the EU and the Council of Europe) are individuals and how to best guarantees their rights.

Section 2. Informational Privacy in the United States

In Chapter I concerning the approach of the United States to legally protect private interests, it has been mentioned that Americans show a certain 'cautiousness' towards governmental involvement in their lives. This cautionary stance can be traced back to the Revolutionary era, when colonial authorities used their power abusively to- among other things- collect, control and misuse private information about individuals.[222] This general distrust of government led to a 'hands-off approach'[223] to legislation, including when it came to regulating data processing activities. Federal government intervention is generally only accepted when a particular need arises, usually created by or because of the market.[224] The sectorial methodology used to grant legal protection to private interests can also be found in what is called 'information privacy'. The legal standards imposed on data processing activities were enacted to respond to specific needs and pressures in specific industries.[225] There is no 'overall' fundamental right to data protection (or data/informational privacy, depending on which terminology is used). Rather, different guarantees are granted depending on the kind of data at stake. This varies depending on the specific industry or field (e.g. health services[226], credit,[227] finances[228]), the data subject (e.g. children[229]) or the sector (e.g. private or public[230]). In addition to federal legislation, States have also the power to regulate activities taking place inside their borders, resulting to hundreds of independent

[217] Handbook on European Data Protection Law (n 133) 18.
[218] van der Sloot (n 107) 6.
[219] Directive 1995 (n 15) art 1: "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" (emphasis added).
[220] EU Charter (n 7) art 7 and 8.
[221] To read more on the European courts' opinions on this: See Kokott/Sobotta article (n 9).
[222] Alo (n 192) 1116.
[223] Ibid.
[224] Ibid.
[225] Ritter/Hayes/Judy (n 80) 96.
[226] The Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936. (hereinafter HIPAA).
[227] Fair Credit Reporting Act, Pub.L. 114-38, 15 USC § 1681 (2012). (hereinafter FCRA).
[228] Gramm-Leach-Bliley Act of 1999, Pub. L. No. 106-102, 113 Stat. 1338, (codified at 15 U.S.C. §§ 6801-–09). (hereinafter GLBA).
[229] Children's Online Privacy Protection Act of 1998, 15 U.S.C. §§ 6501–06. (hereinafter COPPA).
[230] Privacy Act, Pub. L.93-579, 5 USC §552a (1994).

laws intensifying the sectorial approach and making it very difficult to navigate for companies and individuals.[231]

A. Frameworks

As already mentioned, no distinct legal regime regulating data processing in the United States exists. The different regulatory schemes are understood as falling under the 'privacy umbrella'. This explains the terminology of 'informational privacy'. The frameworks detailed here are therefore only the main ones regulating (exclusively or not) processing of certain data.

At the constitutional level, there is no articulated right to informational privacy. There is therefore no general constitutional regulation of the private sector. The federal government is not bound to actively set up conditions to guarantee respect of fundamental rights.[232] That said, there are two provisions in the Constitution of the United States that grant some protection to individuals' information: the Fourth Amendment and the Due Process Clause of the Fourteenth Amendment. Both, however, are a poor fit to regulate effectively modern data processing activities.

Firstly, the Fourth Amendment only grants a right to individuals to 'be secure in their persons, houses, papers and effects against unreasonable searches and seizures'. This therefore does not concern any kind of data processing activities by governmental authorities other than search and seizure. Any processing and use of information found in routinized databases for example is not covered- even if used for delivering public services.[233] On top of that, the Fourth Amendment only looks at the initial search or seizure and its 'reasonableness', and does not protect further use of such information.[234] The Supreme Court also stated that information is not protected by the Fourth Amendment when the individual has provided it to a 'third party', e.g. to his/her banking institution.[235] For its part, the Fourteenth Amendment has been used by the Supreme Court as the legal basis to declare the existence of a general right to 'informational privacy'.[236] In *Whalen v Roe* the Court stated:

> We are not unaware of the threat to privacy implicit in the accumulation of vast amounts of personal information in computerized data banks or other massive government files. […] The right to collect and use such data for public purposes is typically accompanied by a concomitant statutory or regulatory duty to avoid unwarranted disclosures.[237]

---

[231] Ritter/Hayes/Judy (n 80) 96.
[232] Schwartz/Peifer (n 146) 132.
[233] Ibid, 133.
[234] This is the so-called 'first-party doctrine', for more on this and its link on data mining See: Paul M Schwartz, 'Regulating Data Mining in the United States and Germany: Constitutional Courts, the State, and New Technologies' (2011) 53 Wm & Mary L. Rev. 351, 356.
[235] 'Third-party doctrine': in these cases, individuals cannot claim a 'reasonable expectation of privacy-' requirement necessary to enjoy the protection granted by the 4th Amendment. *Smith v Maryland*, 442 US 765 (1979) at 744.
[236] *Whalen v Roe* 429 US 589 (1977) 605-606.
[237] Ibid, 605.

It then went on to recognize that an individual's 'interest in avoiding disclosure of personal matters' is an aspect of the right of privacy[238]. This finding has fuelled extensive debate.[239] The classic privacy torts[240] (intrusion upon seclusion, appropriation of name or likeness, publicity given to private life, and publicly placing a person in false lights) are also not appropriate to deal with data. Not only were they established before the invention of computers and new technological developments such as Big Data analytics, social media or cloud storage, they also don't address problems caused by mass collection and use of personal information.[241] Certain statutory regulations specifically concerning data processing activities exist. As mentioned before, these follow a sectorial approach, referencing a 'fragmented, cross-governmental, and industry-specific regulation. (…) the laws are (…) narrowly tailored, addressing particular elements of personal information or discrete uses of discrete data'.[242] There are statutes at the federal and state levels. At the federal level, statutes regulate data processing occurring in health services,[243] credit reporting,[244] financing,[245] and video rentals.[246] A special statute exists regulating children's' data[247] and another that regulates personal information handling by federal agencies.[248] A comprehensive legislation would harmonize the field, but Congress seems resolved not to go down that route and most commentators agree that this approach is unlikely in the near future.[249]

In the United States, if the plaintiff cannot bring evidence of concrete harm, there is no 'case or controversy', which means the judicial system cannot offer any redress.[250] This makes it quite difficult for individuals whose data is mishandled to find judicial redress. As detailed in Chapter I dedicated domestic privacy laws, the US legal system always had difficulty conceptualizing what kind of activities could harm private interests, especially what kind of information practices would amount to a 'concrete injury'[251] worth of legal protection- and therefore recovery.[252]

---

[238] Ibid, 606.
[239] See Paul M Schwartz, 'Privacy and Participation: Personal Information and Public Sector Regulation in the United States' (1995) 80 Iowa L. Rev. 553, 574-82." One court openly expressed doubted if the Whalen interest was anything more than a 'mere dicta' (Am. Fed'n of Gov't Emps, AFL-CIO v Dep't of Hous. & Urban Dev. 118 F.3d 786, 791 (D.C. Cir. 1997) and the Supreme Court has not pronounced itself to clarify the situation: in *Nasa v Nelson* it "assume without deciding" the existence of the Whalen interest (*Nasa v Nelson*, 526 US 134 (2011) 138) ; while Judge Scalia explicitly stated that in his opinion "there was no constitutional right to informational privacy" (syllabus p 4).
[240] Restatement (Second) of Torts, §§ 652B (Intrusion Upon Seclusion), 652C (Appropriation of Name or Likeness), 652D (Publicity Given to Private Life), 652E (Publicly Placing Person in False Lights) (1977).
[241] Gellman (n 1) 134.
[242] Cunningham (n 207) 422-3.
[243] HIPAA (n 226).
[244] FCRA (n 227).
[245] GLBA (n 228).
[246] Video Privacy Protection Act, 18 USC § 2710 (2012). (hereinafter VPPA).
[247] COPPA (n 229).
[248] Privacy Act (n 230).
[249] Cunningham (n 207) 425.
[250] *Clapper v Amnesty Int'l USA*, 133 S. Ct. 1138, 1155 (2013).
[251] For example, the Supreme Court in *Spokeo v Robin* case reaffirmed the need to prove the existence of an 'injury in fact', 'concrete and particularized' *Spokeo, Inc v Robins*, 126 S. Ct. 1540, 1550 (2016).
[252] Schwartz/Peifer (n 146) 134-5.

B. Analysis

The US sectorial approach to informational privacy leads to a confusing patchwork of multiple regulations, both at the federal and state levels. The *laissez-faire* system relies on a combination of a 'disjointed mix of state and local law, federal legislation, executive orders, and self-regulation'[253]. As a general rule, US privacy laws are usually reactive.[254] The momentum behind a legislative initiative to regulate certain data processing activities needs proof that such regulation is really necessary: the 'presence of a horror story, that is, convincing evidence of abusive data practices'.[255]

In the United States, the individual is conceived as an actor engaged in a specific market relationship. This is shown by the vocabulary used to identify the individual whose information is protected: 'consumer',[256] 'customer',[257] or 'subscriber'[258]. The importance of the marketplace discourse has consequences: because the individual is seen as a player in a market relationship, he is not granted a fundamental right to data privacy as such, but only certain guarantees in the context of that specific relationship. In participating in such activity, the individual agrees to exchanging his personal data in exchange for a service. As Schwartz and Peifer write: 'In this legal universe, the rhetoric of bilateral self-interest holds sway. Personal information is another commodity in the market (…) The focus of information privacy in the United States is policing fairness in exchanges of personal data'.[259] Under US law, consumers are to be protected from blatant market failures, but in general the system favours data processors. This is not a legal system where the centre of protection is the individual whose data is affected. Regulatory schemes are conceived to palliate certain abusive market practices, but overall there is a general trust that the market will self-regulate and that technological companies should not be too restrained in order to keep them stable and growing.[260]

Section 3. Comparative Analysis

The analysis above already reveals that the EU and the United States have different views on how to regulate data processing practices and why they should regulate such activities in the first place. After enumerating the main differences between the two systems (1), and the problems they cause (2), an analysis of the paradigms hidden behind these two types of data regulatory schemes will take place (3).

---

[253] Cunningham (n 207) 421.
[254] Lauren Movius/Nathalie Krup, 'US and EU Privacy Policy: Comparison' (2009) 3 International Journal of Communication 169, 174.
[255] Schwartz/Peifer (n 146) 136. To read more on how 'external events' jump-start policy initiatives: See Priscilla M Regan, *Legislating Privacy: Technology, Social Values, and Public Policy* (1995) 199.
[256] FCRA (n 227); GLBA (n 228); VPPA (n 246). Another example is the report issued in 2012 by the White House which concentrated on 'consumers trust' in technologies companies: White House, 'Consumer Data Privacy in a Networked World' (February 2012) 1.
[257] Telecommunications Act 47 USC § 222(a) (2012).
[258] Cable Act 47 USC §551(a) (2012).
[259] Schwartz/Peifer (n 146) 132.
[260] Ibid, 137-8.

A. Differences

The biggest and most obvious difference between the two systems is their approach to regulatory schemes: sectorial or omnibus. But this is not just a disagreement on the form. Behind this, lies a very different conception of data regulation. The EU envisions fundamental rights protecting the respect of private life and personal data,[261] with governments having a duty actively participate in setting up such standards and controls. Omnibus legislative frameworks are best suited to achieve this vision. Contrariwise, in the United States privacy is understood as a commodity that individuals are free to trade in exchange of specific services.[262] Sometimes certain guarantees are necessary to palliate certain needs, in specific sectors. Government is seen as a 'latent rule maker of last resort'.[263] In turn, this leads to different conceptions of the 'individual as a bearer of legal interests'.[264]

The EU conceptualizes individuals as bearers of fundamental rights, whose personhood is essential and of which they are in control. In the United States, the individual is identified as a consumer of a service, who needs to be protected from market unfairness.[265] The object of protection is also not the same. There is no doubt in the EU what personal data means: '"personal data" means any information relating to an identified or identifiable natural person ("data subject")'.[266] In the United States, on the other hand, there is no overall definition. Indeed, different legislations contain different definitions.[267] Using (personal) information to boost commerce is more important in the United States- with its consumer driven economy- than in the EU.[268]

At the core of the US system is the principle of free information flow and the freedom to process any data without restrictions, unless a specific statute regulates or forbids it. There is no equivalent to the constitutional European fundamental right to data protection, no 'safety net' of a general provision or 'omnibus law'- which means that many data fall outside of the scope of these specific regulations and are therefore not protected in any way. Their processing is not guided by any legal requirements.[269] In the United States, there is also no requirement for data processors to operate on 'a legal basis'. Data processors do not need to obtain the individual's consent or to establish a contract. The only thing they are required to do is to follow any specific regulatory scheme that might apply to the kind of data they are processing. The opposite is true for the European system. European data protection laws require a legal basis for any type of processing practices (whatever the industry or sector).[270]

---

[261] EU Charter (n 7) arts 7 and 8.
[262] Alo (n 192) 1115.
[263] Movius/Krup (n 254) 174.
[264] Schwartz/Peifer (n 146) 119.
[265] For a detailed comparison of 'EU's data subject and US privacy consumer across three dimensions: constitutional protections, statutory protections and relative legal status compared to the entities that collect and process personal data See: Ibid, 121 ss.
[266] GDPR (n 15) art 4.
[267] For example: the VPPA (n 246) defines it as "information which identifies a person" para 2710; while the GLBA (n 228) defines 'personally identifiable financial information' as 'non-public personal information' para 6809(4)(A)
[268] Movius/Krup (n 254) 172.
[269] Schwartz/Peifer (n 146) 137.
[270] Eg, GDPR (n 15) art 6.

Obtaining the individual's consent is one of the cornerstones of the system[271] and is considered as an 'expression of individual self-determination'.[272]

At the heart of the European data protection system is the data subject. The European data protection regime follows the main FIPs, which as discussed previously,[273] embody the paradigm of 'control' rather than that of 'freedom from interference'. The focus is on the individual. The United States on the other hand is looking to correct certain market failures. The focus is on the abusive practices, such as deception or unfairness, that could potentially harm individuals. Information privacy laws respond to specific issues in specific industries, they do not grant an overall system of protection such as the one found in the EU. In the US system, legal action is conceived as necessary to protect individuals from an undesirable external action. The first chapter of this thesis developed the idea that privacy protection in the United States is centred around the notion of protecting individuals from undesirable interference with their private lives. The focus of the regulatory scheme is on the interference itself and how to minimize or avoid its negative impact on individual's enjoyment of their right to privacy. This paradigm seems to confirm itself when analysing US informational privacy laws. Regulation of data processing activities are understood as being a subset of general privacy laws in the United States, it therefore makes sense that the same theoretical paradigm is found.

B. Problems

The different approaches taken by the United States and the EU lead to situations where identical information might be subject to different regulatory controls, potentially generating regulatory conflicts. An individual whose data is processed is therefore protected differently depending which legal system applies. These differences have also fuelled scepticism on both sides of the Atlantic. The United States considers Europe as hiding a form of protectionism behind its regulatory controls,[274] while the Europeans fear that the American system does not provide sufficient protection to the data of their citizens when they are used by private and public actors in their jurisdiction.[275]

To resolve such problems several solutions have been put on the table. There are in fact a number of possibilities: a multilateral binding convention, a model law, non-binding instruments (technical standards, international guidelines, recommendations and codes of practices, policy standards).[276] This won't be discussed here in detail as it falls outside of the scope of this study, but three main propositions have been at the centre of the debate: bilateral

[271] Eg, Ibid, art 6(1)(a).
[272] Schwartz/Peifer (n 146) 156. But the doctrines of consent and contract are not completely without limitations in the EU. Because of the negative consequences uncontrolled use of consent and contract could lead to, EU data protection law regulates them.
[273] See Section: Relationship between the Right to Privacy and Data Protection.
[274] Schwartz/Peifer (n 146) 118. Or a form of jealousy over 'successful US internet companies': eg Obama speech in Ibid, 157.
[275] This is, for example, the main reason why the ECJ voided the Safe Harbor case in the Schrems case: the United States were found missing an adequate level of protection- meaning an 'essentially equivalent' in *Schrems* (n 177) para 73.
[276] To see the advantages and disadvantages of each in the context of data protection: See Christopher Kuner, 'An International Framework for Data Protection: Issues and Prospects' (2009) 25 Computer L. & Security Rev. 314.

agreements, one global instrument or the emergence of a customary norm. Bilateral agreements are how States mainly cooperate at the moment when it comes to transborder data flows. This implies mutually accepted standards of protection, which may be hard to reach as the Safe Harbor-Privacy Shield saga illustrates.[277] Calls have also been made for the conclusion one single international instrument. This would solve problems created by the multitude of different regulatory schemes all over the world, including the heavy burden of compliance caused by this confusing patchwork of rules.[278] One global framework could clarify the whole field by harmonizing standards, leading to a better protection of individuals' data regardless of where they are in the world. It would also simplify transborder data flows.[279] Unfortunately, this would be difficult to achieve considering the numbers of different regulations and the different approaches they represent- in form and substance. The likelihood of countries giving up, or even compromising on, their well-established procedures and beliefs is low.[280] Additionally, discussion has taken place regarding the potential recognition of the right to data protection as a rule of customary international law. However, there does not seem to be, at this point, enough ground to support this idea. In view of the divergences in data protection regulatory schemes across the world, neither the elements of *opinio juris* nor of state practice[281] can be said to be realized.[282]

Conclusion

Surveillance online regulation mobilizes the international right to privacy and data protection frameworks. The confusion between the two regimes arises from their history, their overlapping scope, and a disorientating terminology.

Data protection frameworks were enacted at the end of the 20th century to specifically address the challenges raised by the emerging information technologies. Initially understood as a "subset" of the general right to privacy, data protection gradually became an independent legal regime- at least at the international level and in Europe.[283] The two regimes, although related, cover nonetheless different issues. Whereas the right the privacy's scope includes *private* data processing, data protection laws regulate data processing practices, regardless of the nature of the data involved.

The confusion is aggravated by the differences in the vocabulary used in data protections frameworks. Firstly, the core principles of data protection are found under different names in different international instruments, making it unnecessarily difficult to identify the similarities between frameworks. Secondly, the regime of data protection as a whole is framed differently in different parts of the world. The terminology of 'data protection' is usually found in European instruments, while the United States prefers to refer this field as

[277] *Schrems* (n 177); to read more on this *See* Valsamis Mitsilegas, 'Surveillance and Digital Privacy in the Transatlantic War on Terror: The Case for a Global Privacy Regime' (2016) 47 Colum. Hum. Rts. L. Rev. 1.
[278] Reidenberg (n 17) 1128.
[279] Ibid, 1129.
[280] Especially where they are regulating sectors such as finance or insurance, De Hert/Papakonstantinou (n 4) 290.
[281] The two elements of custom: Statute of the International Court of Justice, art 38.1.b.
[282] For opposite view: See Zalnieriute (n 12) 113 ss.
[283] Both at the EU and the Council of Europe levels.

“informational privacy”. This difference in terminology actually illustrates different approaches to data processing regulation: European countries understand data protection as a fundamental right, focusing clearly on empowering individuals with an overall system of protection; whereas the United States enacts sectorial laws to correct specific abusive practices. This corresponds to the approaches identified in the first chapter of this thesis: the United States focuses on specific interferences and ensuring individual’s freedom, while the continental understanding of the protection takes the form of granting individuals more control over their private life. At the international level, the three main goals behind the main data protection frameworks (namely regulating data processors activities, granting rights to data subjects and establishing enforcement mechanisms) illustrate the paradigm of control: individuals should be granted more control over their personal data.

International conversation around surveillance regulation is inevitably linked to the broader debate on how to conceptualize data protection.

PART II – JURISDICTIONAL AND SUBSTANTIVE CHALLENGES OF ONLINE SURVEILLANCE REGULATION

CHAPTER IV: Jurisdictional Challenges of Online Surveillance

Introduction

Online mass surveillance challenges many traditional international legal principles, not only because of its obvious impact on the right to privacy, but also of the way it is operated: in cyberspace. While the first part of the thesis focused on the regulation of privacy and data protection, the second addresses the substantive technical challenges of online surveillance. In order to deal with online surveillance and minimize its implications on the enjoyment of fundamental rights, it is necessary to rethink and re-interpret how we understand traditional legal frameworks. While Chapter V analyses this question through the angle of regulation and compliance with substantive international law provisions, this chapter focuses particularly on the question of jurisdiction in the context of surveillance. More specifically, it will look at two types of surveillance activities conducted by States: the interception of communications and the access to data located in another Sate's territory.

The analysis of "jurisdiction principles" is difficult because the term encompasses different meanings in international law, often leading to confusing and sometimes contradictory case-law, scholarship[1] and State practice.[2]

The question of jurisdiction and online surveillance will be examined from two different angles. Part I addresses the question of jurisdiction under general international law and how traditional principles are understood/transposed in the context of digital technology, more specifically in the context of online surveillance. Part II looks at the notion of jurisdiction under international human rights law, and how cyberspace questions traditional approaches to the issue of extraterritorial application of human rights treaties. Each part begins with the relevant legal framework (section 1) before assessing the question of online surveillance (section 2).

For the purpose of this chapter, the notion of "foreign surveillance" refers to "the clandestine surveillance by one State during peacetime of the communications of another's State officials or citizens, when those communications take place partly or entirely outside the

*The research for Chapter IV on the jurisdictional challenges of online surveillance was carried out as part of the 'Eyes Online Project: Taking Surveillance Apart', funded by the Nordforsk Consortium. An executive summary of the report based on this chapter can be accessed at <https://sites.dundee.ac.uk/eyes-online-project/reports-resources/>. However, the chapter has not been published elsewhere and is the author's sole work.

[1] Marko Milanovic, *Extraterritorial Application of Human Rights Treaties* (OUP 2011) 19.

[2] Ibid, 30.

surveillance State's territory, using electronic means, including cyber-monitoring, telecommunications monitoring, satellites, or drones".[3]

Part I – General International Law

Section 1. Theory

A. Notion of jurisdiction

Under general international law, the term 'jurisdiction' defines "the limits of the legal competence of a State or other regulatory authority to make, apply, and enforce rules of conduct upon persons".[4] It can be understood as "the authority of the state, based in and limited by international law, to regulate the conduct of persons both natural and legal, by means of its own domestic law".[5] Jurisdiction is traditionally considered as territorial: it is primarily restricted to persons, property and acts within the State's territory, unless certain exceptions occur.[6] What constitutes valid legal exceptions to the principle of territoriality actually constitutes most of the law on jurisdiction. The general principle beyond any theoretical bases allowing States to assert jurisdiction beyond their own borders is the need of a connection between the State itself and the conduct it wants to regulate.[7] The degree of connection may differ depending on the type of jurisdiction the State seeks to assert.[8]

The purpose of the law on jurisdiction is to delimit regulatory power among States. The jurisdictional rules point to the "worthiest State" to assert jurisdiction over a conduct, the one that is the most closely connected to it.[9] It has long been accepted that multiple States can claim jurisdiction over the same person, or the same conduct, at the same time.[10] The assessment of what a "close connection " means needs to be done in context. It needs to be more than simply the existence of an abstract connection, it is a compromise between States' interests and the necessity to limit the number of States being able to assert their jurisdiction over the same conduct.[11]

To avoid confusion when discussing principles of jurisdiction in the context of surveillance, a brief summary of the different types and bases of jurisdiction seems useful.

B. Different types of jurisdiction

A State's jurisdiction can be divided in three categories of powers: prescriptive, adjudicative and enforcement jurisdiction.

---

[3] Ashley Deeks, 'An International Legal Framework for Surveillance' 55 Va J IntlL 291, 299.
[4] Christopher Staker, 'Jurisdiction' in Malcom D Evans (ed), *International Law* (4dn, OUP 2014) 309.
[5] Milanovic, *Extraterritorial Application of Human Rights Treaties* (n 1) 23.
[6] ILC, 'Annual Report on the work of the 58th Session: Annex E – Extraterritorial Jurisdiction' (2006) 229. (hereinafter 'ILC Report').
[7] Milanovic, *Extraterritorial Application of Human Rights Treaties* (n 1) 24.
[8] ILC Report (n 6) 237.
[9] Uta Kohl, *Jurisdiction and the Internet* (CUP 2007) 20.
[10] Ibid, 21.
[11] Ibid, 23.

Prescriptive jurisdiction refers to "the authority of a State to adopt legislation providing norms of conduct which govern persons, property or conduct"[12]. Adjudicative jurisdiction refers "to the authority of a State to determine the rights of parties under its law in a particular case"[13]. Enforcement jurisdiction refers to "the authority of a State to ensure compliance with its law".[14]

Distinguishing these three different types of jurisdiction is necessary because the requirements to assert jurisdiction legally may vary depending on the type of jurisdiction.[15] As a general rule a State can never assert enforcement jurisdiction on another State's territory without the latter's consent[16], whereas it can exercise its jurisdiction to prescribe outside its territory in certain cases, even without the foreign State's consent.[17] Extraterritorial application of a State's jurisdiction refers to the exercise of sovereign power to regulate conduct outside the State's own borders by means of *domestic* legislation, adjudication or enforcement.[18] National law may provide for the exercise of jurisdiction, but the assessment of the legality of such an assertion is regulated by international law.[19] In that respect, international law recognizes different bases on which a State can validly assert jurisdiction.

C. Different bases of jurisdiction

Two traditional bases of prescriptive jurisdiction are linked to the notion of the modern nation-State: territory and population. A State may exercise legislative jurisdiction over all persons, property and activities in its own territory (territoriality principle) and over all its nationals, wherever they are in the world (nationality principle).[20]

On one hand, the territoriality principle is linked to the sovereignty of the State, exercised in all aspects over its own territory. Because one act can occur in different territories, two variants to that principle have been accepted. The first is that of subjective territorial jurisdiction, which allows States to assert prescriptive jurisdiction over an act that started in their territory but was completed outside of it. The second one is objective territorial jurisdiction and concerns acts initiated outside the State's borders but completed within them.[21] A variant of the territorial principle is the effect doctrine which allows a State to assert jurisdiction over " the conduct of a foreign national occurring outside the territory of a State which has substantial effect within that territory. [It] does not require that an element of the conduct take place in the territory of the regulating State".[22]

---

[12] ILC Report (n 6) 229.
[13] Ibid.
[14] Ibid.
[15] Bernard H Oxman, 'Jurisdiction of States' in Rudolf Bernhart (ed), *Encyclopedia of Public International Law*, vol 3 (Elsevier 1997) 55.
[16] Ibid.
[17] Milanovic, *Extraterritorial Application of Human Rights Treaties* (n 1) 24.
[18] ILC Report (n 6) 229.
[19] Ibid, 230; A state can never invoke its domestic legislation to justify a violation of international law. *See* Article 3 of the Articles on State Responsibility for International Wrongful Acts and Article 27 of the Vienna Convention on the Law of Treaties, art 3.
[20] Oxman (n 15) 55.
[21] Staker (n 3) 317.
[22] ILC Report (n 6) 231. This concept has been controversial, especially the position of the US in the Uranium Antitrust Litigation case, for more details *See* Staker (n 3) 321.

On the other hand, the nationality principle—also a corollary to State sovereignty—allows the State to claim jurisdiction over any activities of its nationals abroad (including legal entities).[23] A variant of this principle is the passive personality principle: "jurisdiction that a State may exercise with respect to conduct abroad which injures one or more of its nationals".[24] This ground of jurisdiction used to stir controversy, but it is now increasingly accepted.[25] It is also mostly accepted when prosecuting terrorists.[26]

However, many problems would arise if claims to jurisdiction were confined to these two grounds of jurisdiction. Thus, certain additional bases of jurisdiction have been recognized.[27] These are:

- the protective principle[28]: "jurisdiction that a State may exercise with respect to persons, property or acts abroad which constitute a threat to the fundamental national interests of a State".[29] The typical example is the act of counterfeiting the State's currency, but the concept of "vital national interest" is still open and there has been some debate over the extent of this kind of jurisdiction.[30]
- the universal principle: "jurisdiction that any State may exercise with respect to certain crimes under international law in the interest of the international community"[31], for example piracy.

The application of these principles in concrete cases is not always straightforward. For example, the territoriality principle, even with its objective and subjective variants, assumes that the act can be easily located, which is not always the case.[32] Furthermore, a specific act may also raise jurisdictional claims by different States, grounded on different bases. The scenario of overlapping jurisdictions might therefore give way to questions of priority.[33] International law on jurisdiction does not provide concrete rules but sets a general regulatory framework. In the words of B. Currie: "A jurisdictional rule is an odd creature among laws. It never tells what the result will be, but only where to look to find the result".[34] The general principle underlying this regulatory framework is the necessity to balance the sovereign powers of different States and the prohibition of interference in another State's internal affairs[35] (more on this in Section 2).

---

[23] ILC Report (n 6) 231.
[24] Ibid.
[25] ICJ Separate Opinion: "passive personality jurisdiction for so long regarded as controversial […] today meets with relatively little opposition at least so far as a particular jurisdiction is indeed concerned" in *Arrest Warrant of 11 April 2000 (Democratic Republic of the Congo v Belgium*) [2002] ICJ Rep 3, Joint Separate Opinion of Judges Higgins, Kooijmans, and Buergenthal, 11.
[26] Staker (n 3) 327.
[27] Oxman (n 15) 55.
[28] To learn more about the protective principle, See Iain Cameron, *The Protective Principle of International Criminal Jurisdiction* (Dartmouth Publishing 1994).
[29] ILC Report (n 6) 231.
[30] Staker (n 3) 321. For example, the United Sates have argued that illegal trade in narcotics threatened the American society and that therefore the protective principle allowed them to extend their jurisdiction extraterritorially on this matter.
[31] ILC Report (n 6) 231.
[32] Staker (n 3) 328.
[33] Ibid, 329.
[34] Brainerd Currie, *Selected Essays in the Conflict of Laws* (CUP 1963) 170, quoted in Kohl (n 9) 15.
[35] Kohl (n 9) 23.

The rules dealing with the extraterritorial application of the *enforcement* jurisdiction are in comparison very simple: extraterritorial enforcement jurisdiction is not allowed unless the other State agrees to it, by a judicial or police agreement, or by treaty.[36] States can therefore conclude agreements on the matter they agree to cooperate on and allow another State to exercise jurisdiction in their territory. Such agreements have been concluded to enhance cooperation on the fight over narcotics, piracy and terrorism.[37]

D. Approaches to jurisdiction: *Lotus* case

There are two different perspectives under which one can approach the question of jurisdiction in general international law. Thus, it may be considered either that States are free to assert jurisdiction over any conduct they seek to regulate, unless there is an international rule prohibiting them from doing so, or that they cannot exercise jurisdiction unless a permissive rule exists allowing them to do so.[38] The first approach is the one taken by the Permanent Court of International Justice (PCIJ) in the *Lotus* case[39] in 1921, whereas the second is supported by customary international law. The Court's position on this question was widely criticized in scholarship, Staker for example calling the conclusion of the Court "a tiresome and oddly persistent fallacy".[40]

The Court was therefore of the opinion that a State is allowed to assert extraterritorial prescriptive jurisdiction as it wishes, unless a specific rule in international law prohibits it from doing so. This view has been widely rejected by doctrine and today is often considered as obsolete.[41] Nonetheless, its influence cannot be completely overlooked; States still sometimes refer to it.[42]

When talking about a State's e*nforcement* jurisdiction, the Court simply stated what was already accepted as a general rule:

> "the first and foremost restriction by international law upon a State is that- failing the existence of a permissive rule to the contrary- it may not exercise its power in any form in *the territory of another State*. In this sense jurisdiction is certainly territorial; it cannot be exercised by a State outside its territory except by virtue of a permissive rule derive from international custom or from a convention"[43]

However, it then proceeded to add what would later become a very controversial paragraph:

> "It does not, however, follow that international law prohibits a State from exercising jurisdiction *in its own territory, in respect of any case which relates to acts which*

[36] Mireille Hildebrandt, 'Extraterritorial jurisdiction to enforce in cyberspace? Bodin, Schmitt, Grotius in cyberspace' (2013) 63 U.T.L.J. 196, 199.
[37] Staker (n 3) 322.
[38] Cedric Ryngaert, *Jurisdiction in International Law* (OUP 2008) 21.
[39] *Case of the S.S. "Lotus" (France v. Turkey*), Judgment No. 9 (7 September 1927) PCIJ Rep 1928, Series A, No 10. (hereinafter Lotus case)
[40] Staker (n 3) 313.
[41] Ryngaert (n 38) 26.
[42] Ibid, 26-27.
[43] Lotus case (n 39) 18-19. (emphasis added)

have taken place abroad, and in which it cannot rely on some permissive rule of international law".[44]

Customary international law, as it has been developed over time by State practice, does not provide for extraterritorial prescriptive jurisdiction unless grounded on a permissive rule (such as the effects doctrine, protective or universality principles).[45] State practice shows indeed that States decided not to follow the Lotus principle. When objecting to another State's assertion of jurisdiction, a prohibitive rule is never brought up – instead, it is usually stated that a State "has no right" to assert jurisdiction in a specific case, unless it can prove that it bases its claim upon one of the accepted under international law grounds.[46]

State practice points therefore to a consensus that extraterritorial prescriptive jurisdiction is not strictly prohibited under international law, but a connecting factor is essential between the State and the conduct it seeks to assert jurisdiction over. This connecting link should constitute the basis for one of the accepted under international law permissive rules. To not in any way restrict States in their jurisdictional claims would run contrary to the central purpose of international law of jurisdiction: defining States' spheres of action and limiting potential conflicts.[47]

Section 2. Online surveillance

When analyzing the concepts of jurisdiction and online surveillance, two different aspects of the question need to be approached. One is the context in which online surveillance takes place: cyberspace. Cyberspace as a novel medium brings a set of challenges of its own concerning the question of jurisdiction, and more specifically the understanding of the territoriality principle. The other aspect relates to the nature of surveillance itself and the different forms it can take.

A. Challenge of the Internet

Today, most communications takes place online, our data passing daily by an international IT infrastructure. The internet straddles different legal spaces [48], which raises questions on how international law is going to deal with this new challenging medium. The cyber context requires a "reconceptualization of jurisdiction in terms of novel spatialities".[49] The core

[44] Ibid, 19. (emphasis added). The Court then elaborated: "Such a view would only be tenable if international law contained a general prohibition to States to extend the application of their laws and the jurisdiction of their courts to persons, property and acts outside their territory, and if, as an exception to this general prohibition, it allowed States to do so in certain specific cases. But this is certainly not the case under international law as it stands at present. Far from laying down a general prohibition to the effect that Sates may not extend the application of their laws and the jurisdiction of their courts to persons, property and acts outside their territory, it leave them in this respect a wide measure of discretion which is only limited in certain bases by prohibitive rules; […] In these circumstances all that can be required of a State is that it should not overstep the limits which international law places upon its jurisdiction; within these limits, its title to exercise jurisdiction rests in its sovereignty." 19.
[45] Ryngaert (n 38) 27.
[46] Staker (n 3) 315.
[47] Ryngaert (n 38) 27.
[48] Hannfried Leisterer/Julian Staben, 'International Cross-Surveillance: Global IT Surveillance Arbitrage and the Principle of Proportionality as a Counterargument' (2017) 15 Surveillance and Society 108, 109.
[49] Hildebrandt (n 36) 198.

transnational nature of the internet is problematic in legal terms. Legal systems have always been underpinned by the assumption that activities could be "geographically delimited". In the words of Kohl: "The Internet presents an entirely new dimension to the problem of squeezing transnational activity into the national legal straitjacket".[50] Data's unique characteristics require a new analysis of the validity and effects of the traditional territoriality doctrine.[51]

A.1. Applying the territoriality principle in the digital context

The Internet has not provoked the earthquake it was thought it would bring along.[52] In most areas of international law, traditional principles have "simply" been transposed to the cyber context (more or less successfully). States do not view Internet as beyond their competences and have now passed discussing whether it should be regulated, debating instead the modalities of effectively doing so.[53]

The field of international criminal law is a good example of the literal application of the territoriality principle to the digital context. For example, the 2001 Convention on Cybercrime of the Council of Europe[54] grounds its regime on the traditional territoriality principle of jurisdiction.[55] Moreover, in regulating cyber warfare, the Tallinn Manual approaches the question of jurisdiction from the exact same angle.[56] Its Rule 2 allows States to exercise jurisdiction over persons and infrastructure located *on its territory*, and "extraterritorially in accordance with international law".[57] It continues: "The principle basis for a State to exercise its jurisdiction is physical or legal presence of a person (*in personam*) or object (*in rem*) *on its territory*".[58] It recognizes the technological problems that might arise because of the infrastructure potentially straddling different national borders, leading to conflicting simultaneous jurisdictions but repeats that "these technical challenges do not deprive a State of its legal right to exercise jurisdiction over persons and cyber infrastructure located on its territory".[59] The other provisions on jurisdiction try to resolve such technical problems, but do not in essence challenge the territoriality principle.[60]

---

[50] Kohl (n 9) 4.
[51] Jennifer Daskal, 'The Un-Territoriality of Data' (2015) 125 Yale L. J. 326, 334. For a detailed analysis on data's characteristics See Daskal, Ibid, 365-378.
[52] Staker (n 3) 329.
[53] Kohl (n 9) 12.
[54] Convention on Cybercrime (opened for signature 23 November 2001, entered into force 1 July 2004) 2296 UNTS 167.
[55] Article 22.1.d. *See* Council of Europe, *Explanatory Report on the Convention on Cybercrime* (2001) ETS No 185 <https://rm.coe.int/16800cce5b> accessed 22 September 2019.
[56] *Tallinn Manual on the International Law Applicable to Cyber Warfare*, Michael Schmitt (ed.), (CUP 2013) (hereinafter Tallinn Manual).
[57] Ibid, Rule 2, 18. (emphasis added)
[58] Ibid, Rule 2(2), 18. "For instance, pursuant to its *in personam* jurisdiction a State may adopt laws and regulations governing the cyber activities of individuals *on its territory*. It may also regulate the activities of privately owned entities registered (or otherwise based as a matter of law) in its jurisdiction but physically operating abroad, such as Internet services providers (ISPs). *In rem* jurisdiction would allow it to adopt laws governing the operation of cyber infrastructure on its territory". Ibid, 18. (emphasis added)
[59] Ibid, Rule 2(3), 19.
[60] Ibid, Rule 2(4-5), 19: "With regard to jurisdiction based upon territoriality it must be noted that although individuals using information and communications technology have a specific physical location, the location of mobile devices can change during a computing session. […] Any State from which the individual has operated enjoys jurisdiction because the individual, and the devices involved, were located on its territory when so used". "Even with technology such as mobile cloud computing, the devices from which the human user is

In the field of data protection, it is recognized that delimiting the exterritorial reach of data protection rights will be "one of the most challenging questions for applying fundamental rights to the online environment"[61], but the (future) General Data Protection Regulation (GDPR) still associates data and territory when analyzing jurisdiction.

A.2. Moving away from territoriality

Certain online activities can transit through the territory of a States without actually establishing any substantial link with the State in question.[62] Their presence may be "incidental or just of passing nature".[63] Courts also face real difficulties in practically applying the territoriality principles to cases involving data (like the Microsoft case, analyzed *infra*). Certain scholars have therefore questioned the merits of transposing the territoriality principle to cyberspace for jurisdictional matters, calling for a new paradigm/paradigm shift.

This debate is however not novel. In the mid-nineties, in the beginning of the debate on how to approach the challenges brought by the Internet, some scholars proposed to completely abandon the principle of "state-based laws", considering them to be inadequate to regulate cyberspace. Johnson and Post[64] for example asserted that territoriality could not be transposed to the transnational online world. They advocated considering the cyber context as a new and separate place for regulatory purposes.[65] But most of the scholarship in the early days of the digital revolution focused on private law. Little attention has been paid to the "constitutional and sovereignty implications of the government reaching […] across borders to search and seize"[66].

Svantesson calls for a "broad reform of how international law approaches [prescriptive, adjudicative and enforcement] jurisdiction"[67]. Arguing that territoriality was not useful as a "starting point for jurisdictional claims" due to the challenges Internet raises[68], he advocated for jurisdiction to only be asserted when a substantial connection between the activity and the requesting State exists and only if the State has a legitimate interest in doing so.[69] He has also argued that a balance between the asserting State's and other States' interest need to be

initiating requests can be geo-located; software services and applications may track the geo-coordinates of the computing devices […]. It is possible under certain circumstances for someone […] to spoof the geo coordinates advertised by his or her computing device. It is also possible that user-location will not be made available […]. Actual physical presence is required, and sufficient, for jurisdiction based on territoriality; spoofed presence does not suffice".

[61] Christopher Kuner, 'Extraterritoriality and the Fundamental Right to Data Protection' (*EJIL: Talk! Blog Post*, 16 December 2013) <https://www.ejiltalk.org/extraterritoriality-and-the-fundamental-right-to-data-protection/> accessed 20 October 2017.

[62] Dan Jerker Svantesson, 'A New Jurisprudential Framework for Jurisdiction Beyond the Harvard Draft' (2015) 109 AJIL BOUND 69, 69.

[63] Cedric Ryngaert, 'An Urgent Suggestion to Pour Old Wine into New Bottles- Comment on A New Jurisprudential Framework for Jurisdiction' (2015) AJIL UNBOUND 81.

[64] David Johnson/David Post, 'Law and Borders – The Rise of Law in Cyberspace' (1996) 48 Stanford Law Review 1367, 1367.

[65] Kohl (n 9) 11.

[66] Daskal (n 51) 332.

[67] Svantesson (n 62) 69.

[68] Ibid, 70.

[69] Ibid, 71.

sought.[70] This theoretical change would according to him help resolve jurisdictional issues in controversial areas by allowing more creative solutions rather than mechanical binary ones.[71] Certain scholars have reacted positively to this proposed paradigm shift, doubting however the radicalism of this particular proposition[72], especially at the light of the evolution of private international law.[73]

Others have been wondering if jurisdiction could be based on another location than the data's, like the user's, the company headquarters, or wherever the terms of services decide.[74]

B. Online surveillance

International law approaches the question of surveillance only marginally.[75] Very few treaties deal with it directly, except for certain mutual agreements of cooperation.[76] States have been sending spies in foreign countries for centuries in order to gather information. Usually States will by virtue of domestic legislation prohibit and try to impede information gathering by foreign States in their territory, while at the same time trying to protect their own capacity to do so abroad.[77] Domestically spying and intercepting communications can be- and often is- a criminal act. Online surveillance is just another way of practicing the same activities that have always occurred: gathering intelligence to strengthen the national security of the country. Some even argue that not sending agents to another State's territory actually decreases the degree of interference with the territorial sovereignty of the affected State.[78] The literature on espionage is not uniform on its assessment of the legality of peacetime espionage. Some are of the opinion it is legal, others disagree, and some claim "it is neither legal nor illegal- perhaps as Nietzsche would say, it is beyond good and evil"[79]. The complicated legal status of peacetime espionage in international law will be detailed in the following chapter. For the purpose of this analysis however, the situation can be summarized by stating that it doesn't seem to be an international consensus on the question, because States are silent on the matter and benefit from the lack of clear regulatory framework.

The question of jurisdiction and surveillance will depend on the kind of online surveillance at stake. As mentioned *supra,* this chapter will look at two surveillance activities conducted by States: the interception of communications and the access to data located in another Sate's territory.

---

[70] Ibid.
[71] Ibid, 72.
[72] Ryngaert, 'An Urgent Suggestion' (n 63) 82.
[73] Horatia Watt, 'A Private (International) Law Perspective Comment on a 'New Jurisprudential Framework for Jurisdiction' (2015) 109 AJIL UNBOUND 75, 75.
[74] Daskal (n 51) 395; To read more on the pros and cons of each approach, *See* Kate Westmoreland, 'Jurisdiction over user date – What is the ideal solution to a very real world problem?' (*CIS Blog*, 24 July 2014) <http://cyberlaw.stanford.edu/blog/2014/07/jurisdiction-over-user-data-what-ideal-solution-very-real-world-problem> accessed 15 October 2017.
[75] Simon Chesterman, 'The Spy Who Came in From the Cold War: Intelligence and International War' (2006) 27 Mich. J. Int'l L. 1071, 1072.
[76] For example: "The United Kingdom – United States of America Agreement", also known at the Five Eyes Agreement.
[77] Chesterman (n 75) 1072.
[78] Lothar Determann/Karl Gutenberg, 'On War and Peace in Cyberspace: Security, Privacy, Jurisdiction' (2014) 41 Hastings Const. Law Q. 875, 883.
[79] Afsheen John Radsan, 'The Unresolved Equation of Espionage and International Law' (2007) 28 Mich. J. Intl L. 595, 602.

B.1. Interception of electronic communications

"Communication surveillance" can be defined as "monitoring, intercepting, collecting, obtaining, analysing, using, preserving, retaining, interfering with, accessing or similar actions taken with regard to information that includes, reflects, arises from or is about a person's communications in the past, present, or future"[80].
"Communications" in this context refer to "activities, interactions, and transactions transmitted through electronic mediums, such as content of communications, the identity of the parties to the communications, location-tracking, information including IP addresses, the time and duration of communications, and identifiers of communication equipment used in communications" [81].

Different types of surveillance impinge upon different jurisdictional issues. Domestic surveillance does not raise, in term of jurisdiction, any particular problem. It is a typical application of the territoriality principle. Transnational and extraterritorial surveillance are however more challenging.

Transnational surveillance can be defined as "the surveillance of communication that crosses state borders, including those that begin and end overseas but incidentally pass through the collecting state".[82] Extraterritorial surveillance is the surveillance of communications that takes place entirely outside the State's territory.[83] This type of surveillance is conducted via programs which allow to tap fiber-optic cables to collect data in bulk (Prism, Tempora, Upstream,…).[84] Domestic legislation sets up and regulates these programs, which means States allow themselves to legislate on transnational and extraterritorial matters.[85]

The United States Foreign Intelligence Surveillance Act (FISA) Amendment[86] is a good example of a State enacting domestic law allowing "the conduct of extraterritorial surveillance to intercept communications in foreign jurisdictions"[87]. In 2008, the United

[80] Necessary and Proportionate, 'International Principles on the Application of Human Rights to Communication Surveillance' (March 2014) <https://necessaryandproportionate.org/principles> accessed 3 September 2019.
[81] Ibid.
[82] Deeks (n 2) 299-300. For example in practice this could involve communications whose sender and recipient are in other countries but incidentally transit in the collecting State, or communications whose only the sender is abroad, but would be the target of surveillance measures, in Deeks, Ibid, 311.
[83] Ibid, 299.
[84] For more information on this *See*: Amnesty International/Privacy International, 'Two Years After Snowden, Protecting Human Rights in an Age of Mass Surveillance' (June 2015) <https://www.amnestyusa.org/wp-content/uploads/2017/04/ai-pi_two_years_on_from_snowden_final_final_clean.pdf> accessed 9 October 2017; Ewen Macaskill, et al. 'GCHQ taps fibre-optic cables for secret access to world's communications' (*The Guardian,* 21 June 2013) <https://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa> accessed on 22 September 2019.
[85] *See* for example the practice of the United Kingdom, which led to the case *Big Brother Watch and others v United Kingdom*, App nos 58170/13, 62322/14 and 24960/15 (13 September 2018).
[86] An Act to amend the Foreign Intelligence Surveillance Act of 1978 to establish a procedure for authorizing certain acquisitions of foreign intelligence, and for other purposes (10 July 2008).
[87] Laura Pitter, 'Comments of Human Rights Watch to Privacy and Civil Liberties Oversight Board Hearings' (19 March 2014) <https://www.hrw.org/news/2014/03/19/comments-human-rights-watch-privacy-and-civil-liberties-oversight-board-hearing> accessed 19 October 2017.

States Congress changed important features of FISA. The controversial Section 702[88] allows electronic surveillance targeting non-US persons located outside the US territory to be conducted without a warrant, with no probable cause or requirement to prove a link with a foreign power. It authorizes foreign data collection activities conducted under PRISM and UPSTREAM programs. PRISM is a collection program that allows the National Security Agency (NSA) to require electronic communications service providers to turn over all communications received or sent from a specific "selector[89]" associated with the individual targeted.[90] The UPSTREAM collection program involves retrieving the data from the Internet's "backbone" with the help of the providers that control the fiber optic cables over which Internet and telecommunications transit.[91] Under Section 702, more than 250 million Internet communications are being collected per year.[92]

Executive Order 12333 regulates surveillance that is not meant to target anyone in particular, but collects bulk of information without using any selector or criterion to filter the data collected. It has collected Internet metadata, webcam chats, and cellphone's location data…[93]

These surveillance activities raise the question whether States have the prescriptive jurisdiction to legislate on such a matter. If transnational surveillance could potentially be justified by the territorial doctrine, the same cannot be said for extraterritorial surveillance. States could invoke the protective principle, or maybe even the effect doctrine, to claim extraterritorial prescriptive jurisdiction but interestingly they do not do so. States have been completely silent on the question of jurisdiction and interception of communications- even when targeting foreigners abroad (conduct which would usually have raised objections from other States). This is probably explained by the fact that every State is engaging in such surveillance activities, and the majority of them benefit from the non-regulated status quo.

This attitude of *laissez-faire* in regard to foreign surveillance seems actually aligned to the PICJ's position in the Lotus case: States seem to consider themselves free to exercise extraterritorial jurisdiction in the absence of a prohibitive rule.

B.2. Extraterritorial access to data

Is a State allowed to unilaterally access data located outside its territory? Certain States do so, but does this not raise question over respect of sovereignty and jurisdiction principles? Law enforcement agencies regularly request access to data, exercising thus the State's enforcement jurisdiction.

---

[88] FISA Amendment Act §702, codified as U.S. Code §1881a – "Procedures for targeting certain persons outside the United States other than United States persons".
[89] For example a specific email address used by the individual.
[90] Privacy & C.L. Oversight Board, 'Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act' (2 July 2014) 7 <https://www.pclob.gov/library/702-Report.pdf> accessed 22 September 2019.
[91] Ibid, 8.
[92] 'FISA court ruling on illegal NSA e-mail collection program' (*Washington Post*, 21 August 2013) <https://www.washingtonpost.com/apps/g/page/national/fisa-court-ruling-on-illegal-nsa-e-mail-collection-program/409/> accessed 30 October 2017.
[93] Daskal (n 51) 351-52.

The jurisdiction to enforce is defined as: "state's authority under international law to exercise *investigative*, coercive or custodial powers in support of law […], whether through police or executive action or through its courts"[94]. Undertaking surveillance and investigating are some of the attributes of the enforcement jurisdiction, especially in the criminal context.[95]

The prohibition of extraterritorial exercise of enforcement jurisdiction limits the room for manoeuver of a State in terms of pre-charge and pre-trial investigation. States have no obligation under international law to assist one another in criminal matters, but still often do so.[96] Law enforcement agencies have powers conferred upon them by legislation, which they can exercise either while carrying out their duties, or under certain circumstances after authorization by a judicial, executive or administrative entity.[97] The reach of statute granting these powers is traditionally limited to the State territorial jurisdiction. An exercise of powers by an agency outside its territorial jurisdiction would therefore be illegal (which is not the same to a domestic action creating extraterritorial effects).[98]

A brief look into US laws illustrates well this type of surveillance and the jurisdictional questions it raises, because they are accessible, the mechanisms they set up are being used on a daily basis by US law enforcement agencies, and they have been the object of discussion at the governmental, judicial and academic level.

The USA Patriot Act[99] created some additional procedural mechanisms for US law enforcement agencies to access data for their investigations. Some of these mechanisms grant access to data stored in the cloud.[100] For example the Patriot Act and its infamous Section 215 broadened the scope of FISA Orders, giving the opportunity for FBI agents to obtain "an order requiring the production of any tangible things (including books, records, papers, documents and other items) for an investigation to protect against international terrorism and clandestine intelligence activities"[101]. Data stored in the cloud fall under the "other items" category that could be requested.

National Security Letters (NSL) can also be used as a mechanism by the FBI to access data. They are a type of administrative subpoena that US law enforcement agencies can produce in order to obtain data and records relating to their investigations.[102] Before the Patriot Act,

---

[94] Roger O'Keefe, *International Criminal Law* (OUP 2015) 29. (emphasis added)
[95] Ibid, 29.
[96] Ibid, 38.
[97] Ian Walden, 'Accessing Data in the Cloud: The Long Arm of the Law Enforcement Agent' in Siani Pearson and George Yee (eds), *Privacy & Security for Cloud Computing* (Springer-Verlag 2013) 49.
[98] Ibid.
[99] Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act" (USA PATRIOT Act) of 2001, made changed to FISA and ECPA, See: 18 U.S.C. § 3127(3) as amended by the USA PATRIOT Act § 216 and 50 U.S.C. § 1804(a)(7)(B) as amended by USA PATRIOT Act § 204.
[100] Alex Lakatos, 'The USA Patriot Act and the Privacy of Data Stored in the Cloud' (*Mayer and Brown Online*, 18 January 2012) <https://www.mayerbrown.com/publications/the-usa-patriot-act-and-the-privacy-of-data-stored-in-the-cloud-01-18-2012/> accessed 18 October 2017.
[101] Title II, Sec. 215 "Access to records and other items under the foreign intelligence surveillance act", amending FISA by inserting "Sec. 501. Access to Certain Business Records for Foreign Intelligence and International Terrorism Investigations (a.1.)".
[102] Lakatos (n 100).

agencies (mainly the FBI) could already access information such as financial records[103], names of financial institutions where the individual targeted has/had an account (including its identifying information such as name, address, employment history)[104], or information about subscriber of wire or electronic providers (name, address, length of service), toll billing records information and transaction records[105]. The National Security Act allowed all these information to be requested if needed when investigating government employees for security checks or if believed that they might be foreign spies.

Thus, these kinds of requests were not new when the Patriot Act was enacted in 2001. But its Title V[106] once more broadens the scope of these already existing mechanisms. The 56 field offices were allowed to make NSL requests, there is no need to prove a link with a foreign power (need to prove a relation to international terrorism or foreign spying)… US authorities can therefore make a NSL request to Internet providers to obtain access to data stored in the cloud. The FBI does not have the authority to request the content of the communications of a specific individual, but can ask certain meta-data such as the name, address and length of service of the user. Providers don't legally need to provide more than that, and some of them start to refuse to comply with more expansive requests.[107]

There are other more traditional mechanisms for agencies to request information they need for their investigations: search warrants and grand jury subpoenas can be both requested to access data stored in the cloud. When asked to produce a document, an entity has the duty to produce "any documents within its possession, custody or control"- which involves not only documents that can be located on the US territory, but also materials that the entity controls abroad.[108]

Without even mentioning the obvious privacy and due process concerns this type of provisions raise (which already led to public outcry and a Reauthorization Act), this also poses serious questions regarding jurisdiction.

Under US law, an individual can only be subject to the types of measures described above if he is "amendable to personal jurisdiction". The meaning and requirement of "personal jurisdiction" can be found in the US Constitution, and the US Patriot Act did not change this.[109] A minimum of contact with the forum needs to be shown for an individual to fall under the scope of "personal jurisdiction". US law interprets this requirement as meaning that any corporation based in the United States, having a location in the United States or conducting continuous and systematic business fulfills the criteria of "minimum contact with the forum" and falls under US jurisdiction (and can therefore be subject to FISA orders, NSLs, search warrants and grand subpoenas).[110] Consequently, in theory, any cloud service *provider or customer* that is based in the US, that has an office in the US or conducts

[103] Authorized by the Right to Financial Privacy Act (1978) 12 U.S.C. paras 3401-3422.
[104] Authorized by the Fair Credit Reporting Act, 15 USC §paras 1681 et seq.
[105] Authorized by the Electronic Communications Privacy Act (1986) 18 U.S.C. paras 2510-22.
[106] "Removing Obstacles to Investigating Terrorism".
[107] Lakatos (n 100).
[108] Ibid.
[109] Ibid.
[110] Ibid.

systematic or continuous business with the US can therefore be subject to a US law enforcement request to produce materials, even if the data is stored outside the United States.[111]

The authority of a judicial warrant is only territorial; a State cannot enforce its jurisdiction extraterritorially without the other State's consent. Consequently, domestic judges are not allowed to unilaterally grant warrant to seize or search material extraterritorially.[112] This principle applies to warrants produced under the Wiretap Act[113] or under the Stored Communications Act[114] (SCA). The territorial principle is very clear, but its application to collecting data less so.[115]

This has led to a contentious case[116] in which Microsoft refused to turn over data requested by US federal law enforcement agents under the SCA[117], arguing that because the data was located in Dublin the US could not assert jurisdiction over it. The federal magistrate judge and district court disagreed, stating that it was the provider's location, and not the data's, that was the reference point to assess warrant jurisdiction. Because Microsoft had offices and employees working on the US territory, the warrant was not reaching extraterritorially and was therefore valid. But in July 2016, the Second Circuit unanimously reversed the previous decisions[118], interpreting the SCA as meant to be applied only territorially and that the word "warrant" was suggesting a delimited territory. The US government filed a petition for an *en banc* rehearing by the Second Circuit, which the Court split 4-4 on a vote, therefore keeping the previous judgment in favor of Microsoft. The saga continued as the US Department of Justice appealed to the Supreme Court in June 2017. The legal community was looking forward to hearing the Supreme Court's decision on the subject, as this was a great opportunity to clarify the current jurisdictional issue. Unfortunately, the judgment never came to be. Just after the oral hearings of the case in front of the Supreme Court, Congress introduced the "Cloud Act"[119]. The legislation introduced a new provision modifying the SCA: companies are now obliged to provide the requested data "regardless of whether such communication, record, or other information is located within or outside of the United States."[120] The Act was adopted in March 2018. The following month, the Supreme Court issued a declared that the Microsoft case was therefore considered moot.[121]

---

[111] Ibid.
[112] Daskal (n 51) 354.
[113] 18 U.S.C. (2012) paras 2510-2522; allowing collection of electronic communication in real time with a warrant.
[114] 18 U.S.C. paras 2701-2712, allowing collecting stored communication with a warrant.
[115] Daskal (n 51) 355.
[116] *In the Matter of a Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corporation* 15 F.Supp.3d 466 (S.D.N.Y. 2014).
(hereinafter Microsoft Case)
[117] Stored Communications Act 1986, in the Electronic Communications Privacy Act, Pub. L. No. 99-508, 100 Stat. 1848 (1986) (codified as amended at 18 U.S.C. paras 2701 et seq. (1986)).
[118] *In re Warrant to Search a Certain E-Mail Account Controlled & Maintained by Microsoft Corp.,* 829 F.3d 197 (2d Cir. 2016)
[119] Clarifying Lawful Overseas Use of Data: Consolidated Appropriations Act, 2018, Pub. L. No. 115-141, §§ 101-106, 132 Stat. 348, 1213-25 (2018).
[120] Part I of the Cloud Act.
[121] *United States v Microsoft Corporation*, 584 US (2018).

If the United States managed to "bypass" the complicated question of jurisdiction in this case, the issues under international law stay the same. This case typically illustrates the challenges brought by the digital revolution. It challenges the territoriality doctrine at its core and the assumptions underlying it: that objects can be identified and have a specific location, that location matters and should have normative effect.[122] It shows how difficult it is to actually assess what can be considered territorial or extraterritorial.[123] It also demonstrates the difficulties brought by concurrent jurisdictions: in this case, in one hand, the United States could ground their jurisdiction claim on their interpretation of the territoriality principle, the nationality principle and potentially the protective principle. Ireland on the other hand could also argue his position with the territorial principle.[124] Both Microsoft and the Government can argue that they respect the territoriality principle but just disagree on the assessment whether certain acts happen territorially or not and how to interpret the SCA.[125]

This is not the first time problems occur because of concurring jurisdictions, the international community has been dealing with these issues in various other fields for years, but the digitalization and globalization of our information and communication networks is only going to increase the complexity of the issues at hand.

C. Solutions for problems of jurisdiction?

International law gives some discretion to States on how they give effect to a foreign regulation within their territory. There are three types of responses a State can adopt when facing a case of "regulatory extraterritoriality" (meaning in this context: "the exercise of direct authority [by a State] over entities in foreign jurisdiction"[126]). The State can either not react (if the extraterritorial act has no strong impact on domestic affairs), it can answer negatively and aggressively contest the action (ie. diplomatic protests, non-recognition of laws, claw-back statutes, judicial injunctions,…)[127] or it can react positively and embrace the claim of authority by the other State.[128] In short, States can accept and recognize the effect of an extraterritorial norm on their territory (if valid under international law standards) or they can refute it.[129] It is not uncommon for some States to promulgate extraterritorial regulations. The United States in particular have done so in various fields, as for example in regard to competition law, trade and sanctions[130] (which was starkly rejected by other States).

---

[122] Daskal (n 51) 329.
[123] Svantesson (n 62) 70.
[124] Ibid.
[125] Daskal (n 51) 289.
[126] Yuko Suda, 'Transatlantic Politics of Data Transfer; Extraterritoriality, Counter-Extraterritoriality and Counter-Terrorism' (2013) 51 JCMS 773.
[127] ILC Report (n 6) 234-35.
[128] Suda (n 126) 775.
[129] Mahir Al Banna, 'The Long Arm US Jurisdiction and International Law: Extraterritoriality against Sovereignty' (2017) 60 J.L. Pol'y & Globalisation 60.
[130] For example, Helms-Burton and D'Amato Act: measures to extend their Cuban embargo policy (vividly rejected by other States). For more on this subject, *See* the International Bar Association, 'Report of the Task Force on Extraterritorial Jurisdiction' (2009) <file:///C:/Users/2158047G/Downloads/ETJ_Task_Force_Report.pdf> accessed on 18 January 2018.

Intelligence sharing in multiple forums is becoming increasingly common.[131] The different European intelligence services work in close partnership, from information sharing to helping and advising each other on how to bypass restrictive domestic laws.[132] The international community is becoming aware of the need for "new cross-border mechanisms that facilitate law enforcement access to data, yet also respect the sovereign interest in setting privacy protections and controlling law enforcement operations within one's jurisdiction"[133].

The fight against terrorism, including in its prevention aspect, is only strengthened by cooperation between States, particularly through bilateral and multilateral agreements.[134] A number of these cooperation agreements have already been made between Europe and the United Sates[135], such as the Passenger Name Record Agreement (PNR)[136], the Society for Worldwide Interbank Financial Transactions Agreement (SWIFT)[137] or the Container Security Initiative Agreement (CSI)[138].

The three Agreements mentioned before (PNR, SWIFT and CSI Agreements) were all the result of negotiation between the US "assertive" claim of extraterritorial reach of its domestic counterterrorism regulations, and the EU answers to it[139]. These Agreements were reached not only to render these operations more efficient but especially to bring solutions to certain "legal compatibility problems", including jurisdictional ones. In the case of the CSI, the negotiations focused on solving technical issues such as border cooperation, but in the PNR and SWIFT talks, the debate focused on question of legality and compatibility with the EU data protection and privacy framework.

Bilateral or multilateral Mutual Legal Assistance Treaties (MLATs) can be concluded to cooperate on investigations and enforcement regarding criminal offenses.[140] These types of agreements offer a valid answer to jurisdictional questions.[141] The United States and European Union concluded one in 2003[142], which includes a provision on mutual assistance to administrative authorities[143] and on data protection[144]. Unfortunately the MLAT has not

---

[131] Chesterman (n 75) 1095.
[132] Julian Borger, 'GCHQ and European spy agencies worked together on mass surveillance' (*The Guardian*, 1 November 2013 <https://www.theguardian.com/uk-news/2013/nov/01/gchq-europe-spy-agencies-mass-surveillance-snowden> accessed 20 October 2017.
[133] Daskal (n 51) 393.
[134] UNSC Res 1373 (28 September 2001) UN Doc S/RES/1373, 3.
[135] To read more on this subject: *See* Suda (n 126) 772-788.
[136] Agreement by which Europeans airlines give their passenger names records to the U.S. Homeland Security.
[137] Agreement by which the financial transactions by the SWIFT can be accessed by the US Treasury Department and its section Terrorist Finance Tracking Program (TFTP).
[138] Agreement allowing US customs officers to identify "high risk containers before they are shipped to the United States" in European ports. – Illustrative example of States agreeing to another State's exercise of extraterritorial enforcement jurisdiction.
[139] Suda (n 126) 783.
[140] *See* Model Treaty by the UN General Assembly on Mutual Assistance in Criminal Matters: UNGA, Res 45/117, 14 December 1990.
[141] Daskal (n 51) 395.
[142] Agreement on Mutual Legal Assistance between the United States of America and the European Union, 25 June 2003.
[143] Article 8.
[144] Article 9.

been as effective as hoped, requests taking months before going ahead[145], pushing States' governments to try to access private data straight from the service providers and take unilateral action not included in the MLAT[146] (taking measures such as improving their surveillances capabilities, restricting use of encryption, or expanding the extraterritorial application of their domestic laws..).[147]

A solution would therefore be to reform the MLAT system to make it more effective, something than many actors have been calling for.[148] That would allow the requesting State to obtain the other State's consent raising thus no jurisdictional problems. These calls seemed to have been heard by the US Department of Justice, which proposed in July 2016 a new legislation on cross-border Data Access. It would reform the way the MLAT works currently by allowing governmental agencies to directly request data from the foreign companies[149], which would make the process faster than the current one.

However, this solution does not answer the fundamental question of when and under which conditions a State can legally assert jurisdiction over specific data, even if that data is found outwith its territory. It keeps a simplistic view on the question of data location and does not take into account the challenges of its "mobility, manipulability and divisibility".[150]

Regarding the substance of the agreements a jurisdictional test should be adopted at the international level, and it should be the same regarding regulation and compulsion. That would solve the problem of States having different jurisdiction standards depending on the activity they wish to pursue. For example: the United States recognizes the territorial limits of its regulatory authority (like the SCA having only a limited territorial reach), but then claims that the government can request data to be turned over, regardless of its location – has long as it has jurisdiction over the provider. This ambiguity leads to complications: potential conflicts of law and potential sovereignty violation – like illustrated by the Microsoft case(s)[151]. The Agreements should also decide on specific substantive and

---

[145] It takes an average of ten months for a request to be answered by the United States, Kate Westmoreland, 'A New International Convention on International Legal Cooperation?' (ACS Blog, 2 September 2015) <https://www.acslaw.org/acsblog/a-new-international-convention-on-international-legal-cooperation> accessed 21 October 2017.
or as Brad Smith puts it "government authorities must go through bureaucratic hurdles that address 21st century problems at 19th century speed" in 'Time for an International Convention on Government Access to Data' (*Microsoft Blog*, 20 January 2014) <https://blogs.microsoft.com/on-the-issues/2014/01/20/time-for-an-international-convention-on-government-access-to-data/> accessed 21 October 2017.

[146] Smith (n 145); Daskal (n 51) 393.

[147] Tiffany Lin/Mailyn Fidler, 'Cross-Border Data Access Reform: A Primer on the Proposed U.S.-U.K. Agreement' (Berkman Klein Centre for Internet & Society, Berklett Cybersecurity publication 7 September 2017) 2. <https://dash.harvard.edu/bitstream/handle/1/33867385/2017-09_berklett.pdf?sequence=1> accessed 15 October 2017.

[148] Westmoreland (n 145). Initiatives have been undertaken at the inter-governmental, governmental, industry, and civil society levels: See Kate Westmoreland/Gail Kent, 'International Law Enforcement Access to User Data: A Survival Guide and Call for Action' (2015) 13 Canadian Journal of Law and Technology 225, 249-253.

[149] For more information on this, *See* Lin/Fidler (n 147).

[150] Daskal (n 51) 394.

[151] Ibid, 395-396. As developed *supra*, the Cloud Act resolved this issue domestically, but the question stays the same at the international level.

procedural mechanisms under which one State could request access to data located in another State's jurisdiction[152], to provide a certain level of harmonization in terms of protection.[153]

Another solution would involve the promulgation of an international treaty specifically addressing governments' requests for user data. Calls have been made for an international legal framework to be created to regulate transnational and extraterritorial surveillance and data-access, which would supplement the MLAT system.[154] This idea would be difficult to realize (harmonization of standards, compatibility with international standards,…) but would ideally lead to a better system both for the individuals targeted (clearer and better protection of their privacy rights) and for governments (more efficient mechanism to access extraterritorially data, respect of their sovereignty and enforcement jurisdiction). This would in turn be a great incentive for other States to join in.

At the regional level, the Council of Europe has done so in its Convention on cybercrime[155], its Chapter III being dedicated to international cooperation and mutual assistance[156]. It also tackles the question of search and seizures of stored computer data[157], and real-time collection of traffic data[158]. It is the most advanced treaty focused on harmonizing procedural and substantive criminal matters, including mutual assistance, with more than fifty signatures, including non-European countries such as the United States, Canada, Australia, Japan,...[159] The EU General Data Protection Regulation[160] also addresses specifically this type of data transfer, reiterating the necessity to respect data protection norms[161].

There is no doubt that an enhanced cooperation between States is necessary to answer problems raising from extraterritorial jurisdictional claims. As much as an international treaty specifically regulating requests to access data sounds appealing on paper, it is unlikely to emerge in practice. Right now, an MLAT is the strongest instrument available to States to

[152] Ibid, 396.
[153] For example establishing a "bilateral parity" principle by which each State would have the obligation to provide non-citizens the same level of protection than to its own citizens, Daskal (n 51) 397.
[154] Smith (n 145).
[155] Convention on Cybercrime (n).
[156] Articles 25-35.
[157] Article 19.
[158] Article 20.
[159] For more details on the substantive content of the Convention and European criminal procedures when it comes to data access: *See* Walden (n 97).
[160] 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 (hereinafter 'GDPR').
[161](115) "Some third countries adopt laws, regulations and other legal acts which purport to directly regulate the processing activities of natural and legal persons under the jurisdiction of the Member States. This may include judgments of courts or tribunals or decisions of administrative authorities in third countries requiring a controller or processor to transfer or disclose personal data, and which are not based on an international agreement, such as a mutual legal assistance treaty, in force between the requesting third country and the Union or a Member State. The extraterritorial application of those laws, regulations and other legal acts may be in breach of international law and may impede the attainment of the protection of natural persons ensured in the Union by this Regulation. Transfers should only be allowed where the conditions of this Regulation for a transfer to third countries are met. This may be the case, inter alia, where disclosure is necessary for an important ground of public interest recognised in Union or Member State law to which the controller is subject" 22.

cooperate on this matter (even though current ones need to be reformed as soon as possible to keep their relevancy).

Part II - International Human Rights Law

States are bound to comply with the treaties they are parties to[162]. In the context of surveillance, the respect of the right to privacy is potentially at stake. The right to privacy is protected by both international and regional instruments, such as the Universal Declaration of Human Rights (UDHR)[163], the 1966 International Covenant on Civil and Political Rights (ICCPR)[164] and the European Convention on Human Rights (ECHR)[165].

This chapter will not look at the content of the right to privacy in the context of online surveillance, but will try to answer the preliminary question of whether these provisions even apply to (extraterritorial) surveillance in the first place. To answer this question, it will look at the notion of 'jurisdiction' in the context of human rights treaties, and more specifically the jurisdictional clauses they contain (section 1). The second part of the analysis will turn to the question of jurisdiction under international human rights treaties in relation to online surveillance, and how cyberspace challenges the traditional standards.

The interpretation given to the jurisdictional clauses of human rights treaties influences their scope[166], and therefore the scope of the protection afforded to individuals. The question of extraterritorial application of human rights treaties is an important one because the decentralized infrastructure of the internet has led to "unpredictable routing of connections and mostly unencrypted transfer of data", which means that the majority of users could be subjects of surveillance by other states that their own.[167]

Since a lot has already been written on this issue, the present chapter will flesh out the main lines of the debate but will not address the relevant arguments in detail.[168]

---

[162] Vienna Convention on the Law of Treaties (adopted 23 May 1969, entered into force 27 January 1980) 1155 UNTS 331, art 26.

[163] Universal Declaration of Human Rights (adopted 10 December 1948) UNGA Res 217 A(III) art 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".

[164] International Covenant on Civil and Political Rights (adopted 16 December 1966, entered into force 23 March 1976) 999 UNTS 171, art 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".

[165] Convention for the Protection of Human Rights and Fundamental Freedoms (adopted 4 November 1950, entered into force 3 September 1953) 213 UNTS 221, art 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".

[166] Marko Milanovic, 'Human Rights Treaties and Foreign Surveillance: Privacy in the Digital Age' (2015) 56 Harv. Int'l. L. J. 81, 101.

[167] Hannfried Leicester/Julian Staben, 'International Cross-Surveillance: Global IT Surveillance Arbitrage and the Principle of Proportionality as a Counterargument' (2017) 15 Surveillance and Society 114.

[168] In particular *See* Samantha Besson, 'The extraterritoriality of the European Convention on Human Rights: Why Human Rights Depend on Jurisdiction and What Jurisdiction Amounts to' (2012) 25 Leiden Journal of International Law 857; Marko Milanovic on the question on extraterritoriality of human rights law in general:

Section 1. Jurisdiction and extraterritoriality of human rights treaties

The concept of jurisdiction under human rights treaties is different than the one in general international law. Jurisdictional clauses can be found in human rights treaties, setting a certain threshold to assess whether States have jurisdiction over an individual. If the threshold is met, the State's treaty obligations are triggered.[169] Jurisdiction under general international law focuses on the application of domestic law regulating persons, property and acts.[170] Its purpose is to determine if a claim by a State to regulate a certain activity is lawful or not, it "sets out limits on the domestic legal orders of states, so that they do not infringe upon the sovereignty of others"[171]. Jurisdiction under human rights treaties involves a factual analysis of the situation: whether a State exercises power over a territory or its people[172] - in order to assess if the international treaty will apply to the situation or not. Human rights treaties restrict their scope to certain geographical or jurisdictional conditions, limiting their obligations to specific "factual situations or certain groups of people"[173].

A. United States Constitution

Understanding the United States' position on the extraterritorial application of its Constitution is an interesting starting point on the general question of whether a State should grant fundamental rights to foreigners located outside its territory.

The United States have a narrow interpretation of extraterritorial application of the Constitution. In *U.S. v. Vertugo-Urquidez*[174] the Supreme Court hold that the Fourth Amendment was not protecting non-citizens from search and seizure of property abroad, rejecting arguments of certain American scholars advocating for the Bills of Rights to be binding regardless of identity or location.[175] Citizenship is recognized as a ground for fundamental rights.[176]

Eighteen years later, the Supreme Court stated in *Boumediene v. Bush* that the Constitution (in this case the Suspension Clause) applied to combatants in captivity in Guantanamo Bay.[177] The case was a big step in the discussion of the extraterritoriality of the US Constitution. The standard used by the Court to affirm extraterritorial jurisdiction was the physical control of the State over "territories, facilities and proceedings" (not control over

Extraterritorial Application of Human Rights Treaties (n 1); and in the context of surveillance: 'Human Rights Treaties and Foreign Surveillance: Privacy in the Digital Age' (n 166).

[169] Besson, ibid, 860; Milanovic, *Extraterritorial Application of Human Rights Treaties* (n 1) 19-20.

[170] Milanovic, ibid, 27.

[171] Ibid, 29.

[172] Ibid, 27.

[173] Ashley Deeks, 'Does the ICCPR Establish an Extraterritorial Right to Privacy?' (*Lawfare Blog*, 14 November 2013) <https://www.lawfareblog.com/does-iccpr-establish-extraterritorial-right-privacy> accessed 4 October 2017.

[174] 494 U.S. 259, 261 (1990).

[175] Daskal (n 51) 338.

[176] Milanovic, 'Human Rights Treaties and Foreign Surveillance' (n 166) 88. For more on why this position is actually a moral one and why the justification behind it doesn't hold under scrutiny: See Milanovic, Ibid, 89.

[177] *Boumediene v. Bush*, 553 U.S. 723 (2008) 794-95.

people[178] which will be recognized as a valid approach by European countries). But this case has not led to a shift in American legal culture on the question of extraterritoriality of the Constitution. Lower courts keep interpreting *Boumediene's* teaching only to the Suspension Clause and other "structural" provisions, and *Verdugo-Urquidez* is still relied on to assert that non-citizens without close links to the US are not protected by the Fourth Amendment and other fundamental individual rights.[179]

B. European Convention of Human Rights

Article 1 of the European Convention of Human Rights (ECHR) stipulates that State Parties "shall secure to everyone *within their jurisdiction* the rights and freedoms defined in Section I of this Convention"[180]. The question of how to interpret this jurisdictional clause, and what does "within their jurisdiction" mean, led to several, sometimes contradictory, decisions of the European Court of Human Rights (ECtHR). Not dwelling on the intricacies of the debate this chapter will summarize briefly the position of the Court on the question.[181] The current status of the Court's jurisprudence is that jurisdiction can be presumed extraterritorially when States have effective control over a territory[182] or over individuals[183]. The Court clarifies that "a State need not exercise all public powers to meet the jurisdictional test; even exercise of 'some' public powers may be sufficient"[184]. This clarification implies that one state's jurisdiction is not always exclusive of all others', meaning jurisdiction could be divided.[185]

C. International Covenant on Civil and Political Rights

---

[178] Valsamis Mitsilegas, 'Surveillance and Digital Privacy in the Transatlantic 'War on Terror': The Case for a Global Privacy Regime' (2016) Colum. Hum. Rts. L. Rev., 69.
[179] Daskal (n 51) 341-342.
[180] (emphasis added).
[181] For more details on the ECtHR case-law on extraterritorial jurisdiction: *See* Besson (n 168); Sarah Miller, 'Revisiting Extraterritorial Jurisdiction: A Territorial Justification for Extraterritorial Jurisdiction under the European Convention' (2009) 20 EJIL 1223; CoE, 'Factsheet Extra-territorial jurisdiction of States Parties to the European Convention on Human Rights' (February 2016) <http://www.echr.coe.int/Documents/FS_Extra-territorial_jurisdiction_ENG.pdf> accessed 10 October 2017. For more details on the ECtHR case-law on mass surveillance: *See Kennedy v UK*, App no 26839/05 (18 May 2010); *Roman Zakharov v Russia,* App no 47143/06 (4 December 2015); *Szabó and Vissy v Hungary,* App no 37138/14 (12 January 2016); *See* CoE, 'Factsheet Mass Surveillance' (November 2017) <http://www.echr.coe.int/Documents/FS_Mass_surveillance_ENG.pdf> accessed on 19 January 2018). *See* also UK case: IPT, *Human Rights Watch Inc v. The Secretary of State for the Foreign & Commonwealth Offices* (16 May 2016) UKIPTrib 15_165-CH.
[182] *Loizidou v Turkey*, App no 15318/89 (23 February 1995) para 62: "Bearing in mind the object and purpose of this Convention, the responsibility of a Contracting Party may also arise when […] it exercises *effective control of an area* outside its national territory" and para 138; the court reaffirmed this position and stated the need to reject the "regrettable vacuum in the system of human-rights protection" that would result otherwise", in *Cyprus v Turkey*, App no 25781/94 (10 May 2001) para 78; *Al-Skeini and Others v United Kingdom*, App no 55721/07 (7 July 2011) para 138; *Bankovic and others v Belgium,* App no 52207/99 (12 December 2001) para 70; *Ilascu and Others v Moldovia*, App no 48787/99 (8 July 2004) paras 314-316.
[183] *Al-Skeini* ibid, paras 136-137; *Isaak and Others v Turkey*, App no 44587/98 (28 September 2006); *Medvedyev and Others v France*, App no 3394/03 (29 March 2010) para 67; *Hirsi Jamaa and Others v Italy*, App no 27765/09 (23 February 2012); *Jaloud v the Netherlands*, App no 47708/08 (20 November 2014); *Isari v Moldova and Russia*, App no 42139/12 (19 October 2015).
[184] *Ocalan v Turkey*, App no 46221/99 (12 May 2005).
[185] Peter Margulies, 'The NSA in Global Perspective: Surveillance, Human Right, and International Counterterrorism' (2014) 82 Fordham L. Rev., 2149-50.

The vast majority of States conducting (foreign) surveillance are parties to the ICCPR. Article 17 enshrines the right to privacy. Article 2(1) states that:

> "Each State Party to the present Covenant undertakes to respect and to ensure to all individuals *within its territory and subject* to its jurisdiction the rights recognized in the present Covenant […]"[186].

The United States reads Article 2(1) as requiring the individual to be *both* within the territory *and* subject to its jurisdiction in order to enjoy the rights consecrated in the ICCPR. This narrow lecture of the text interprets the "and" as requiring both elements to be satisfied in order to fall under the scope the ICCPR, therefore restricting the Covenant to US territory and rejecting any potential extraterritorial reach.[187] This interpretation is in minority today[188], and voices are increasingly calling for a change of position.[189]

European States differ in their interpretation of this jurisdictional clause from the US. They consider the Covenant applicable to any person within a State party's territory *or* within its jurisdiction. Even States that traditionally align their position with that of the United States such as the United Kingdom, Germany, the Netherlands or Belgium accept some extraterritorial reach for the ICCPR[190], even if only in certain limited scenarios.[191]
International courts have recognised that the ICCPR indeed has extraterritorial reach, either under the spatial model[192] (effective control over territory), or the personal one (effective control over individuals)[193]. The Human Rights Committee has stated in its General Comment N°31[194] that: "a State party must respect and ensure the rights laid down in the Covenant *to anyone within the power or effective control* of that State Party, *even if not situated within the territory* of the State Party"[195], adding that "the enjoyment of Covenant rights is not limited to citizens of States Parties but must also be available to *all individuals*, regardless of nationality or statelessness, (…), who may find themselves in the territory or subject to the jurisdiction of the State Party. This principle also applies to *those within the*

---

[186] (emphasis added).
[187] Deeks, 'Does the ICCPR Establish an Extraterritorial Right to Privacy?' (n 173); Mitsilegas (n 178) 71; for more details on the history of this position and on arguments to reverse it, *See* Memo by Former Legal Adviser of the Department of State Harold Koh, 'Memorandum Opinion on the Geographic Scope of the International Covenant on Civil and Political Rights' (19 October 2010) <https://www.justsecurity.org/wp-content/uploads/2014/03/state-department-iccpr-memo.pdf> accessed 19 October 2017. (hereinafter Koh Memo)
[188] Deeks, 'Does the ICCPR Establish an Extraterritorial Right to Privacy?' (n 173).
[189] *See* Koh Memo (n 187); Privacy & C.L. Oversight Board Report (n 90) 100.
[190] Pitter (n 87).
[191] For more details on specific countries' position: See Koh Memo (n 187) 37-42.
[192] *Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory* (Advisory Opinion) [2004] ICJ Rep 136, para 108: "The Court would observe that, while the jurisdiction of States is primarily territorial, *it may sometimes be exercised outside the national territory.* Considering the object and purpose of the [International Covenant on Civil and Political Rights], it would seem natural that, even when such is the case, States parties to the Covenant should be bound to comply with its provisions. The constant practice of the Human Rights Committee is consistent with this. Thus, the Committee has found the *Covenant applicable where the State exercises its jurisdiction on foreign territory*". (emphasis added); *Case concerning Armed Activities on the Territory of the Congo (Democratic Republic of the Congo v. Uganda)* [2005] ICJ Rep 168.
[193] *Lopez Burgos v Uruguay* (29 July 1981) n52/1979, UN Doc A/36/40, para 12.2-3; *Celiberti de Casaregio v Uruguay* (29 July 1981) n56/1979, UN Doc A/36/40, para 10.3.
[194] UNHRC, 'General Comment No 31: The nature of the general legal obligation imposed on States Parties to the Covenant' (26 May 2004) UN Doc CCPR/C/21/Rev.1/Add.13.
[195] Ibid, point 10., 4. (emphasis added).

power or effective control of the forces of a State Party acting outside its territory, regardless of the circumstances in which such power or effective control was obtained"[196]. The Office of the United Nations High Commissioner for Human Rights wrote in its report in 2014: "A State party must respect and ensure the rights laid down in the Covenant to *anyone within the power or effective control* of that State Party, even if not situated within the territory of the State Party"[197]. This extends to persons within their "authority"[198]. The test used is again "effective control" and the relevant element is the relationship between the individual and the State, not the location of the violation.[199] This position is supported by the ICJ and the majority of legal scholarship.[200]

A third way of reading Article 2 is to differentiate duties of a State depending whether people are "within its territory" *or* "subject to its jurisdiction". States would have the duty to *provide* the Covenant's rights to people within its territory, but only to *respect* them in regard to individuals within their jurisdiction.[201] This interpretation has increasingly been gaining attention in the international community.[202]

Section 2. Extraterritorial Jurisdiction and Online Surveillance

The digital world has brought new challenges with respect to the protection of fundamental human rights. A fresh interpretation of the content of the right to privacy itself is of course necessary[203], but this chapter will focus on the jurisdictional questions online surveillance raises.

A. Problems

The traditional criterion of "effective control" is difficult to transpose to the context of online surveillance. Most of the cases that have dealt with the "effective control" test have unfolded in the context of detention or have involved at least some form of physical power and control over the plaintiff.[204] Surveillance however requires no control over a person.[205] Intercepting or storing a foreigner's data for surveillance purposes is radically different to holding that person in detention.[206] Can thus surveillance activity even be conceptualized as a form of control over a specific person or group of persons?

The ICCPR indeed applies to domestic surveillance because individuals (nationals or not)

---

[196] Ibid. (emphasis added).
[197]UNHRC, 'The Right to Privacy in the Digital Age: Report of the Office of the United Nations High Commissioner for Human Rights' (30 June 2014) UN Doc A/HRC/27/37, para 32. (hereinafter 'High Commissioner Report').
[198] Ibid.
[199] Ilina Georgieva, 'The Right to Privacy under Fire – Foreign Surveillance under the NSA and the GCHQ and Its Compatibility with Art. 17 ICCPR and Art. 8 ECHR' (2015) Utrecht J. Int. Eur. Law 111.
[200] Mitsilegas (n 178) 71.
[201] Milanovic, *Extraterritorial Application on Human Rights Treaties* (n 1); Koh memo (n 187) 8.
[202] Mitsilegas (n 178) 72; Margulies (n 185) 2139; Pitter (n 87).
[203] This topic will be developed in the Part II of the thesis.
[204] Amongst others: *Al Saadoon and Mufdhi v UK*, App no 61498/08 (2 March 2010); *Al-Skeini* (n 182); *Al Jedda v UK*, App No 27021/08 (7 July 2011); *Hassan v UK*, App no 29750/09 (16 September 2014): *Jaloud* (n 183).
[205] Mitsilegas (n 178) 72.
[206] Deeks, 'Does the ICCPR Establish an Extraterritorial Right to Privacy?' (n 173).

are within the State's territory.[207] However in case of transnational and extraterritorial surveillance the application of the Covenant comes into question. Does, for example, monitoring transnational or extraterritorial communications fall under the State's jurisdiction? If the spatial model of jurisdiction is used in a case of extraterritorial surveillance, a court would probably find that the surveying State lacks effective control over the territory in which surveillance is being exercised. If the personal model is chosen, could a court find the individual under the control and authority of the surveying State simply because its communications have been intercepted, or his data transferred? The International Group of Experts who wrote the Tallinn Manual on Cyber Operations could not reach a consensus as to whether a cyber activity operated by a State could amount to 'power or effective control' over an individual located outside that State's territory[208]. The majority was of the view that 'in the current state of the law, physical control over territory or individual is required before human right law obligations are triggered'[209]. How States and human rights courts will position themselves on this question remains unclear.[210]

All this indicates that the time has come to adapt the traditional concepts of jurisdiction over territory and persons when it comes to mass surveillance. According to Pitter "mass digital surveillance […] can produce the reality of control even through remote means. A government can now easily violate the privacy of an individual without having physical control over that person, and without that person being located inside an area under its control because a government may have power or effective means over the individual's communications (or over the company that stores or transmits them)"[211]. The globalization of international information and communication networks has made territorial concepts of human rights in some respects obsolete, in particular when trying to regulate State surveillance.[212]

B. Solutions

Increasingly more voices are calling for a new understanding of the traditional criterion of "effective control". The Office of the United Nations High Commissioner for Human Rights (OHCHR) tries to apply the effective control standard to surveillance. In June 2014 it wrote in a report:

> "Digital surveillance therefore may engage a State's human rights obligations if that surveillance involves the *State's exercise of power or effective control in relation to digital communications infrastructure,* wherever found, for example, through direct tapping or penetration of that infrastructure. Equally, where the State exercises regulatory jurisdiction over a third party that *physically controls* the data, that State also would have obligations under the Covenant. If a country seeks to assert jurisdiction over the data of private companies as a result of the incorporation of those companies in that country, then human rights protections must be extended to

[207] And therefore subject to the state's jurisdiction under Article 2.
[208] Michael Smith (ed), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (CUP 2017) 185.
[209] Ibid.
[210] See *infra*, ECtHR's position in the Big Brother case.
[211] Pitter (n 87).
[212] Leicester and Staben (n 167) 108.

those whose privacy is being interfered with, whether in the country of incorporation or beyond. This holds whether or not such an exercise of jurisdiction is lawful in the first place, or in fact violates another State's sovereignty"[213].

Another solution involves the recognition of "virtual" control as an adequate standard[214]: "the mere surveillance as such does not constitute physical control but it may (depending on the extent and intensity) constitute virtual control. It is not too far-fetched in the cyber-age to imagine that this type of control might also trigger the human rights obligations of the 'virtual' controller" [215]. The virtual control test would meet the challenge of rapidly evolving technologies, which the physical control test cannot do[216]. It also has the advantage of not completely walking away for the notion of control used by courts.[217] The majority of the authors of the Tallinn Manual 2.0 was nonetheless of the opinion that: 'the premise of exercising power or effective control by virtual means such that human rights obligations attach runs contrary to both extensive State practice and the paucity of expressions of *opinio juris*"[218].

Courts have traditionally used the claimant's location as the relevant element to look at. However, in the context of cyberspace this could be changed to the data's location, or the place of interception. The communication or data itself could be the unit of reference, rather than the individual- which could be more suitable in respect to the nature of the electronic environment in which surveillance is being conducted.[219]

The ECtHR had the opportunity to pronounce itself on this applicability of the Convention to extraterritorial surveillance for the first time in the Big Brother Watch case[220], its first case involving the interception of communications by the Government Communication Headquarters (GCHQ)[221]. Unfortunately, the Court avoided the difficult question: it simply assumed that the Convention applied- ignoring the fact that many applicants were not actually based in the United Kingdom. It managed to do so because the UK government did not raise an objection to the applicability of the Convention. The case is currently being heard in front of the Grand Chamber, but the argumentation to justify following the UK government's position is nonetheless interesting. The Court stated:

"They [the government] did not, however, raise any objection under Article 1 of the Convention; nor did they suggest that *the interception of communication (...) was taking place outside the United Kingdom's territorial jurisdiction*. The Court will therefore

[213] High Commissioner Report' (n 197) para 34. (emphasis added).
[214] 'Virtual control' would apply when "a State can assert control over an individual's communication" or data in Margulies (n 185) 2139.
[215] Anne Peters, 'Surveillance Without Borders: the Unlawfulness of the NSA Panopticon, Part II' (*EJIL: TALK!*, 1 November 2013) <https://www.ejiltalk.org/surveillance-without-borders-the-unlawfulness-of-the-nsa-panopticon-part-ii/> accessed 10 October 2017.
[216] Margulies (n 185) 2152.
[217] Georgieva (n 199) 113.
[218] Tallinn Manual 2.0 (n 208) 185.
[219] Deeks, 'An International Legal Framework for Surveillance' (n 2) 300.
[220] *Big Brother Watch and Others* (n 85).
[221] Intelligence and security organisation for the United Kingdom.

proceed on the assumption that the matters complained of fall within the jurisdictional competence of the United Kingdom"[222].

The Court refers to the place of interception, not the location of the individual whose communication is being intercepted. The Court therefore seems to suggest- but not decide- that if the surveillance is taking place inside the borders of a State party to the Convention, the conduct will be covered by the Convention, even if the individual is not physically in that territory.[223] This shows a change of focus: it is the location of the interception that matters, not the individual's. This sounds promising: the location of the interception is where the State's activity (and therefore the interference with the right to privacy and its potential violation) actually takes place. Using it as the relevant location seems therefore more adapted to online surveillance cases. It will be interesting to see whether this "suggestion" is followed by the Grand Chamber.

Concerns have been raised that any type of processing of personal data has a negative impact on the enjoyment of the right to privacy for the individuals concerned. Certain scholars have argued that such processing constitutes both effective and virtual control and therefore should trigger the application of treaties protecting the right to privacy.[224] Milanovic writes in this respect: "The only truly coherent approach to the threshold question of applicability […] is that human rights treaties should apply to virtually all foreign surveillance activities."[225]. This echoes the position taken by a *minority* of Experts writing the Tallinn Manual: in their opinion, if the exercise or the enjoyment of a human right by an individual is within the power or effective control of a State, then the State in question is considered as having power or effective control over the individual in question.[226]

Of course, this position only implicates the right, it does not equate to a violation- which is the object of a separate determination.[227] The fact that a treaty applies to a situation does not mean that the surveillance activity is unlawful. The lawfulness of the activity (foreign or domestic) is examined on the merits of its compliance with the right to privacy. This is the subject of the next chapter.

Conclusion

Online surveillance challenges our understanding of traditional principles of jurisdiction. The notion of jurisdiction under general international law is based on the territoriality doctrine, allowing extraterritorial assertions of jurisdiction in specific cases supported by recognized permissive rules. By questioning the relevance of the territoriality principle as a viable ground for sharing regulation (or at least the feasibility of its concrete application), cyberspace "chips away" the notion that a State is "territorially defined and territorially

[222] *Big Brother Watch and Others* (n 85) para 271. (emphasis added).
[223] Marko Milanovic, 'ECtHR Judgment in Big Brother Watch v. UK' (*EJIL Talk!,* 17 September 2018) <https://www.ejiltalk.org/ecthr-judgment-in-big-brother-watch-v-uk/> accessed 29 September 2019.
[224] Mitsilegas (n 178) 73.
[225] Milanovic, 'Human Rights Treaties and Foreign Surveillance' (n 166) 87.
[226] Tallinn Manual 2.0 (n 208) 185. "In other words, if an individual cannot exercise a human right, or enjoy the protection of one because of a State's action, international human rights law applies extraterritorially" ibid.
[227] Ibid, 186.

empowered regulatory institution"[228]. If certain forms of surveillance (such as accessing data extraterritorially) are being discussed, others are being conducted under the radar. This causes concerns because of the general lack of conceptual clarity on the issues that it raises in regard to jurisdictional issues or sovereignty violations. The need for a novel interpretation of traditional standards is also clear under international human rights law. The effective control test needs to be adapted to the cyber context. The protection offered by human rights treaties is considerably weakened by uncertainty. The international community has to find concrete solutions to these problems, which will lead to a clearer regulatory framework enhancing individuals' protection and securing States in the respect of their jurisdiction and sovereignty. While doing so, it will clarify one important aspect of the legal discourse on online surveillance regulation. Another essential issue concerns the substantive regulation of surveillance activities at the international level and is the subject of the following chapter.

[228] Kohl (n 9) 8-9.

CHAPTER V: Substantive Challenges of Online Surveillance

Introduction

As it has been demonstrated in chapters I, II, and III of this thesis, confusion surrounding the legal discourse on surveillance regulation is created by a multitude of factors: the different approaches to protecting private interests at the domestic level, which in turn influence the international provisions; the unclear conceptualization and scope of the latter. The emergence of data protection frameworks, and how they shaped our understanding of how privacy should be protected in the 21st century, added an extra layer of confusion to an already murky field. Surveillance activities have brought their own challenges to the existing framework: jurisdictional and substantive ones. Chapter IV examined the jurisdictional challenges. The present chapter turns to the substantive ones to assesses the substantive regulation of online surveillance under international law.

'The total surveillance society' is according to Joan Cocks one of the aspects of the 'maelstrom of globalisation'.[1] In her words, Walter Benjamin once alluded to the shocks of modernity through his now-famous image of an angel of history who looks backwards at wreckage piled upon wreckage while being catapulted forwards by the storm 'we call progress''.[2] States have engaged in surveillance activity since remote communications became possible, gathering individuals' personal information to assess their intentions, and (future) actions. Intercepting communications has always been a valuable tool for law enforcement purposes, either for preventing or prosecuting crimes.[3] The modernization of information and communication technologies and the invention of the Internet not only changed greatly the way people communicate, but also expanded the way States conduct surveillance. This has had an impact upon almost every aspect of surveillance activities: the nature and frequency of the measures, the amount of information collected, the number of people surveilled, and the legal implications of such practices.[4]

The question of online surveillance in international law is addressed in this chapter under two angles. The first one assesses the legality of espionage in general international law (Part I). First, the silence of the international community on the question, which can be interpreted as ambiguity, is discussed; then, three approaches to the issue will be detailed. The second part of this chapter turns to the conformity of online surveillance activities with international human rights law, more specifically with the right to privacy (Part II). The first section looks at how the legality of surveillance is assessed under Article 17 of the ICCPR and Article 8 of the ECHR. It assesses if and which surveillance activities are understood as amounting to an interference with privacy,[5] to then look at how the traditional limitation standards inherent

[1] Joan Cocks, *On Sovereignty and Other Political Delusions* (Bloomsbury, 2014) 1.
[2] Ibid.
[3] UNHRC, 'Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue' (17 April 2013) UN Doc A/HRC/23/40, para 12.
[4] Ibid, para 13.
[5] For the purpose of clarity, we will use the word 'privacy' in this chapter to cover both the concepts of 'privacy' as understood by the ICCPR and the concept of 'private life' found in the ECHR. As detailed in the Chapter II of this thesis, the content of these two concepts (and of the scope of their respective legal

in the right to privacy have been interpreted in the context of online surveillance. The second section presents a succinct summary of the main discussions concerning the need to 'update' existing human rights frameworks in order for them to adequately account for new surveillance techniques and calls for the elaboration of a new legal instrument specifically aimed at regulating electronic surveillance.

Part I. General International Law

This chapter focuses on one aspect of peacetime espionage: communications surveillance. 'Communications surveillance' is understood for the purpose of this study as 'the monitoring, intercepting, collecting, obtaining, analysing, using, preserving, retaining, interfering with, accessing or similar actions taken with regard to information that includes, reflects, arises from or is about a person's communications in the past, present, or future'.[6] 'Espionage' can be described as 'the consciously deceitful collection of information, ordered by a government or an organisation hostile to or suspicious of those the information concerns, accomplished by humans unauthorized by the target to do the collecting'.[7] The focus here is on peacetime espionage, as wartime espionage is regulated by a specialised legal framework[8] and falls outside the scope of this study.

The question whether surveillance practices for the purpose of intelligence gathering are lawful under international law has been the subject of widespread debate. The position of general international law on the matter is rather unclear and the answer to the question but for straightforward. States have been operating silently in the dark for a long time. Benefiting from the unregulated *status quo* they have carried on with their practices, without any actual obligation to disclose their capabilities.

The first section describes the silence of international law on the question of the peacetime espionage under international law. It then turns to discuss how the 2013 Snowden revelations challenged the *status quo* by unveiling the far-reaching surveillance capabilities of and measures taken by the United States and its allies. These revelations put surveillance in the limelight. The second section looks at three different ways international law has approached the question of legality of spying activities: by not pronouncing itself (nor legal or illegal) (A); by allowing them (B); or prohibiting them (C).

---

protections) is not clear- but to avoid numerous 'privacy/private life' quotes, for the purpose of this specific chapter, the word 'privacy' will be used to cover both terms.

[6] Necessary and Proportionate, International Principles on the Application of Human Rights to Communications Surveillance (2014) 4. <https://necessaryandproportionate.org/principles> accessed 29 August 2019. 'Communications' consist of 'activities, interactions, and transactions trans- mitted through electronic mediums, such as content of communications, the identity of the parties to the communications, location-tracking, information including IP addresses, the time and duration of communications, and identifiers of communication equipment used in communications' Ibid, 4.

[7] Geoffroy Desmaret, 'Espionage in International Law' (1996) 24 Denv. J. Int'l L. & Pol'Y 321, 325-26.

[8] Eg. Treatment of 'spies' in international humanitarian law: Laws and Customs of War on Land (Hague, IV) (adopted 18 October 1907, entered into force 26 January 1910) Treaty Series 539, arts 29, 30, 31; Geneva Convention Relative to the Protection of Civilian Persons in Time of War (adopted 12 August 1949, entered into force 21 October 1950) 75 UNTS 287, art 5; Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflict (adopted 8 June 1977, entered into force 7 December 1978) 1125 UNTS 3, arts 45(3) and 46.

Section 1. Silence of international law

The relationship between peacetime espionage and international law is an obscure, somewhat hidden, one; international law has never addressed the question directly. Different reasons exist behind this attitude.

Peacetime espionage has always been conceived as a matter of domestic rather than international law, even in cases when it has an international nexus.[9] International law has generally been quiet on the question of regulation of peacetime surveillance activities: there is no international regulation addressing specifically the topic, and until recently there existed no clear official, governmental positions or documents, linking surveillance practices and international law.[10] Scholarship is also meagre when it comes to these issue.[11] The international regulation of surveillance has therefore been deemed as 'underdeveloped',[12] 'virtually unstated',[13] and 'remarkably oblivious'.[14] As Dieter Fleck puts it: 'The fact that no explicit treaty norms address peacetime espionage is paradoxical in light of the enormous amount of intelligence activities and their relevance for international relations between states.'[15]

Ashley Deeks identifies several reasons why international law has had so little to say about spying. One of the main explanations is the secrecy surrounding surveillance practices: surveillance intrinsically takes place undercover. The fact that such operations take place in secret makes it difficult to regulate or limit them, but also to discern when an actor violates such regulations or the corresponding obligations. This also makes rather complex the question of attribution.[16] In addition, States prefer to keep their surveillance capabilities confidential.[17] Discussing openly about the need to effectively regulate surveillance might put States in a position to have to reveal their spying abilities, which defies the exact purpose of keeping their intelligence gathering activities undercover. Another reason identified by Deeks behind why States have been reluctant to legislate on surveillance at the international level is the fact that national security interests are at the core of conducting peacetime espionage.[18] The unregulated *status quo* allows states to gather decisive information about other States or non-State actors that might threaten their security. This includes, among others, the violation of sanctions regimes, the proliferation of weapons, and the organisation of terrorist attacks. There are therefore great incentives for States to prohibit spying at the domestic level (which they do) and at the same time keep it unregulated at the international level. This allows them to collect intelligence abroad, while protecting their own secrets.[19]

---

[9] Desmaret (n 7) 330.
[10] Ashley Deeks, 'An International Legal Framework for Surveillance' (2015) 55 Virginia Journal of International Law 291, 291.
[11] Afsheen John Radsan, 'The Unresolved Equation of Espionage and International Law' (2007) 28 Mich. J. Int'l L. 595, 596.
[12] Craig Forcese, 'Spies Without Borders: International Law and Intelligence Collection' (2011) 5 Journal of National Security Law & Policy 179, 185.
[13] Desmaret (n 7) 321.
[14] Richard Falk, *Foreword Essays on Espionage and International Law* (Roland J Stanger ed, 1962) v.
[15] Dieter Fleck, 'Individual and State Responsibility for Intelligence Gathering' (2007) 28 Mich J. Int'l L. 687, 690.
[16] Deeks (n 10) 314.
[17] Ibid, 314.
[18] Ibid, 313.
[19] Ibid, 313-14.

Different States have different spying capabilities. Those with limited abilities to carry extensive surveillance tend to be keen on regulating spying, while the 'stronger' ones[20] do not (or at least have not so far) felt that need and would benefit less from such regulation.[21]

For all these reasons, States have been quite reluctant to discuss – even more so to regulate – surveillance practices. The situation, however, dramatically changed in 2013 when Edward Snowden disclosed the extent of surveillance practices of the US national security and intelligence services (and its allies), triggering a major public debate.

The Snowden revelations put the surveillance practices of the United States and its partners in the limelight. It exposed secret alliances between the United States and its partners such as the Five-Eye Agreement,[22] but also the scope and scale of national surveillance programmes such as Prism,[23] Tempora,[24] and Optic Nerve.[25],… Historically, foreign surveillance activities focused on the collection of information from people with 'decision making' capabilities in governments.[26] The surveillance of individuals was costly and therefore not frequent. The Snowden disclosures brought to the light a significant shift in who was being targeted:[27] individuals are now also the subjects of surveillance measures both by their own governments and foreign ones, and very frequently so.

Public outcry and unprecedented political scandals followed. This change in surveillance practices undermined the original justifications for the non-regulation of foreign surveillance. The need for secrecy was still present, but the unwanted disclosures rendered such secrecy somewhat redundant. Governments with extensive surveillance capabilities found themselves under pressure to be more transparent about their activities in order to restore public trust. The rationale of 'protecting national security interests' behind surveillance practices was also questioned. Doubts were voiced whether States had started to collect more (and other types of) information than what was necessary for the protection of such national security interests.[28]

---

[20] Eg. United States, United Kingdom, France, Russia, and China.
[21] Deeks (n 10) 315.
[22] More on this *infra*. Amongst many things, Snowden revealed that the telephone records from millions of Verizon customers were collected by the NSA; the existence of many different surveillance programs such as EvilOlive, Stellar Wind, Prism, Fairview, Muscular, Tempura,…; that the NSA bugged EU offices in NY, Washington, and Brussels, spied on Indian diplomats, Dilma Roussef, Angela Merkel, and at least 38 foreign embassies and missions, on millions of citizens from Germany, France, Italy, Spain, and many Latin American countries; that secret deals were struck between agencies from the Five-Eye coalition,…
For a comprehensive and clear overview of the Snowden revelations, See: Paul Szoldra, 'This is everything Edward Snowden revealed in one year of unprecedented top-secret leaks' (*Business* Insider, 16 September 2016) <https://www.businessinsider.com/snowden-leaks-timeline-2016-9?r=US&IR=T> accessed 29 January 2020.
[23] A program ran by the NSA which tap fiber-optic cables to collect communication data such as phone and Internet traffic in bulk.
[24] The UK equivalent of Prism.
[25] Program collecting and storing in bulk images of Yahoo webcams chat, even if users were not identified as targets.
[26] Eg. State agents, State organs and State representatives and officials.
[27] Eliza Watt, 'The Right to Privacy and the Future of Mass Surveillance' (2017) 21 The International Journal of Human Rights 773, 785.
[28] Deeks (n 10) 315-16.

The lack and gap of international regulation on the matter became evident. Pressures to remedy this situation were exercised from different players: NGO's,[29] the United Nations,[30] private companies.[31] Even certain States advocated for the development of some sort of normative framework.[32] Indeed, because international law was so silent on the matter, it was 'an inappropriate and inadequate reference for either condemnation or justifications of actions involving intelligence gathering'.[33] All of these changes, and challenges, led to a new aspiration of States to put in place rules supervising surveillance activities.[34]

Section 2. Is espionage legal under international law?

With the international community being so quiet on the practice of peacetime espionage, its (il)legality is a question that no straightforward answer. Three positions can be identified in the international legal discourse addressing the issue: first, espionage is neither allowed nor prohibited under public international law (A); second, it is allowed (B); and, third, it is prohibited (C).

A. International law neither allows nor prohibits peacetime espionage

The majority position amongst international legal scholars is that surveillance practices for the purpose of intelligence gathering is neither allowed nor prohibited in international law.[35] In the absence of specific prohibition, the findings of the Permanent Court of International Justice in the *Lotus* case – as seen in the previous chapter- become pertinent: in the absence

[29] Amongst many others: Privacy International, 'Fighting Mass Surveillance in the Post Snowden Era' <https://privacyinternational.org/impact/fighting-mass-surveillance-post-snowden-era> accessed 29 August 2019.

[30] The debate that followed Snowden disclosures led the United Nations to decide to appoint a Special Rapporteur on the Right to Privacy: 'It is precisely the intersection of privacy with state security interests and surveillance in cyberspace that led to the creation of the Special Rapporteur's mandate in 2015 in the wake of the Snowden revelations ongoing since June 2013' in UNHRC, 'Report of the Special Rapporteur on the Right to Privacy – Note by the Secretariat (28 February 2018) UN Doc A/HRC/37/32, para 13.

[31] Max Ehrenfreund, 'Google, responding to Edward Snowden's leaks, challenges gag order on NSA' (*The Washington Post*, 19 June 2013) <https://www.washingtonpost.com/world/national-security/google-responding-to-edward-snowdens-leaks-challenges-gag-order-on-nsa/2013/06/19/e6bdea0a-d8ef-11e2-a9f2-42ee3912ae0e_story.html?noredirect=on> accessed 19 August 2019.

[32] For example, Dilma Rousseff stated at the UN General Assembly in 2013 that: 'The United Nations must play a leading role in the effort to regulate the conduct of States with regard to these technologies. For this reason, Brazil will present proposals for the establishment of a civilian multilateral framework for the governance and use of the Internet and to ensure the effective protection of data that travels through the web.' in H.E. Dilma Rousseff, 'Statement at the Opening of the General Debate of the 68th Session of the United Nations General Assembly' (New York, 24 September 2013) <https://gadebate.un.org/sites/default/files/gastatements/68/BR_en.pdf> accessed 19 August 2019.

[33] Desmaret (n 7) 321.

[34] For a detailed analysis of why States want to regulate foreign surveillance; *See* Deeks (n 10) 327-628. She identifies three main reasons: 'a personalized and widespread understanding of the way in which foreign government surveillance affects individuals on an intimate level […] An unusual alignment of interests among corporations, elite opinions and ordinary citizens pointing in a pro-regulation direction [and the fact that] the governments most impacted by the Snowden revelations are Western democracies, which are sensitive to public-including international public- pressures'.

[35] Radsan (n 11) 596: 'My survey of the scholarship concludes by leaving us in an ambivalent position: espionage is neither legal nor illegal under international law. Espionage exists between the tectonic plates of legal systems' and at 605: 'espionage is neither condoned nor condemned under international law'; Christopher D Baker, 'Tolerance of International Espionage: A Functional Approach' (2004) 19 Am. U. Int'l L. Rev. 1091, 1092: 'international law neither endorses nor prohibits espionage, but rather preserve the practice as a tool by which to facilitate international cooperation' 1092.

of a specific positive rule in international law, States are free to act.[36] The Lotus principle has been discussed in more detail in the previous chapter on the questions of jurisdiction, but the logic of the argumentation has further consequences than jurisdictional matters. With this judgement, the Court discussed the nature of international law.[37] It implied that international law is by nature permissive: actions by States should be regarded as permitted, unless explicitly prohibited.[38] The opposite approach is to consider that a certain behaviour is only allowed if a rule says so.[39]
As demonstrated in the previous chapter concerning jurisdiction, the Lotus position, notwithstanding that it has been thoroughly criticized[40], seems to be *de facto* the one adopted by most States and scholars. If international law is silent on the (il)legality of surveillance practices, this has to mean that the practice is unregulated. If the practice is unregulated, nothing stops States from engaging in such activity: they may spy on each other- and on each other's citizens.[41]

B. International law allows spying

Another approach on the legality of online surveillance is that international law positively allows it. The end result is the same with the one arrived at under the 'Lotus approach' (surveillance is not considered as violating international law) but the reasoning is different. Rather than deeming the legality as emerging from an unregulated status quo, the proponents of this position affirm that international law actually permits surveillance practices.

The partisans of this position usually base their argumentation on two points: the existence of a widespread State practice showing that all States engage in such activities asserting a rule of customary international law and a specific interpretation of the principle of self-defence as allowing surveillance. The argument goes that States have always engaged in surveillance practices, trying to gather intelligence on their neighbours and potential enemies.[42] There are multiple statements by State officials acknowledging that governments participate in such activities and addressing issues or justifications for their existence.[43] According to certain authors, decades of State practice would therefore be the proof that

---

[36] *Case of the S.S. 'Lotus' (France v Turkey*) Judgment No. 9 (7 September 1927) PCIJ Reports 1928, Series A, No 10. 19 (hereinafter Lotus case).
[37] Jan Klabbers, *International Law* (CUP, 2013) 22.
[38] Lotus case (n 36) 19. For more details on this, See Chapter IV of this thesis.
[39] Klabbers (n 37) 22.
[40] Cedric Ryngaert, *Jurisdiction in International Law* (OUP, 2008) 21.
[41] Deeks (n 10) 301.
[42] Roger D Scott, 'Territorially Intrusive Intelligence Collection and International Law' (1999) 46 A.F.L. Rev. 217, 218: 'Espionage has been practiced by the nations of the world for centuries'; Jeffrey H Smith. 'Symposium: State Intelligence Gathering and International Law: Keynote Address' (2007) 28 Mich J. Int'l *L. 5*43, 544: 'virtually every State has an intelligence service that seeks to collect information on potential adversaries'; Christopher D Baker, 'Tolerance of International Espionage: A Functional Approach' (2004) 19 Am. U. Int'l L. Rev. 1091, 1091: 'all developed nations, as well as many less-developed ones, conduct spying and eavesdropping operations against their neighbors'.
[43] Eg. Barack Obama, 'Speech on National Security Agency Data Collection Programs' (*The New York Times*, 17 January 2014) <https://www.nytimes.com/2014/01/18/us/politics/obamas-speech-on-nsa-phone-surveillance.html> accessed 15 August 2019; Alan Travis, 'UK-US surveillance regime: statements by political figures before the ruling' (*The Guardian*, 6 February 2015) <https://www.theguardian.com/uk-news/2015/feb/06/mass-surveillance-gchq-key-statements-political-figures> accessed 15 August 2019.

international law accepts surveillance activities.[44] Jeffrey Smith, former General Counsel of the CIA, for example has said: 'Because espionage is such a fixture in international affairs, it is fair to say that the practice of states recognizes espionage as a legitimate function of the state, and therefore it is legal as a matter of customary international law'.[45] In the words of Christopher Baker:

> As a result of its historical acceptance, espionage's legal validity may be grounded in the recognition that 'custom' serves as an authoritative source of international law. According to this argument, international espionage is legal because states have spied and eavesdropped on each other throughout history.[46]

These two authors refer to the existence of a widespread practice of States engaging in surveillance. Widespread practice, however, is only one of the two constituting elements of international customary law. The existence of an international customary norm is proven by a widespread State practice *and* a correlated *opinio juris.*[47] Can the necessary *opinio juris* be identified in the context of surveillance? Do States conceive their surveillance activities as legal? There is no denying that States do engage in surveillance activities in a regular basis. But what legal status do they attach to such conduct? States generally do not seem to react to surveillance practice as violating international law.[48] But 'not a violation' does not necessarily mean that they actually think that online surveillance is positively allowed. Debates amongst scholars on the legal status of peacetime espionage are still ongoing, while on the other hand the majority of States is quasi-silent on the question. This lack of consensus makes it difficult to affirm without any doubt the existence of the *opinio juris* element. Therefore, establishing the existence of a customary rule *allowing* peacetime espionage does not seem possible at this point. Only one element of custom can be identified without doubt: the widespread practice. When it comes to proving the requisite *opinio juris*, there does not seem to be enough ground to affirm its existence. Affirming that espionage is legal because it's practised by many States only does half of the job.

Another argument advanced to justify that public international law actually allows espionage is to interpret the right to self-defence as including spying activities. Under Article 51 of the United Nations Charter and customary international law States have an inherent right to self-defence against armed attacks.[49] A branch of the scholarship writing on surveillance has advanced the argument that surveillance has been necessary to effectively exercise the right of States to self-defence because it has been an integral part of it:[50] gathering information on foreign military and political intentions is an indispensable part of effectively anticipating a

---

[44] William C Banks, 'Cyber Espionage and Electronic Surveillance: Beyond the Media Coverage' (2017) 66 Emory Law Journal 513, 518.
[45] Smith (n 42) 544.
[46] Baker (n 42) 1094-5.
[47] *North Sea Continental Shelf Cases* [1969] ICJ Rep 3; *Jurisdictional Immunities of the State (Italy v Germany)* [2012] ICJ Rep 99; Martin Dixon, *International Law* (7th edn, OUP, 2013) 36.
[48] Eg. Smith (n 42) 544: 'I can recall no instance in which a receiving state has said that these activities violate international law'; Baker (n 42) 1094: 'Although no international agreement affirmatively endorses espionage, states do not reject it as a violation of international law.'
[49] Charter of the United Nations (adopted 26 June 1945, entered into force 24 October 1945) art 51.
[50] Scott (n 42) 225: 'the surreptitious collection of intelligence in the territory of other nations that present clear, articulable threats based on their past behavior, capabilities, and expressions of intent, may be justified as a practice essential to the right of self-defense.'

potential threat of an armed attack.[51] To consider spying as unlawful would therefore undermine the right to self-defence, something that States would not support.[52] This is, however, a far-reaching interpretation of the right to self-defence and is only supported by a minority of scholars.

C. International law prohibits espionage

Finally, certain scholars argue that espionage is actually prohibited in international law. Manuel Garcia-Mora, for example, asserts that peacetime espionage is a violation of international law.[53] This, however, does not seem to be supported by States' behaviour. As mentioned above, when addressing the question of surveillance practices, and even when facing strong public scrutiny, Sates do not seem to react to espionage as a violation of international rules.

Although it may be difficult to uphold the position that international law prohibits peacetime espionage *per se*, other foundational principles of the international legal system might be interpreted as prohibiting peacetime surveillance. The principle of sovereignty and non-intervention[54] are both essential pillars of general international law.[55] These two rules are interlinked and have the status of customary international law.[56]

From this perspective, it could be argued that spying activities violate the sovereignty of the State that is subject to surveillance activities, also violating its territorial integrity. Quincy Wright writes, for example, that:

> In time of peace (…) espionage and in fact any penetration of the territory of a state by agents of another sates in violation of the local law, is also a violation of the rule of international law imposing a duty upon states to respect the territorial integrity and political independence of other states.[57]

But the type of surveillance Wright refers to is carried on by agents- individuals- clearly entering another State's territory. Is it really the same scenario when surveillance is carried

---

[51] Baker (n 42) 1096: 'in order to ensure that the right to self-defense retains a substantive meaning, international law must permit States to predict armed attack. Therefore, for States to enjoy the positively-codified right to self-defense, they should retain the right to acquire information that would indicate whether they face imminent armed attack.'

[52] Forcese (n 12) 199; Deeks (n 10) 302; Baker (n 42) 1096: stating that the right to self-defence would be empty without the possibility for States to legally prepare themselves against armed attack, and the need for them to appreciate unfriendly States' intentions.

[53] Manuel R Garcia-Mora, 'Treason, Sedition and Espionage as Political Offenses Under the Law of Extradition' (1964) 26 U. Pitt. L. Rev. 65, 79-80. See also Ingrid Delupis, 'Foreign Warships and Immunity for Espionage' (1984) 78 Am. J. Int'l L. 53, 67.

[54] UN Charter (n 49) art 2(1) and (7).

[55] Declaration on Principles of International Law Concerning Friendly Relations and Co-operation among States in Accordance with the Charter of the United Nations, UNGA Res 2625 (XXV) (24 October 1970) UN Doc A/RES/25/2625; *Case Concerning Military and Paramilitary Activities in and against Nicaragua (Nicaragua v United States of America)* [1986] ICJ Rep 14: paras 202-05 concerning the principle of non-intervention and paras 212-14 concerning the principle of sovereignty.

[56] Philip Kuning, 'Intervention, Prohibition of' (April 2008) *Max Planck Encyclopedias of International Law* (OUP) <https://opil-ouplaw-com.ezproxy.lib.gla.ac.uk/view/10.1093/law:epil/9780199231690/law-9780199231690-e1434> accessed 11 September 2019.

[57] Quincy Wright, 'Espionage and the Doctrine of Non-Intervention in Internal Affairs' in *Essays on Espionage and International Law* (Roland J Stanger ed, 1962) 12.

on electronically? Technological progress allowed States to spy over other governments and their citizens without having to enter their territory, or even airspace.[58]

Even if both these principles could be interpreted as impinging upon the legality of surveillance practices, States' behaviour doesn't seem to support this conclusion. State do not frame peacetime espionage as illegal and the fact that they so heavily participate in such activity makes it difficult to argue that these two principles are understood as prohibiting spying.[59]

D. Conclusion

The very fact that there are three different positions on the question whether peacetime espionage is allowed or not under international law illustrates the legal opacity around the field of surveillance. The mere existence of such an unresolved debate seems to indicate that the first opinion is probably the correct one: international law does not pronounce itself clearly on surveillance practices and therefore neither allows nor prohibits it. If spying is prohibited in the vast majority of domestic legal systems, when it comes to its regulation at the international level, States seem 'content with an artful ambiguity on the question'.[60]

Part II. International Human Rights Law

The second part of this chapter looks at the conformity of surveillance practices with international human rights law. It has been repeatedly asserted that:

> it is of utmost importance that States respect the right to privacy, which is based on human dignity, on a global level. Surveillance activities (…) must only be carried out in compliance with fundamental human rights such as privacy. Any national laws or international agreements disregarding this fact, must be considered outdated and incompatible with the universal nature of privacy and fundamental rights in the digital age.[61]

---

[58] The Tallinn Manual on cyber operations states that: "Cyber espionage *per se*, as distinct from the underlying acts that enable the espionage (see discussion in Rule 32), does not qualify as intervention because it lacks a coercive element" in Michael Smith (ed), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (CUP 2017) 323. But its Rule 32 states that: "Although peacetime cyber espionage by States does not per se violate international law, the method by which it is carried out might do so." The Experts agreed that "there is no prohibition of espionage *per se*, they likewise concurred that cyber espionage may be conducted in a manner that violates international law due to the fact that certain of the methods employed to conduct cyber espionage are unlawful. The Experts noted in particular that this may be the case with regard to respect for the principle of sovereignty (Rule 4) and the prohibition of intervention (Rule 66)." 170.
For an example of a surveillance activity that do not even enter another State's territory: *See* the example given by Deeks (n 10) 305: 'Data packets that originate in Europe may pass through servers in the United States before being routed back to Europe. If the United States intercepts those packets while they are transiting the United States, it is hard to argue that the United States has violated the territorial integrity of the states from which the packets originated. When states conduct surveillance from within a host state, however, a stronger argument can be made that a violation of the host state's territorial integrity has occurred.'

[59] Deeks (n 10) 305.

[60] Forcese (n 12) 204.

[61] UNHRC, 'Report of the Special Rapporteur on the right to privacy, Joseph A Cannataci – Note by the Secretariat' (27 February 2017) UN Doc A/HRC/34/60, para 29 (hereafter Cannataci Second Report).

Hence, this part tries to unpack what it means for surveillance activities to 'be carried out in compliance with' the right to privacy: how the current legal framework on the right to privacy is interpreted and applied to surveillance practices at the moment (Section 1) and what are the calls for new developments to be enacted to answer more efficiently these new challenges. This latter inquiry will look both at attempts to interpret more broadly the existing standards and at opinions advocating the enactment of a brand new legal instrument to regulate online surveillance (Section 2).

Section 1. Online Surveillance and the Right to Privacy

As we have detailed in Chapter 2 of this thesis, the right to privacy is regulated at the international level by many different instruments, both at global and regional level. Despite the fact that as already demonstrated the content and scope of these protections, and the various provisions that comprise them, are still open to debate, no doubt exists about their existence and widespread recognition.

The idea that human rights, including the right to privacy, apply online to the same extent that they do offline is generally accepted,[62] but its application and interpretation in practice is far from straightforward. The lack of consensus on the substantive content of the right to privacy has proven rather problematic when assessing the legality of surveillance practices. Outrage has indeed followed the Snowden revelations[63] but no agreement has formed on the way to bring so far unregulated surveillance activities in line with human rights standards. The silence of international law with regard to online surveillance and the extensive programmes ran by States to conduct large scale covert surveillance have been identified as seriously hindering respect for the right of privacy.[64] A few pertinent questions in that regard are how electronic surveillance infringes upon people's privacy and how we assess whether it violates the right to privacy.

The following discussion mainly addressed the interpretation of two, central to the matter, provisions: Article 17 of the ICCPR[65], which is considered to be 'the most important legally binding treaty provision on the human right to privacy at the universal level'[66]- and Article 8 of the ECHR, as the Strasbourg Court has been at the forefront of dynamically interpreting privacy protections in the surveillance context.

---

[62] UNHRC, 'The Promotion, Protection and Enjoyment of Human Rights on the Internet' (20 June 2012) UN Doc A/HRC/20/L.13, para 1; UNGA Res 68/167, 'The Right to Privacy in the Digital Age' (18 December 2013) UN Doc A/RES/68/167, 3.

[63] Eg. Dilma Roussef (n 32) 1-2: 'Recent revelations concerning the activities of a global network of electronic espionage have caused indignation and repudiation in public opinion around the world. (…) Tampering in such a manner in the affairs of other countries is a breach of International Law (…) We face, Mr. President, a situation of grave violation of human rights and of civil liberties.'

[64] UNGA, 'Right to Privacy: Note by the Secretary General transmitting the Report of the Special Rapporteur of the Human Rights Council on the Right to Privacy, Joseph A Cannataci' (19 October 2017) UN Doc A/72/540, para 4.

[65] International Covenant on Civil and Political Rights (adopted 16 December 1966, entered into force 23 March 1976) 999 UNTS 171, art 17.

[66] UNHRC, 'Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Martin Scheinin' (28 December 2009) UN Doc A/HRC/13/37, para 14.

Both Article 17 ICCPR[67] and Article 8 ECHR[68] make clear that the right to privacy is not absolute. It is a qualified right, which can be limited under certain conditions. In the language of the ICCPR, interferences with the right to privacy can be accepted, but not if they are arbitrary or unlawful. The ECHR for its part is more explicit in that respect, containing a limitation clause which lists the precise conditions under which an interference with the right to privacy can be justified. Therefore, in order to assess whether there has been a violation of the right to privacy under international human rights law by a surveillance measure, two questions need to be answered: first, is there an interference with the individual's privacy (A); second, if an interference has occured, can it be justified (B)?

A. Is there an interference?

The very first question to be answered is an obvious one: does the measure of surveillance at stake amount to an interference with the right to privacy? This, in turns, is connected to the question what kind of harm does surveillance cause upon an individual's privacy. The notion of harm has been a complicated one in the field of privacy and it has sometimes been difficult to substantiate exactly the harm specific violations have caused.[69] 'Traditional' privacy intrusions, such as for example searches or telephone wiretapping, are delimited in time, place, and person. But the new possibilities created by information technologies, such as the Internet, have created an entirely different environment.[70] If individuals do not even realise that they are being subjected to surveillance or that their personal data are being collected, the question arises whether they can really claim to have been harmed. In such cases, we need to ask whether an interference has taken place and whether a violation of the individual's right to privacy has really occurred.
In answering these questions, we will see that, first, certain online surveillance measures have straightforwardly been qualified as interfering with the right to privacy and, second, that courts, especially the European Court of Human Rights, have thoroughly discussed the 'victim status' of individuals claiming to be subject of surveillance measures.

A.1. Types of Actions

Different types of actions have so far been qualified as interference with an individual's privacy. One of the main points of reference in interpreting the notion of interference contained in the ICCPR is General Comment No 16 of the Human Rights Committee, which

[67] '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' (emphasis added), ICCPR (no 65), art 17.
[68] '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' (emphasis added). Convention for the Protection of Human Rights and Fundamental Freedoms (adopted 4 November 1950, entered into force 3 September 1953) 213 UNTS 221, art 8.
[69] Bart van der Sloot, 'Is the Human Rights Framework Still Fit for the Big Data Era? A Discussion of the ECtHR's Case Law on Privacy Violations Arising from Surveillance Activities' in Serge Gutwirth et al. (eds), *Data Protection on the Move* (Springer 2016) Law, Governance and Technologies Series 24, 414.
[70] Ibid, 414.

as already discussed in Chapter II focuses on Article 17.[71] According to the Committee: 'Compliance with article 17 requires that the integrity and *confidentiality of correspondence* should be guaranteed de jure and de facto. Correspondence should be delivered to the addressee *without interception* and without being opened or otherwise read.'[72] This obligation means that '[s]urveillance, whether electronic or otherwise, interceptions of telephonic, telegraphic and other forms of communication, wire-tapping and recording of conversations should be prohibited',[73] while it is required that 'the gathering and holding of personal information on computers, data banks and other devices, whether by public authorities or private individuals or bodies, must be regulated by law'.[74] Even though General Comment No 16 was issued in 1988, what the Committee is saying seems rather straightforward: any kind of interception of correspondence, surveillance, and collecting of personal data amounts to an interference with the right to privacy. The further use of the information collected is not a decisive factor: any capture, collection, retention of personal information creates an interference with privacy.[75]

The European Court of Human Rights (ECtHR) has dealt with many claims concerning a wide range of surveillance measures. As a result, it developed an extensive case-law on the question and has established early on principles on targeted surveillance measures such as telephone tapping. When new technologies emerged, and consequently new means of surveillance came to the forefront, the ECtHR already had a solid case-law assessing the legality of more traditional, targeted, surveillance activities. To deal with the new situation it continued to interpret extensively and dynamically the scope of Article 8 of the ECHR, and its precedent findings. The Court has stated numerous times that telephone conversations and emails are included in the notions of private life and correspondence.[76] The following actions have been found as amounting to an interference with the right to respect of private life: the storage and release of private information without the possibility for the individual concerned to refuse it,[77] the interception of telephone calls[78] or electronic communications[79], the collection of a communication's metadata,[80] the systematic storage and collection of

[71] UNHRC, 'General Comment No. 16: Article 17 (Right to Privacy): The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation' (8 April 1988) UN Doc HRI/GEN/1/Rev.9 (Vol. I).
[72] Ibid, para 8.
[73] Ibid, para 8.
[74] Ibid, para 10.
[75] UNHRC, 'The Right to Privacy in the Digital Age: Report of the Office of the United Nations High Commissioner for Human Rights' (30 June 2014) UN Doc A/HRC/27/37, para 20. (hereinafter 'High Commissioner Report').
[76] Telephone conversations: *Klass and others v Germany*, App no 5029/71 (Judgment) (6 September 1978) para 41; *Malone v United Kingdom*, App no 8691/79 (Merits) (2 August 1994) para 64; *Amann v Switzerland*, App no 27798/95 (16 February 2000) para 44; *Liberty and Others v United Kingdom*, App no 58243/00 (1 July 2008), para 56; *Roman Zakharov v. Russia,* App no 47143/06 (Judgment) (4 December 2015), para 173. Emails: *Copland v the United Kingdom*, App no 62617/00 (Judgment) (3 April 2007) para 41; *Kennedy v United Kingdom,* App no 26839/05 (Judgment) (18 May 2010), para 118: 'it is not disputed that mail, telephone and email communications, including those made in the context of business dealings, are covered by the notions of 'private life' and 'correspondence' in Article 8 §1.'
[77] *Leander v Sweden*, App no 9248/81 (Judgment) (1987) para 48; *Amann* (n 76) para 69; *S and Marper v United Kingdom*, App nos 30562/04 and 30566/04 (4 December 2008) para 67.
[78] *Kopp v Switzerland*, App no 13/1997/797/1000 (25 March 1998) para 53 ('the subsequent use of the recordings made has no bearing on that finding'); *Amann* (n 76) para 45.
[79] *Szabo and Vissy v Hungary,* App no 37138/14 (6 June 2016) para 52.
[80] *Malone* (n 76) para 84.

data,[81] even if data was collected in a public place,[82] or concerned exclusively the person's professional or public activities,[83] and 'the transmission of data to and their use by other authorities'.[84]

A.2. Victim status of an individual complaining of secret surveillance measures

A.2.1. ECtHR case law

According to Article 34 of the ECHR, an individual may only bring a case before the Court if he or she has a personal interest in it, i.e. only if he or she has been the victim of a violation by one of the State Parties to the Convention.[85] In terms of Article 8, individuals have to show that they have been victims of a violation of this provision, meaning they have to prove a personal and concrete injury. Specifically in the context of online surveillance, the relevant questions then are what kind of harm surveillance programmes may cause and how individuals can even know that they are subject to mass surveillance programmes potentially violating their rights, let alone actually prove a direct, concrete personal interest.

In 1978, the Court pronounced for the first time on the victim requirement in the context of surveillance activities in the case of *Klass and others v Germany*.[86] The Court held:

> The question arises in the present proceedings whether an individual is to be deprived of the opportunity of lodging an application with the Commission because, *owing to the secrecy* of the measures objected to, *he cannot point to any concrete measure specifically affecting him.* In the Court's view, the effectiveness (l'effet utile) of the Convention implies in such circumstances some possibility of having access to the Commission. If this was not so, the efficiency of the Convention's enforcement machinery would be materially weakened. (…) The Court therefore *accepts that an individual may, under certain conditions, claim to be the victim of a violation occasioned by the mere existence of secret measures or of legislation permitting secret measures, without having to allege that such measures were in fact applied to him.* The relevant conditions are to be determined in each case according to the Convention right or rights alleged to have been infringed, the secret character of the measures objected to, and the connection between the applicant and those measures.[87]

---

[81] *Leander* (n 77)*, S and Marper* (n 77).
[82] *Peck v United Kindom,* App no 44647/98 (Judgment) (28 January 2003) para 59, *P.G. and J.H. v. the United Kingdom,* App no 44787/98 (Judgment) (25 September 2001), paras 57-59, *Shimovolos v Russia*, App no 30194/09 (Judgment) (21 June 2011).
[83] *Amann* (n 76) paras 65-67; *Rotaru v Romania,* App no 28341/95 (Judgment) (4 May 2000) paras 43-44.
[84] *Weber and Saravia v Germany,* App 54934/00 (Decision as to Admissibility) (29 June 2006*)* para 79: 'the transmission of data to and their use by other authorities, which enlarges the group of persons with knowledge of the personal data intercepted and can lead to investigations being instituted against the persons concerned, constitutes a further separate interference'.
[85] Article 34 of the ECHR (n 68) reads: 'The Court may receive applications from any person, nongovernmental organisation or group of individuals claiming to be the victim of a violation by one of the High Contracting Parties of the rights set forth in the Convention or the Protocols thereto. The High Contracting Parties undertake not to hinder in any way the effective exercise of this right.'
[86] *Klass and others* (n 76).
[87] Ibid*,* para 34 (emphasis added).

The Court then decided specifically the question of the existence of an interference with Article 8. After recalling that telephone conversations fell indeed under the scope of 'private life' and 'correspondence',[88] the Court said:

> Clearly, any of the permitted surveillance measures, once applied to a given individual, would *result in an interference* by a public authority with the exercise of that individual's right to respect for his private and family life and his correspondence.
>
> Furthermore, in the *mere existence of the legislation* itself there is involved, for all those to whom the legislation could be applied, a menace of surveillance; this menace necessarily strikes at *freedom of communication* between users of the postal and telecommunication services and *thereby constitutes an 'interference by a public authority'* with the exercise of the applicants' right to respect for private and family life and for correspondence.[89]
>
> (…)
>
> The Court points out that where a State institutes secret surveillance the existence of which remains unknown to the persons being controlled, with the effect that the surveillance remains unchallengeable, *Article 8 ... could to a large extent be reduced to a nullity*. It is possible in such a situation for an individual to be treated in a manner contrary to Article 8 …, or even to be deprived of the right granted by that Article (art. 8), without his being aware of it and therefore without being able to obtain a remedy either at the national level or before the Convention institutions. (…) *The Court finds it unacceptable that the assurance of the enjoyment of a right guaranteed by the Convention could be thus removed by the simple fact that the person concerned is kept unaware of its violation.*[90]

This judgment is important because it addresses two vital points. The first one is the situation where individuals could have their right to privacy infringe upon without them even being aware of it happening. The Court clearly accepts that an individual can claim to be the victim of a violation of the ECHR, even if he or she is not able to prove that he or she has been 'subject to a concrete measure of surveillance'. [91] The Court therefore agreed to receive an *in abstracto* claim, as not doing so would have led to a real gap in the protection granted by the Convention. The requirement to prove a concrete and personal injury was therefore discarded in the context of secret surveillance measures. The second important point made by the Court is that the '*mere existence* of the legislation itself there is involved (…) a menace of surveillance; this menace necessarily strikes at freedom of communication (…) and thereby constitutes an 'interference by a public authority''.[92] Equating the 'mere existence of legislation' to an interference is a bold move. It is also one of the rare instances in which the Court has expanded a little on its understanding of the nature of interference caused by surveillances practices, that is that they hinder the freedom of communications. This approach by the Court reinforces drastically the protection granted by the ECHR and ensures that surveillance activities fall under its scope. It has been since reiterated in several

[88] Ibid, para 41.
[89] Ibid, para 41 (emphasis added).
[90] Ibid, para 36 (emphasis added).
[91] Ibid, para 38.
[92] Ibid, para 41.

cases,[93] including one involving the secret bulk surveillance of international wireless communications.[94]

In 1997, in *Halford v* UK, the Court diverged slightly and introduced the criterion of 'likelihood of interception; in order to assess the victim status of the applicant:

> The evidence justifies the conclusion that *there was a reasonable likelihood* that calls made by Ms Halford from her office were intercepted by the Merseyside police (…) This interception constituted an 'interference by a public authority', within the meaning of Article 8 para. 2 (art. 8-2), with the exercise of Ms Halford's right to respect for her private life and correspondence.[95]

This approach of 'reasonable likelihood' was favoured by the former Commission, which it applied in several cases.[96] The Commission thought that the *Klass and others* and *Malone* positions could not imply that anyone who worried they might be surveilled upon by the UK secret services might claim an interference with their rights. However, the Court used it again in 2008.[97]

The Court eventually summarized and clarified its case-law in the *Kennedy v UK* case.[98] It started its reasoning by recalling that it usually does not review the relevant law and practice *in abstracto* but assess if the way they have been applied in a particular case has given rise to a violation of the Convention. However, it pointed out that in the particular context of secret surveillance measures, the Court has accepted such abstract claims in order to effectively supervise and control such activities.[99] It acknowledged that two different approaches have been taken in the past: on one hand, the '*Klass and others*' position has been used when the individual brought a general complaint about legislation allowing secret surveillance measures. On the other hand, if the claimant argued that he or she was the victim of an actual interception, they had to prove that there was a reasonable likelihood that they were actually the target of such surveillance measures ('*Halford* test')[100]. It then specified:

> In order to assess, in a particular case, whether an individual can claim an interference as a result of the mere existence of legislation permitting secret surveillance measures, the *Court must have regard* to the *availability of any remedies* at the national level and the *risk of secret surveillance measures being applied* to him.[101]

---

[93] *Malone* (n 76) para 64; *Association for European Integration and Human Rights and Ekimdzhiev v Bulgaria* (Judgement) App no 62540/00 (28 June 2007) paras 58-60; *Iliya Stefanov v Bulgaria*, App no 65755/01 (Judgment) (22 May 2008) para 49; *Liberty and Others* (n 76) paras 56 and 57; and *Iordachi and Others v Moldova*, App no 25198/02 (Judgment) (10 February 2009) paras 30-35.
[94] *Weber and Saravia* (n 84) para 78: 'the mere existence of legislation which allows a system for the *secret monitoring of communications* entails a threat of surveillance (…) and thereby amounts in itself to an interference'.
[95] *Halford v United Kingdom*, App no 20605/92 (Judgment) (25 June 1997) paras 47-48.
[96] *Esbester v United Kingdom*, App no 18601/91 (2 April 1993); R*edgrave v United Kingdom*, App no 202711/92 (1 September 1993); and *Matthews v United Kingdom*, App no 28576/95 (16 October 1996).
[97] *Iliya Stefanov v Bulgaria* (n 93) paras 49-50.
[98] *Kennedy v United Kingdom* (n 76).
[99] Ibid, para 119.
[100] Ibid*,* para 123.
[101] Ibid*,* para 124 (emphasis added). It continued: 'Where there is no possibility of challenging the alleged application of secret surveillance measures at domestic level, widespread suspicion and concern among the

The Court therefore seems to have added two more conditions for an individual to be able to contest the mere existence of legislation allowing secret surveillance, departing from its position in *Klass and others*: the Court needs to take into consideration the availability of remedies at the domestic level and the risk for the claimant to actually be targeted by the surveillance measures. In *Zakharov v Russia*, the Court confirmed the two parallel approaches to assessing the victim status of a clamant in secret-surveillance cases.[102] The Court pointed out that when claimants made both general complaints concerning legislation and allegations of actual interception of their communication, the Court used both tests.[103] The Court therefore decided to harmonize its position and declared that the approach taken in the *Kennedy* case was the one to follow.[104] It proceeded to detail the two conditions evoked five years before for cases where the individual made a *general* claim[105]: it will first look at the scope of the legislation allowing the surveillance measures in order to assess the risk of the claimant to have been targeted (either because the legislation in question authorizes the surveillance of all users or because the applicant belong to a group of people targeted specifically by the measure), and secondly the degree of scrutiny will vary depending on the effectiveness of the available remedies at the domestic level.[106]

> As the Court observed in *Kennedy*, where the domestic system *does not afford an effective remedy* to the person who suspects that he was subjected to secret surveillance, widespread suspicion and concern among the general public that secret surveillance powers are being abused cannot be said to be unjustified … In such circumstances the threat of surveillance can be claimed in itself to *restrict free communication* through the postal and telecommunication services, *thereby constituting for all users or potential users a direct interference* with the right guaranteed by Article 8. There is therefore a greater need for scrutiny by the Court, and an exception to the rule denying individuals the right to challenge a law *in abstracto* is justified. In such cases the *individual does not need to demonstrate the existence of any risk that secret surveillance measures were applied to him*.
>
> By contrast, if the national system *provides for effective remedies*, a widespread suspicion of abuse is more difficult to justify. In such cases, the individual may claim to be a victim of a violation occasioned by the mere existence of secret measures or of legislation permitting secret measures *only if he is able to show that,*

---

general public that secret surveillance powers are being abused cannot be said to be unjustified. In such cases, even where the actual risk of surveillance is low, there is a greater need for scrutiny by this Court' (para 124).

[102] *Zakharov* (n 76) paras 167-168: a criteria of 'reasonable likelihood' needing to be proven in case where the applicant alleged actual interceptions of their communications and the 'Klass and others approach' consisting of accepting that the mere existence of legislation allowing secret surveillance measures entailed a threat of surveillance for all those who could be subject to that legislation.

[103] Ibid, paras 167-168: 'Reasonable likelihood' test was used in *Esbester*; *Redgrave*; *Matthews* (n 96); and the 'Klass and others approach' was applied in *Malone* (n 76) para 62, and *Liberty and Others* (n 76) paras 41-42.

[104] Ibid, para 171: 'In the Court's view the *Kennedy* approach is best tailored to the need to ensure that the secrecy of surveillance measures does not result in the measures being effectively unchallengeable and outside the supervision of the national judicial authorities and of the Court.'

[105] Meaning when the applicant claims to be the victim of a violation occasioned by the mere existence of secret surveillance measures or legislation allowing such measures.

[106] *Zakharov* (n 76) para 171.

due to his personal situation, he is potentially at risk of being subjected to such measures.[107]

This position has been followed in subsequent case law.[108] It shows a clear desire from the Court, for the last forty years, to grant individuals the possibility to challenge secret surveillance practices that might violate their right to privacy. The Court has tried to enhance the existing legal protection and make sure that the secrecy of such surveillance does not allow them to become unchallengeable or be outside judicial supervision. This illustrates perfectly how existing traditional international standards (such as the prohibition of *in abstracto* claims) can be 'stretched' to respond to the reality created by secret surveillance measures. The Court has made sure that the provision of Article 8 of the ECHR stays relevant to respond the new challenges and potential new threats in the 21st century.

A.2.2 Consequence at the international level

How is the concept of 'interference' contained in the ICCPR interpreted? Could an individual challenge before the Committee the mere existence of legislation allowing secret surveillance as interfering with the right to privacy? The HR Committee has not yet had a chance to decide the question, but the UN seems to follow the position taken by the ECtHR. The High Commissioner for Human Rights stated in 2014 that: 'the mere possibility of communications information being captured creates an interference with privacy. (…) The very existence of a mass surveillance programme creates an interference with privacy'.[109]

On the other hand, the widespread practice of online surveillance by almost all States indicates that States would generally be unwilling to accept such a far-reaching interpretation. It is also very doubtful that the United States would agree with that interpretation. The United States took another approach to assess the question of standing in court for applicants challenging the legality of secret surveillance measures. In 2008, Yahoo, an online service and search engine provider, was allowed to support its users' Fourth Amendment rights and was found as having standing[110] to challenge a surveillance measures established under the Protect America Act.[111] In 2013, however, when a group of human rights lawyers, journalists and human rights activists challenged the Section 702 of the Foreign Intelligence Surveillance Act[112] in front of the US Supreme Court in *Clapper v Amnesty International USA*,[113] the Court denied the applicants standing.[114] This was due to the fact that they could not prove 'an injury in fact', meaning they could not show they had

[107] Ibid, para 171 (emphasis added).
[108] *Szabo and Vissy* (n 79) paras 36-39; ECtHR, *Centrum Rattvisa v Sweden*, App no 35252/08 (19 June 2018) paras 90-95.
[109] High Commissioner Report (n 75) para 20.
[110] In re Directives to Yahoo! Inc., Pursuant to Section 105B of the Foreign Intelligence Surveillance Act, No. 08-01, 2008 WL 10632524 (FISA Ct. Rev. Aug. 22, 2008) 3-4.
[111] Pub. L. No 110-55, 121 Stat. 552 (repealed in 2008).
[112] FISA Amendment Act §702, codified as U.S. Code §1881a.
[113] *James R Clapper, Jr., Director of National Intelligence, et al., Petitioners v. Amnesty International USA et al*. 568 U.S. 398 (2013).
[114] Standing in the United States is understood as 'under Article III of the Constitution requires that an injury be concrete, particularized, and actual or imminent; fairly traceable to the challenged action; and redressable by a favorable ruling.' *Monsanto Co. v. Geertson Seed Farms*, 561 U.S. 139 (2010) 149.

personally been monitored and suffered a harm occasioned by the measures established by the legislation in question.

The fact that the United States and the ECtHR took different positions on the issue of standing illustrates the difficulty of a harmonised international regulation of online surveillance activities. What could be seen as a technical interpretation of procedural norms (different requirements of standing in front of different courts) actually highlights different conceptualizations of how the legal system and privacy regulations should be applied to surveillance measures: one is trying to interpret dynamically the existing provisions in order to adapt to novel threats caused by online surveillance, while the other is sticking to a restrictive reading, regardless of technological advancements.

B. Is the interference justified?

Once the first question is answered and an interference with the right to privacy is indeed found, then it needs to be addressed whether such the interference is justified. Article 8 of the ECHR contains an express limitation clause in its second paragraph, which details specifically the conditions under which an interference with the right to privacy can be justified, namely such interference needs to be (i) in accordance with the law, (ii) necessary in a democratic society, and (iii) pursuing one of the interests listed in the article.

Article 17 of the ICCPR, on the other hand, prohibits unlawful and arbitrary interferences. It does not contain a specific limitation clause, so the body assessing a violation of Article 17 has to interpret these two criteria in order to decide if the interference at stake qualifies as such or not. Defining what constitutes an arbitrary and/or unlawful interference with the right to privacy is a difficult exercise in the context of surveillance and is 'one of the challenges of the next few years'.[115] The ICCPR contains other provisions with express clauses establishing permissible limitations.[116] The most detailed of these limitation clauses can be found in Article 21 (right to peaceful assembly)[117] and Article 22 (right to freedom of association)[118] . They both spell out three standards a restriction needs to meet in order to be justified: it needs to be (i) in conformity with the law (ii) necessary in a democratic society and (iii) it has to pursue one of the interests listed in the provision. The wording of these clauses is almost identical as the one found in Article 8 of the ECHR. The ICCPR was enacted in 1966, but its drafting process started as early as 1957 and was clearly influenced

[115] UNHRC, 'Summary of the Human Rights Council Panel Discussion on the Right to Privacy in the Digital Age' (19 December 1014) UN Doc A/HRC/28/39, para 44.
[116] ICCPR (n 65) arts 12(3), 18(3), 19(3), 21, 22(2).
[117] ICCPR (n 65) art 21: 'The right of peaceful assembly shall be recognized. No restrictions may be placed on the exercise of this right other than those imposed in conformity with the law and which are necessary in a democratic society in the interests of national security or public safety, public order (ordre public), the protection of public health or morals or the protection of the rights and freedoms of others'.
[118] ICCPR (n 65) art 22: '1. Everyone shall have the right to freedom of association with others, including the right to form and join trade unions for the protection of his interests.
2. No restrictions may be placed on the exercise of this right other than those which are prescribed by law and which are necessary in a democratic society in the interests of national security or public safety, public order (ordre public), the protection of public health or morals or the protection of the rights and freedoms of others. This article shall not prevent the imposition of lawful restrictions on members of the armed forces and of the police in their exercise of this right.'

by the legal developments happening in Europe at the time.[119] The reason why Article 17 does not have its own limitation clause while certain other provisions do, however, is not clear and the *travaux préparatoires* do not offer a clear answer to this question. But nonetheless, to interpret what 'unlawful' and 'arbitrary' means in the context of Article 17, the permissible limitation test of Article 21 and 22 have been found to apply. In 2009, Martin Scheinin- then Special Rapporteur on human rights and fundamental freedoms while countering terrorism, stated that:

> Despite the differences in wording, Article 17 of the Covenant should also be interpreted as containing the said elements of a permissible limitations test. Restrictions that are not prescribed by law are 'unlawful' in the meaning of Article 17, and restrictions that fall short of being necessary or do not serve a legitimate aim constitute 'arbitrary' interference with the rights provided under article 17.[120]

Frank La Rue, Special Rapporteur on the right to freedom of opinion and expression, followed the same reasoning four years later.[121] The Special Rapporteur on the right to privacy confirmed and detailed this position in February 2019:

> The essential, four-fold test is then that any legitimate infringement of privacy cannot be: a) arbitrary and must be provided for by law; b) for any purpose but for one which is necessary in a democratic society; c) for any purpose except for those of 'national security or public safety, public order, the protection of public health or morals or the protection of the rights and freedoms of others'; and, d) the measure must be proportionate to the threat or risk being managed.[122]

It can therefore be said that both the ICCPR and the ECHR contain the same permissible limitation standards: interference needs to be in accordance with the law (1) and it needs to be necessary in a democratic society to achieve a legitimate aim, which involves a proportionality test (2). The exact content of these standards is assessed in the two following sections.

B.1. Is the interference lawful/in accordance with the law?

The Human Rights Committee is very clear on 'unlawful' means:

> No interference can take place except in cases envisaged by the law. Interference authorized by States can only take place on the *basis of law*, which itself must comply with the provisions, aims and objectives of the Covenant[123].

---

[119] See *supra*: Chapter II.
[120] Scheinin (n 66) paras 16-17.
[121] La Rue (n 3) para 28: 'The framework of article 17 of the ICCPR enables *necessary, legitimate and proportionate restrictions* to the right to privacy by means of permissible limitations. In contrast with the provisions of article 19, paragraph 3, which spell out elements of a test for permissible limitations,13 the formulation of article 17 does not contain a limitation clause. *Despite these differences in wording, it is understood that article 17 of* the Covenant *should also be interpreted as containing elements of a permissible limitations* test already described in other General Comments of the Human Rights Committee.' (emphasis added). And at 29: 'the right to privacy should be subject to the same permissible limitations test as the right to freedom of movement, as elucidated in General Comment 27'.
[122] UNHRC, 'Right to privacy: Report of the Special Rapporteur on the Right to Privacy' (21 February 2019) UN Doc A/HRC/40/63, para 18 (hereinafter 'Report SRP February 2019').
[123] General Comment No 16 (n 71) para 3. (emphasis added).

It has also specified that: 'Even with regard to interferences that conform to the Covenant, relevant legislation must *specify in detail the precise circumstances* in which such interferences may be permitted.'[124]

'Law' has been interpreted by the Committee to mean 'a norm … formulated with sufficient *precision to enable an individual to regulate* his or her conduct accordingly and it must be made *accessible* to the public. A law *may not confer unfettered discretion* for the restriction of freedom of expression on those charged with its execution.'[125] Even though this interpretation was given in the context of the General Comment on the Freedom of Opinion and Expression, the qualification 'lawful' has been identically interpreted in the context of the right to privacy.

Surveillance measures, then, need to have a basis in national law and this legal basis needs to meet certain standards. The 'quality of the law' is therefore assessed.[126] Human rights bodies have interpreted 'lawfulness' as including three criteria: the national law needs to be accessible, offer some foreseeability for individuals, and be compatible with the rule of the law.[127] These criteria apply to legal frameworks establishing surveillance practices, such as interception of communications,[128] collection of personal data (including mass surveillance),[129] collection of metadata,[130] – essentially 'all types of surveillance activities […] including online surveillance for the purposes of State security'.[131]

B.1.1. Accessibility and Foreseeability

The accessibility requirement involves the publication of the legislative framework regulating surveillance measures. Full disclosure is not required as it could lead to surveillance being circumvented and therefore useless, but still a certain level of accessibility needs to be upheld.[132] The accessibility standard also requires the legal basis to be sufficiently precise.[133] This is meant to offer a certain form of foreseeability to individuals[134],

[124] Ibid, para 8. (emphasis added).
[125] UNHRC, General Comment No 34 on Article 19: Freedoms of opinion and expression (12 September 2011) UN Doc CCPR/C/GC/34, para 25. (emphasis added).
[126] *Taylor-Sabori v United Kingdom*, App no 47114/99 (Judgment) (22 October 2002) para 18: 'the phrase 'in accordance with the law' not only requires compliance with domestic law but also relates to the *quality of that law*, requiring it to be compatible with the rule of law'. (emphasis added).
[127] General Comment No 16 (n 71); *Silver and Others v United Kingdom*, Nos 5947/72, 6205/73, 7052/75, 7061/75, 7107/75, 7113/75 and 7136/75 (11 October 1980), para 87; Shimovolos (n 82) para 67; *Kruslin v. France,* App no 11801/85 (Judgment) (24 April 1990); *Lambert v. France*, App No 23618/94 (Merits and Just Satisfaction) (24 August 1998); and *Perry v United Kingdom*, App no 63737/00 (Judgment) (17 July 2003).
[128] UNGA Res 73/179, 'the Right to Privacy in the Digital Age' (17 December 2018) UN Doc A/RES/73/179.
[129] UNGA Res 72/180, 'Protection of Human Rights and Fundamental Freedoms while Countering Terrorism' (19 December 2017) UN Doc A/RES/72/180, para 5(j).
[130] The Office of the Special Rapporteur for Freedom of Expression of the Inter-American Commission on Human Rights, Freedom of Expression and the Internet (31 December 2013) para 153.
[131] HR Committee, 'Concluding observations on the fifth periodic report of Belarus' (22 November 2018) UN Doc CCPR/C/BLR/CO/5, para 44.
[132] Marko Milanovic, 'Human Rights Treaties and Foreign Surveillance' (2015) 56 Harvard International Law Journal 81, 135.
[133] General Comment No 16 (n 71) para 8.
[134] General Comment No 34 (n 125) para 25; HR Committee, *Van Hulst v Netherlands*, Communication No. 903/1999 (1 November 2004) UN DOC CCPR/C/82/D/903/1999, para 7.7.

as they should know the consequences a certain conduct might entail.[135] This does not mean that individuals should be able to anticipate exactly when they may be subject to surveillance, but they should be able to have an adequate indication of the circumstances and conditions under which authorities are empowered to engage in such measures.[136] This applies not only in the special context of interception of communications but also to general programmes of surveillance.[137]

This requirement is rather complicated for governments to meet when enacting secret surveillance programs. By nature, such activities are conducted covertly. The efficiency of surveillance tools depends on users' expectation that their communications or personal data are kept private, as this is what makes them worth prying upon in the first place.[138] Still, the High Commissioner for Human Rights has been clear that '[s]ecret rules and secret interpretations – even secret judicial interpretations – of law do not have the necessary qualities of "law".'[139] The Human Rights Committee has already warned several States that their regulations on surveillance do not meeting the clarity and foreseeability standards.[140]

B.1.2. Safeguards against abusive practice in the context of surveillance

There is a third element contained in the definition of 'law' given by the Human Rights Committee in its General Comment No 34: 'unfettered discretion' cannot be granted to authorities.[141] The secret nature of surveillance practices, and by correlation the lack of public scrutiny, increases the risk of governmental abuse of power. To counter that risk, the ECtHR established that certain standards needed to be present and detailed in any statutory law setting up secret surveillance schemes.[142] The ECtHR has developed six minimum

---

[135] High Commissioner Report (n 75) para 28.
[136] *Malone* (n 76) para 67; *Weber and Saravia* (n 84) para 93; *Zakharov* (n 76) 229; *Szabo v Hungary* (n 79) para 62, *Shimovolos* (n 82) para 68.
[137] *Liberty* (n 76) para 63: 'The Court does not consider that there is any ground to apply different principles concerning the accessibility and clarity of the rules governing the interception of individual communications, on the one hand, and more general programmes of surveillance, on the other.'
[138] UNGA, 'Promotion and protection of human rights and fundamental freedoms while countering terrorism: report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Ben Emmerson' (23 September 2014) UN Doc A/69/397, para 15; This is also the line of argumentation of the US and their allies to condemn Snowden disclosures: Eg. Clapper, Director of National Intelligence, stating in 2014: 'The profound damage that his [Snowdens] disclosures have caused and continue to cause. As a consequence, the nation is less safe and its people less secure' in James G Meeks et al., 'Intel Heads: Edward Snowden Did 'Profound Damage' to U.S. Security' (*ABC News*, 29 January 2014) <https://abcnews.go.com/Blotter/intel-heads-edward-snowden-profound-damage-us-security/story?id=22285388> accessed 2 September 2019.
[139] High Commissioner Report (n 75) para 28. The report then goes on pointing out that: 'Several States also require that the legal framework be established through primary legislation debated in parliament rather than simply subsidiary regulations enacted by the executive – a requirement that helps to ensure that the legal framework is not only accessible to the public concerned after its adoption, but also during its development' para 28.
[140] Finding that the regulation was enough precise: UN HRC*, 'Concluding Observations: Jamaica*' (19 November 1997) UN Doc CCPR/C/79/Add.83, para 20; Finding that the regulation not enough clear: UN HRC, 'Concluding Observations on the Russian Federation' (1995) UN Doc CCPR/C/79/Add.54, para 20.
[141] General Comment No 34 (n 125) para 25; *Malone* (n 76) para 68: 'it would be contrary to the rule of law for the legal discretion granted to the executive to be expressed in terms of an unfettered power.'
[142] *Rotaru v Romania* (n 83) para 59: 'The Court must also be satisfied that there exist adequate and effective safeguards against abuse, since a system of secret surveillance designed to protect national security entails the risk of undermining or even destroying democracy on the ground of defending it'.

safeguards that need to be present in a legislative framework permitting surveillance. The statute needs to detail:

> the nature of the offences which may give rise to an interception order; a definition of the categories of people liable to have their telephones tapped; a limit on the duration of telephone tapping; the procedure to be followed for examining, using and storing the data obtained; the precautions to be taken when communicating the data to other parties; and the circumstances in which recordings may or must be erased or the tapes destroyed.[143]

In the *Big Brother Watch* case, applicants requested three additional standards to be added to the list when assessing the legality of mass surveillance programs: 'evidence of reasonable suspicion' in relation to the individual targeted, 'prior judicial authorization' and 'notification' to the subject. All three were refused by the Court, who found the six 'traditional' standards to be sufficient.[144] These six standards have been applied in all the subsequent cases relating to surveillance and have been accepted at the UN level, too.[145]

B.2. Is the interference necessary in a democratic society to achieve one of the listed interests

To be lawful an interference needs to have a basis in law, and in turn that law needs to have certain qualities: accessibility, to be sufficiently precise to offer some foreseeability and establish specific safeguards against (secret) abusive practices. But according to the ICCPR, the interference also needs to not be arbitrary. The concept of arbitrariness was introduced 'to guarantee that even interference provided for by law should be in accordance with the provisions, aims and objectives of the Covenant and should be, in any event, reasonable in the particular circumstances.'[146]

This has been interpreted by the Human Rights Committee as the interference needing to be (1) necessary in a democratic society (2) to pursue a legitimate aim (3) in a proportionate manner,[147] which are the same standards set by the ECHR.[148]

B.2.1. Necessary in a democratic society

The requirement that the interference with the right to privacy has to be 'necessary in a democratic society' is explicitly established by the ECHR.[149] The term is not present in

[143] *Weber* (n 84) para 95.
[144] *Big Brother Watch and Others v UK,* App no 58170/13 (Judgment) (4 September 2013) para 316.
[145] La Rue (n 3) para 81: 'Safeguards must be articulated in law relating to the nature, scope and duration of the possible measures, the grounds required for ordering them, the authorities competent to authorize, carry out and supervise them'; High Commissioner Report (n 75) para 28: 'The State must ensure that any interference with the right to privacy, family, home or correspondence is authorized by law that […] (c) are sufficiently precise, specifying in detail the precise circumstances in which any such interference may be permitted, the procedures for authorizing, the categories of persons who m ay be placed under surveillance the limits on the duration of surveillance and procedures for the use and storage of the data collected'.
[146] General Comment No 16 (n 71) para 4.
[147] UNHRC, 'General Comment No 31: The nature of the general legal obligation imposed on States Parties to the Covenant' (26 May 2004) UN Doc CCPR/C/21/Rev.1/Add.13, para 6.
[148] ECHR (n 68) para 8(2).
[149] Ibid.

Article 17 of the ICCPR but can be found in three other articles.[150] Democracy was considered as an essential context by the Universal Declaration on Human Rights (UDHR) in 1948.[151] As we have developed in the second chapter of this thesis, the UDHR and the ICCPR have a common historical basis (the International Bill of Human Rights) and their authors' interactions and interplay with the ECHR's drafters is considered clear.[152] Once again, the Special Rapporteur on the right to privacy has asserted that, despite the difference in wording, the standard 'necessary in a democratic society' should be applied when assessing interference with the right to privacy.[153]

The principle of necessity has been affirmed numerous times by different UN bodies.[154] States have to justify that any limitation to the right to privacy is 'a necessary means to achieving a legitimate aim. This requires that there must be a rational connection between the means employed and the aim sought to be achieved'.[155] When assessing whether a particular interference is 'necessary in a democratic society', the ECtHR balances the interests of the State against the right of the claimant.[156] The term 'necessary' is not considered, in this context, as flexible as other expressions such as 'useful', 'reasonable' or 'desirable'; the State needs to prove a 'pressing social need' in order to justify the interreference allowed.[157] States have of course a certain margin of appreciation in assessing this 'pressing social need', but their decisions can still be reviewed by the Court.[158]

Following the positions of the European Court of Justice[159] and the UN Special Rapporteur Frank La Rue[160], the ECtHR recognised in the *Szabo and Vissy* case the special potential of new surveillance technologies to interfere with people's privacy and therefore interpreted the standard of 'necessary in a democratic society' as requiring a 'strict necessity' assessment. This assessment consists of two aspects: firstly 'a general consideration for the safeguarding of the democratic institutions'[161], and secondly 'a particular consideration, for the obtaining of vital intelligence in an individual operation'.[162] Once again, the ECtHR interprets existing standards specifically to address issues raised by surveillance activities. The limitation on the right to privacy cannot be considered 'necessary in a democratic

[150] ICCPR (n 65) arts 14 (Right to Free Trial), 21 (Freedom of Association), and 22 (Freedom of Assembly).
[151] Report SRP February 2019 (n 122) para 15.
[152] Ibid, para 15.
[153] Ibid, para 16: 'Special Rapporteur must reasonably apply the same standard i.e. that the right can only be qualified by measures provided for by law (Article 17(2)) and that such measures must be necessary in a democratic society by way of an interpretation of 'arbitrary or unlawful interference' consistent with Articles 14, 21 and 22 of the ICCPR'.
[154] UNHRC, 'Resolution: The Right to Privacy in the Digital Age' (23 March 2017) UN Doc A/HRC/RES/34/7, para 2; HR Committee, 'Concluding observations on the fourth periodic report of the United States of America' (23 April 2014) UN Doc CCPR/C/USA/CO/4, para 22.
[155] Emmerson (n 138) para 51.
[156] CoE, 'Guide on Article 8 of the European Convention on Human Rights: Right to respect for private and family life, home and correspondence' (last updated 30 April 2019 <https://www.echr.coe.int/Documents/Guide_Art_8_ENG.pdf> accessed 2 September 2019, para 22.
[157] *Dudgeon v the United Kingdom*, App no 7525/76 (Judgment) (22 October 1981*)* para 51.
[158] Ibid*,* para 52.
[159] Cases C-293/12 and C-594/12, *Digital Rights Ireland v Minister for Communications & Others* (8 April 2014) para 52: So far as concerns the right to respect for private life, the protection of that fundamental right requires, according to the Court's settled case-law, in any event, that derogations and limitations in relation to the protection of personal data must apply only in so far as is *strictly necessary* (emphasis added).
[160] La Rue (n 3) para 83(b).
[161] *Szabo and Vissy* (n 79) para 73.
[162] Ibid, para 73.

society' if it is not proportionate to a legitimate aim.[163] What is considered a legitimate aim is the subject of the next section.

B.2.2. Pursue a legitimate aim

The ECHR clearly lists the accepted interests in Article 8: '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'.[164] The ICCPR does not contain an exhaustive list of what may be considered a legitimate aim for interference with the right to privacy. It is therefore upon States to explain why they believe a particular goal to be legitimate for interfering with Article 17, and this will be reviewed by the Human Right Committee through the usual procedures of periodic reports and complaints.[165]

Protecting national security and countering terrorism are the two main goals evoked by States when justifying surveillance measures which might interfere with the right to privacy.[166] Because Internet is today one of the main tools of communication, but has at the same time helped to finance and perpetuate terrorist acts, State have argued that conducting extensive surveillance of all Internet traffic is necessary to prevent and suppress terrorism.[167] Protecting national interests and the prevention, suppression and investigation of terrorist acts and crime have indeed been accepted as such legitimate aims,[168] but that does not mean that States have unlimited discretion in targeting individuals by secret surveillance programs. The ECtHR has been very clear on that:

> This does not mean that the Contracting States enjoy an unlimited discretion to subject persons within their jurisdiction to secret surveillance. The Court, being aware of the danger such a law poses of undermining or even destroying democracy on the ground of defending it, affirms that the Contracting States may not, in the name of the struggle against espionage and terrorism, adopt whatever measures they deem appropriate.[169]

The problem with the term 'national security' is that it is an amorphous concept. Its definition is very broad and therefore easily manipulated by States to potentially abuse their prerogatives and target vulnerable groups as journalists or human rights activists.[170] As Martin Scheinin pointed out in 2009: 'Counterterrorism is not a trump card which

---

[163] *Dudgeon* (n 157), para 53.
[164] ECHR (n 68) para 8(2).
[165] Scheinin (n 66) para 18.
[166] Christopher York, 'Barak Obama Justifies PRISM NSA Surveillance Programme Saying it Has Saved Lives' (*The Huffington Post*, 19 June 2013) <https://www.huffingtonpost.co.uk/2013/06/19/prism-obama-germany-merkel_n_3464613.html> accessed 3 September 2019.
[167] Emmerson (n 138) para 34.
[168] Ibid, para 33; *Weber and Saravia* (n 84) para 104; *Klass and others* (n 76) para 48: The Court has therefore to accept that the existence of some legislation granting powers of *secret surveillance over the mail, post and telecommunications* is, under exceptional conditions, necessary in a democratic society in the interests of national security and/or for the prevention of disorder or crime (emphasis added); *Leander v Sweden* (n 77) para 59: There can be no doubt as to the necessity, for the purpose of protecting national security, for the Contracting States to have laws granting the competent domestic authorities power (…) to *collect and store in registers not accessible to the public information on persons* (emphasis added).
[169] *Klass and others* (n 76) para 49.
[170] La Rue (n 3) para 60.

automatically legitimates any interference with the right to privacy. Every instance of interference needs to be subject to critical assessment.'[171] States therefore are required to not only prove that the interference with an individual's right to privacy meets a specific social need, but that the restriction is proportionate to the aim. According to the ECtHR, he degree of interference must 'be assessed against the necessity of the measure to achieve that aim and the actual benefit it yields towards such purpose'.[172] In short: a proportionality test needs to be performed.

B.2.3. Proportionality test

As mentioned above, General Comment No 16 states that 'the introduction of the concept of arbitrariness is intended to guarantee that even interference provided for by law […] should be, in any event, *reasonable*'.[173] The concept of 'reasonableness' has been interpreted by the Committee as implying that 'any interference with privacy must be *proportional* to the end sought and be necessary in the circumstances of any given case'.[174]

The ECtHR for its part has consistently acknowledged that:

> When balancing the interest of the respondent State in protecting its national security through secret surveillance measures against the seriousness of the interference with an applicant's right to respect for his or her private life … [States] enjoy a *fairly wide margin of appreciation in choosing the means* for achieving the legitimate aim of protecting national security.[175]

Still, this margin of appreciation is not limitless. Because secret surveillance carries the risk of undermining or even destroying democracy under the pretence of saving it, certain safeguards against abusive practices need to exist. This evaluation takes into consideration the specific circumstances of the case, such as 'the nature, scope and duration of the possible measures, the grounds required for ordering them, the authorities competent to authorise, carry out and supervise them, and the kind of remedy provided by the national law'.[176] Every decision allowing an interference should consequently be decided on a case-by-case basis[177], the proportionality test being assessed on the particular circumstances of the particular case.[178]

The notion that the 'least intrusive measure' should be favoured by States has been advanced numerous times at the UN level in the context of surveillance.[179] But this interpretation has

---

[171] Scheinin (n 66) para 13.
[172] High Commissioner Report (n 75) para 24.
[173] General Comment No 16 (n 71) para 4 (emphasis added).
[174] HR Committee, *Toonen v Australia*, Communication No. 488/1992, UN Doc CCPR/C/50/D/488/1992 (1994). para 8.; HR Committee, *Van Hulst v Netherlands* (n 134) para 7.6.
[175] *Weber and Saravia* (n 84) para 106 (emphasis added); See also *Klass and others* (n 76) para 49; *Leander* (n 77) para 59; *Malone* (n 76) para 81.
[176] *Weber and Saravia* (n 84) para 106; *Klass and others* (n 76) para 50.
[177] General Comment No 16 (n 71) para 8.
[178] Ibid, para 4; *Van Hulst v The Netherlands* (n 134) para 7.3; *Toonen v Australia* (n 174) para. 8.3; Emmerson (n 138) para 51.
[179] La Rue (n 3) para 29; General Comment No 34 (n 125) para 34; Emmerson (n 138) para 52; UNHRC, 'Report of the Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms while Countering Terrorism, Martin Scheinin: Addendum: Mission to the United States of America' (22 November 2007) UN Doc A/HRC/6/17/Add.3, para 49.

been firmly rejected by the United States. As demonstrated in the previous chapter on the jurisdictional issues raised by surveillance practices, the United States promotes a narrow vision of the extraterritorial reach of the ICCPR.[180] They require that the individual be *both* within the territory *and* subject to its jurisdiction in order to enjoy the protection granted by the ICCPR. When it comes to assessing international human rights standards, jurisdiction is not the only area in which the United States adopts a restrictive view: it interprets the substantive protection narrowly as well. In their submission on the right to privacy in the digital age to the Office of the High Commissioner, the United States expressly stated that:

> We read the use of 'right to privacy', or 'privacy rights' to be describing what is laid out in Article 17 of the ICCPR, which is not an absolute right to privacy but rather a right to protection against *unlawful* or *arbitrary* interferences with privacy. The United States understands this requirement to mean that, to be consistent with Article 17, an inference with privacy must be in accordance with transparent laws and must not be arbitrary.

So far, the US does not diverge from the UN position. But it then continues:

> Some commentators have indicated that an interference under Article 17 has to be essential or necessary and be the least intrusive means to achieve a legitimate objective. Such a test goes beyond the text of the Article 17, which only prohibits unlawful and arbitrary interferences, and is not supported by the *travaux* of the treaty.[181]

This demonstrates that the United States are not willing to 'dynamically' interpret international privacy protections in the context of digital surveillance, contrary to what the UN is trying to put in place and to how the ECtHR has been interpreting the ECHR. They rather advocate for a more traditional, conservative and textual interpretation of the relevant provisions.

The different approaches taken by the United States, the HRC and the ECtHR on the admitted limitations to the right to privacy in the context of surveillance illustrate why the conversation around surveillance regulation at the international level is complicated and confusing. It also shows how difficult reaching international consensus on the question would be. The complexity of the surveillance debate can be illustrated by two specific issues: mass surveillance programs and intelligence sharing. They will be both developed in the following sections.

C. Mass surveillance programs

Mass surveillance programs revolutionized the way States conduct peacetime espionage on citizens- including their own. The nature, scope and scale of such activities completely changed. Valsamis Mitsilegas described this as

[180] See Chapter IV of this thesis; OHCHR, 'United States Response to OHCHR Questionnaire on 'the Right to Privacy in the Digital Age' <https://www.ohchr.org/Documents/Issues/Privacy/United%20States.pdf> accessed 23 September 2019.
[181] OHCHR, 'United States Response to OHCHR Questionnaire on 'the Right to Privacy in the Digital Age' <https://www.ohchr.org/Documents/Issues/Privacy/United%20States.pdf> accessed 23 September 2019.

> a paradigm of surveillance that is both quantitively (in terms of the volume of personal data accessed by the State) and qualitatively (in terms of how and why such data is processed and analysed) different from traditional policing models that focus on the detection of criminality.[182]

Indeed, data mining by tapping fibre optic cables, for example, such as conducted by the Prism and Tempora programs, have the potential to intercept the vast majority of all content and metadata communications. There is no doubt that bulk surveillance constitutes an interference to the right to privacy. The question then arise whether it can ever be legally justified. Can such programmes be considered as in accordance with the law and necessary in a democratic society to pursue proportionally a legitimate aim? Two issues are at the forefront of the debate: the criteria of legality and the proportionality test.

First, as detailed in the previous section, an interference with the right to privacy needs to be 'lawful', meaning it needs to have a basis in law- which in turn needs to be accessible, precise enough to give individuals some kind of foreseeability and set up certain safeguards against abuse. It can be difficult to assess whether mass surveillance programmes meet these requirements. Their legal framework is often kept confidential, which undermines their accessibility and foreseeability. They also often fall short in establishing the necessary precautions against abuses:[183] they do not specify the categories of people that are targeted, there is no limit on duration, there is no open debate about the legislation supervising such activities- worse, sometime States do not even enact a new legal framework for these new digital surveillance tools but purposefully use as basis weaker and outdated domestic laws that were meant to regulate simpler forms of surveillance.

The second point is the proportionality assessment. If mass surveillance programmes are by nature conducted in bulk, it is difficult to justify that a case-by-case analysis of the interference has been carried out.[184] It has been asserted that 'mass interception technology eradicates any considerations of proportionality'[185] and that 'since there *is no opportunity for an individualized proportionality assessment* to be undertaken prior to these measures being employed, such programmes also appear to *undermine the very essence of the right to privacy*. They *exclude altogether the "case-by-case" analysis*'.[186] The only way these programmes would not lead to a violation of the right to privacy would be if States managed to justify that the interference with the right to privacy of a potentially unlimited number of Internet users around the world is proportionate to the aim they are trying to reach for.[187] This is rather difficult task. The basic logic of a proportionality analysis is that the greatest the interference with a human right is, the more persuasive the justification needs to be.[188]

---

[182] Valsamis Mitsilegas, 'Surveillance and Digital Privacy in the Transatlantic War on Terror: The Case for a Global Privacy Regime' (2016) 47 Colum. Hum. Rts. L. Rev. 1, 2.
[183] Emmerson (n 138) 37.
[184] Scheinin (n 66) para 57.
[185] La Rue (n 3) para 62.
[186] Ben Emmerson (n 138) para 52 (emphasis added).
[187] Ibid, para 52.
[188] Ibid, paras 12-13: Since there is no target-specific justification for measures of mass surveillance, it is incumbent upon relevant States to justify the general practice of seeking bulk access to digital communications. *The proportionality analysis thus shifts from the micro level* (assessing the justification for invading a particular individual's or organization's privacy) *to the macro level* (assessing the justification for adopting a system that involves wholesale interference with the individual and collective privacy rights of all

The ECtHR seems to have taken another direction on this issue. In the *Big Brother Watch* case, after reminding that States do have a certain margin of appreciation in choosing the means necessary to protect national security, the Court found that conducting bulk interception activities still fell within that margin.[189] It then stated that with regard to the proportionality assessment, the Court would follow the positions taken by the Independent Reviewer of Terrorism Legislation[190] and the Venice Commission that found, respectively, that bulk interception was an essential capability with no alternative[191] and 'recognised its intrinsic value for security operations, since it enabled the security services to adopt a proactive approach, looking for hitherto unknown dangers rather than investigating known ones'.[192] The Court concluded: 'It is clear that bulk interception is a *valuable means* to achieve the legitimate aims pursued, particularly given the current threat level from both global terrorism and serious crime'.[193]

This is an important statement because the Court does not simply accept mass surveillance programmes as proportionate; it rather views them as valuable. It seems that the Court does not question the *legality* of bulk interception programs, but rather only tries to establish standards on how to operate them.[194] The Court ended up considering that the bulk interception regime operated by the United Kingdom violated Article 8 of the ECHR, but on the ground of a lack of independent oversight, not under the proportionality test.[195] This seems to differ from the position taken by the European Court of Justice (ECJ), which endorsed a 'strictly necessary' approach[196]- implying a stricter proportionality test. The ECtHR followed the same approach in the *Szabo and Vissy* case[197], but seems to have walked away from such a strict assessment with the *Big Brother Watch* case. Certain scholars have then spoken of a 'fragmentation' of the European approach to the regulation of surveillance matters, pointing the differences between the positions taken by the ECJ and the ECtHR,[198]

Internet users). The sheer scale of the interference with privacy rights calls for a competing public policy justification of analogical magnitude.

[189] Big Brother Watch (n 144) para 314. A different chamber of the Court already came to that conclusion in *Centrum for Rattvisa v Sweden* (n 108) para 112: In *Weber and Saravia* and *Liberty and Others* (n 84) the Court accepted that bulk interception regimes did not *per se* fall outside this margin. Given the reasoning of the Court in those judgments and in view of the current threats facing many Contracting States (including the scourge of global terrorism and other serious crime, such as drug trafficking, human trafficking, sexual exploitation of children and cybercrime), advancements in technology which have made it easier for terrorists and criminals to evade detection on the internet, and the unpredictability of the routes via which electronic communications are transmitted, the Court considers that the decision to operate a bulk interception regime in order to identify hitherto unknown threats to national security is one which continues to fall within States' margin of appreciation.

[190] UK oversight body.

[191] Big Brother Watch (n 144) para 384.

[192] Ibid, para 385.

[193] Ibid, para 386 (emphasis added).

[194] Theodore Christakis, 'A Fragmentation of EU/ECHR Law on Mass Surveillance: Initial Thoughts on the Big Brother Watch Judgment' (*European Law* Blog, 20 September 2019) <https://europeanlawblog.eu/2018/09/20/a-fragmentation-of-eu-echr-law-on-mass-surveillance-initial-thoughts-on-the-big-brother-watch-judgment/> accessed 5 September 2019.

[195] *Big Brother Watch* (n 144) paras 340-47.

[196] *Digital Rights Ireland* (n 159) para 52; Case C-362/14, *Schrems v Data Prot. Comm'r* (6 October 2015) 2015 ECR 650, para 94*: 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, as guaranteed by Article 7 of the Charter.*

[197] *Szabo and Vissy* (n 79) para 73, See supra Section on Necessity.

[198] Christakis (n 194).

or highlighting the slippery road undertaken by the ECtHR to so readily accept mass surveillance programs as legal.

Of course, one can argue that the matters at stake are different: the *Big Brother Watch* case deals with bulk interception programme for national security purposes, not data retention (*Digital Rights Ireland*) or data transfers (*Schrems*). Still, it will be interesting to see in the future if the 'strict necessary' test is upheld by the Court exclusively in targeted surveillance measures (like in the *Szabo* case) or not. At the time of writing, both the *Centrum for Rattvisa* and *the Big Brother Watch* cases have been referred to the Grand Chamber.

This area of the law is evidently still evolving. Judgments by high-level courts such as the ECtHR are valuable because they help clarify how the existing frameworks should be interpreted to assess the legality of new surveillances measures such as bulk interception of communications. Another matter that illustrates the legal ambiguity surrounding surveillance regulation is the practice of agencies to share intelligence between each other.

D. Intelligence sharing between agencies

A key concern revolves around what happens to personal data that is shared by one agency to another (especially when it crosses border). One of the most famous international agreements to share intelligence between States is the so-called 'Five-Eyes' alliance. It was initially based on an agreement between the United Kingdom and the United States[199], but then opened to Australia, Canada and New Zealand. Even though Edward Snowden disclosed its existence, the legal basis of this agreement itself is still mostly secret. Following the scandal upon the discovery of such secret alliances, the Five Eyes countries established the 'Five Eyes Intelligence Oversight and Review Council', which was part of a bigger move from the five concerned States to reform their legislative frameworks to reinforce privacy protections.[200] The most important question in this respect is whether the shared data is still protected by the same standards as the agency that collected it in the first place. Is it protected at all?[201] There are different legal aspects that need to be considered when evaluating the legality of States sharing intelligence between government agencies, i.e. law enforcement or security intelligence services, whether the transfer happens to cross a border or not.[202]

One important issue raised by intelligence-sharing practices is their compliance with human rights law, more specifically with the right to privacy. Concerns are raised over the compliance of such transfers with several requirements: the accessibility, foreseeability and proportionality of the legal basis allowing such activities, but also the potential lack of independent oversight. The secrecy surrounding data sharing agreements makes it difficult for individuals to know when their data is being collected in the first place, and if, when, and to whom it is being shared. This raises problems regarding the clarity and foreseeability of these legal instruments. When assessing the proportionality of surveillance measures, it is important to look at what is being collected, but also who is using it. The problem when data

[199] UKUSA Signal Intelligence Agreement (adopted 5 March 1946).
[200] Report SRP February 2019 (n 122) para 38.
[201] Ibid, para 36.
[202] When the data does cross borders, jurisdictional issues might arise- See Chapter IV.

is being shared between different entities is that what could have been necessary and proportionate when collecting certain data, might not be the same for its subsequent use.[203] The ECtHR recently found that sharing intelligence with foreign governments, if properly regulated, does not amount to a violation of the right to privacy enshrined at the Article 8 of the ECHR:

> Due to the nature of global terrorism […] the Court accepts that [taking a stand against terrorism] requires a *flow of information* between the security services of many countries in all parts of the world. Is in this present case, this 'information flow' was embedded into a legislative context providing considerable safeguards against abuse, the Court would accept that the resulting interference was *kept to that which was 'necessary in a democratic society'*.[204]

Another issue might arise under data protection legal regime: for example, many domestic legislations do not have any '*purpose* specification' principle regulating the further use of the data once collected. 'Purpose specification' is one of the core Fair Information Principles found in data protection regimes: it imposes an obligation for the collecting entity to specify the purpose and disclosure of the collection, and to exclusively use the data for the disclosed purpose.[205]

When intelligence is shared between security agencies from different countries, it needs to be inquired whether there is an independent oversight body supervising the transfer. The Special Rapporteur on the right to privacy recommended in February 2019 that States adopt and implement the principle 'if it's exchangeable, then it is *oversightable*'[206]- regardless if the transfer between agencies occur inside or cross borders. Another source of concern is that data protection legislations and domestic laws often exclude national security and law enforcement matters from their scope.[207] In the rare cases where domestic laws do apply, gaps might still exist at the national level when dealing with foreign nationals' data. Domestic privacy safeguards might not be extended to exchange of information with third countries.[208]

Slow progress is being made to fill these gaps, for example a cooperation relationship has been adopted between five European intelligence oversight bodies: Belgium, Switzerland, Denmark, the Netherlands and Norway. They started a process to cooperate and harmonize their approaches and standards when sharing data.[209] The Council of Europe also proposed in 2015 to start regulating cooperation between intelligence agencies.

---

[203] High Commissioner Report (n 75) para 27.
[204] *Big Brother Watch* (n 144) para 446 (emphasis added). To read more on this *See* Tomaso Falchetta, 'Intelligence Sharing and the Right to Privacy after the European Court Judgment in Big Brother Watch v. UK' (*EJIL: Talk!*, 24 September 2018) <https://www.ejiltalk.org/intelligence-sharing-and-the-right-to-privacy-after-the-european-court-judgment-in-big-brother-watch-v-uk/> accessed 24 September 2019.
[205] For more on this, See Chapter III of this thesis.
[206] Report SRP February 2019 (n 122) para 38.
[207] E.g. the GDPR does not apply to national security matters (Recital 16).
[208] UNHRC, 'Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Martin Scheinin' (28 December 2009) UN Doc A/HRC/13/37, paras 20 and 40.
[209] They address issues such procedurals standards of transfers, limitations in disclosing to third parties,.. in Joint Statement: Strengthening Intelligence Oversight Cooperation, <https://english.ctivd.nl/documents/publications/2018/11/14/index> accessed 4 September 2019.

E. Conclusion

Human rights bodies, such as the ECtHR, the Human Rights Committee and the Human Rights Council, have applied human rights standards to online surveillance practices. They have dynamically interpreted existing provisions in order to take into account new digital technologies and address the current challenges of globalized, online, surveillance. Courts in particular have been key actors in developing a stronger regulation of online surveillance practices. As Mitsilegas wrote 'judiciaries have provided the most powerful responses to mass surveillance and upheld the right to privacy in a meaningful and extensive way'.[210]

Still, there is no general discussion around what kind of understanding exists over the concept of legal protection granted over privacy or the nature of the interferences caused by surveillance communications programs. It is often repeated that surveillance activities such as the interception of communications or the collection of personal data impact negatively the enjoyment of human rights, especially when conducted on a mass scale,[211] but there is not a lot of reflexion on exactly what kind of 'negative impact' they are referring to. One of the most recurrent points is how unjustified interreference with the right to privacy affects the enjoyment of other rights as well, mainly the freedom of expression. As shown in the second chapter of this thesis, this approach corresponds to the Special Rapporteur on the right to privacy's view on the nature of the right to privacy: as an *enabling* right.[212] But there is not a lot about the kind of harms online surveillance measures causes on 'privacy' itself. One of the only allusions can be found in one of the UN General Assembly resolutions on the right to privacy in the digital age:

> Emphasizing that unlawful or arbitrary surveillance and/or interception of communications, as well as unlawful or arbitrary collection of personal data, as *highly intrusive acts*, violate the right to privacy, can interfere with the right to freedom of expression and may contradict the tenets of a democratic society, including when undertaken on a mass scale[213].

This vocabulary of 'intrusive acts' seems to refer to the idea a certain 'zone' that should not be intruded upon, that should remain free from interference. This conceptualization of privacy is also the one favoured by Special Rapporteur Frank La Rue. According to him:

> In order for individuals to exercise their right to privacy in communications, they must be able to ensure that these remain private, secure and, if they choose, anonymous.

---

[210] Mitsilegas (n 182) 76.
[211] UNGA Res 19/166, 'The Right to Privacy in the Digital Age' (18 December 2014) UN DOC A/RES/69/166; HRC, 'The Right to Privacy in the Digital Age' (1 April 2015) UN Doc A/HRC/RES/28/16.
[212] UNHRC, 'Report of the Special Rapporteur on the right to privacy, Joseph A Cannataci' (8 March 2016) UN Doc A/HRC/31/64, para 25: 'In order to help focus a fresh, structured debate on fundamentals the SRP intends to provocatively posit *privacy as being an enabling right as opposed to being an end in itself*. Several countries around the world have identified an over-arching fundamental right to dignity and the free, unhindered development of one's personality' (emphasis added).
[213] UNGA Res 19/166 (n 211) (emphasis added), which was repeated by the HRC 'The Right to Privacy in the Digital Age' (23 March 2017) UN DOC A/HRC/RES/34/7.

> Privacy of communications infers that individuals are able to exchange information and ideas in a *space* that is *beyond the reach* of other members of society, the private sector, and ultimately the State itself.[214]

This terminology refers to the paradigm of freedom from unwarranted interference. The rationale behind the protection is that individuals should be free to exchange communications without intrusive *acts*- in this case: interception or collecting by governmental authorities.

The first chapter of this thesis highlighted the important role of courts to initially protect certain private interests and then to progressively create a right to privacy in their respective legal systems. The same pattern can be seen at the international level. Courts have clearly tried to adapt the existing international provisions to ensure appropriate responses to online surveillance. But judicial intervention will soon not be enough to keep developing single-handedly an international privacy regime adapted to respond to these new surveillance challenges.[215] This situation led many stakeholders to call for new developments in the field of privacy and online surveillance regulation.

Section 2. Calls for new developments and regulations

Privacy laws around the world have not been evolving quickly enough with new information technologies. The existing human rights standards have been stretched to supervise the use of new surveillance tools, but they struggled to do so as the nature of the surveillance activities they attempt to regulate is drastically different from the traditional law enforcement procedures they were initially enacted to deal with. The existing international human right protections such as the ICCPR and the ECHR do offer privacy protections, but their application to the digital surveillance context has been complicated- as demonstrated above. The current provisions are not detailed enough to handle the complexity of mass surveillance programs. This situation creates legal gaps and decreases the relevance of important treaties such as the ICCPR. Demands for a clearer, more detailed framework come from all the stakeholders involved.[216] There are two ways to modernise existing surveillance regulation: either by 'updating' our understanding of existing human rights standards or by enacting a brand-new legal instrument regulating specifically electronic surveillance.

The first option is to interpret dynamically the existing framework in order to take into account new surveillance technologies. The Human Rights Committee has been asked multiple times to update the General Comment No 16 on the Article 17 of the ICCPR.[217]

---

[214] La Rue (n 3) para 23. (emphasis added).
[215] Mitsilegas (n 182) 76.
[216] The Special Rapporteur on Privacy wrote in February 2017: I have yet to meet one civil society organisation, one corporation, indeed one reasonable law enforcement agency and security and intelligence service that does not wish to have greater clarity and universally applicable safeguards and remedies in Cannataci Second Report (n 61) para 46(f).
[217] Amongst others: *See* Scheinin (n 66) paras 18 and 74: The Special Rapporteur recommends that the Human Rights Committee begins drafting a new general comment on article 17 of the International Covenant on Civil and Political Rights, with the goal of elaborating a proper limitation test, thereby providing guidance to States on appropriate safeguards. The general comment should also give due attention to data protection as an attribute of the right to privacy, as enshrined in article 17 of the Covenant; La Rue (n 3) para 98.

ACLU has published its own proposal of a new General Comment on the right to privacy.[218] Unfortunately, the Committee does not seem to take into account such demand and no revision or enactment of a new General Comment are on the way.

The ongoing process of States engaging in dynamically interpreting and applying the existing standards granted by the Article 17 of the ICCPR and the Article 8 of the ECHR in the context of electronic surveillance will, simultaneously, slowly impacts the development of international customary law. This process can coexist with the establishment of a separate instrument containing new standards.[219]

Another way to effectively protect individuals' right to privacy against invasive surveillance practices is to enact a separate legal instrument regulating exclusively online surveillance. This is not an easy task. Enacting that kind of multilateral agreements can take years, especially when it touches upon sensitive subjects such as regulating activities that States consider vital for the protection of their national interests and security. There are also different, competing, visions on how cyberspace should be regulated in general: a sovereignty-based governance approach (favoured by Russia and China) and a multi-stakeholders vision (United States and its allies).[220]

Such initiatives could be taken at the global or regional level. If a global framework is in theory preferable, it might be very difficult to reach an agreement on the substantive provisions that the instrument should include. As demonstrated in previous chapters of this thesis, the United States and European countries usually illustrate different approaches on several aspects of privacy regulation: they conceptualize differently domestic privacy regulation and interpret differently the extraterritorial reach of the ICCPR and its limitations standards.[221] All of these issues are essential to substantially regulate online surveillance practices. However, the likelihood of these actors finding a consensus on these difficult questions is low. Regional agreements can be easier to reach because, not only do they require less participants to see eye to eye, the participants' conceptualisation and understanding of how privacy should be protected (and consequently how surveillance practices regulated) might also be more similar. It would also allow States that are willing to progress to fast track their discussions without having to settle to the lowest denominator.[222] Experiences of the Council of Europe for example show that this is a viable option. Its Convention on Cybercrime[223] and Convention No 108[224] both started as regional frameworks but then were opened for signature to non-Members. This transformed these regional instruments into international ones- admittedly not universal, but a successful legal drafting experience at the international level nonetheless.

---

[218] American Civil Liberties Union, 'Privacy Rights in the Digital Age: A Proposal for a New General Comment on the Right to Privacy under Article 17 of the International Covenant on Civil and Political Rights: A Draft Report and General Comment' (March 2014) <https://www.aclu.org/sites/default/files/assets/jus14-report-iccpr-web-rel1.pdf> accessed 3 September 2019.
[219] Deeks (n 10) 343.
[220] See more in Watt (n 27) 785.
[221] 'unlawful and arbitrary'.
[222] Deeks (n 10) 342.
[223] Convention on Cybercrime (adopted on 23 November 2001, entered into force 01 July 2004) ETS 185.
[224] Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (adopted 28 January 1981, entered into force 01 October 1985) ETS 108.

The Special Rapporteur on Privacy has always been in favour of a multilateral agreement regulating surveillance practices.[225] He has started the proceedings to establish a 'Legal Instrument on Government-led Surveillance and Privacy'.[226] It is now at the stage of a comprehensive draft, still open to discussion, fleshing out 18 substantive Articles. This legal instrument 'aims at safeguarding the fundamental rights and freedoms of persons with regard to the deployment and use of surveillance systems, as well as non-surveillance data when used for surveillance purposes'[227]. It would be complementary to other frameworks regulating cyber activities[228] such as the Cybercrime Convention of the Council of Europe.[229]

A coalition of civil society, privacy and technology experts drafted in 2013 a document called: 'International Principles on the Application of Human Rights to Communication Surveillance'[230], often referred to as the 'Necessary and Proportionate Principles'. This document contains thirteen principles that details how international human right law should be applied in the context of communication surveillance.[231] The thirteen principles are: Legality, Legitimate Aim, Necessity, Adequacy, Proportionality, Competent Judicial Authority, Due Process, User notification, Transparency, Public Oversight, Integrity of Communications and Systems, Safeguards for International Cooperation, Safeguards against Illegitimate Access. The reason why this document is worthy pointing out is that it has been signed by 600 organisations so far, but also because there is a clear influence of the Fair Information Principles found of data protection regimes.[232]

Certain scholars also start to propose their own solutions to the absence of surveillance regulation: for example, Sourgens proposes the introduction of a 'general principle of law protecting the right to privacy'[233], Deeks favours the establishment of global procedural standards to regulate foreign surveillance, rather than substantives ones[234] and Mitsilegas called for a global instrument on the right to privacy and surveillance to be enacted, which

---

[225] Cannataci Second Report (n 61) para 46(g): It's no use beating round the bush: the only way this clarity can be achieved, the only way that these safeguards and remedies can be introduced in a way where their enforcement becomes more timely, more even-handed and expedient is through *multilateral agreement enshrined in international law*. What the world needs is not more state-sponsored shenanigans on the Internet but rational, civilised agreement about appropriate state behaviour in cyberspace. Which again brings me back to the subject of surveillance. (emphasis added).

[226] Working Draft Legal Instrument on Government-led Surveillance and Privacy v7 (28 February 2018) <https://www.ohchr.org/Documents/Issues/Privacy/SR_Privacy/2018AnnualReportAppendix7.pdf> accessed 3 September 2019.

[227] Draft Article 1, 7.

[228] UNHRC, 'Report of the Special Rapporteur on the Right to Privacy – Note by the Secretariat' (28 February 2018) UN Doc A/HRC/37/67, para 127.

[229] Convention on Cybercrime (n 223).

[230] Necessary and Proportionate (n 6).

[231] The principles apply to surveillance conducted within a State or extraterritorially, regardless of the purposes behind it, ibid, at 3.

[232] *See* Chapter III of this thesis.

[233] Frédéric Gilles Sourgens, 'The Privacy Principle' (2017) 42 Yale J. Int'l L. 345, 349. For an article refuting Sourgens' argument See: Asaf Lubin, 'A Principled Defence of the International Human Right to Privacy: A Response to Frédéric Sourgens' 42 Yale J. Int'l L. Online 1.

[234] Deeks recommends States to adopt six principles to be adopt internationally: (1) notice to the public of the applicable rules; (2) limits on the reasons that states may collect or query data; (3) a requirement for periodic reviews of surveillance authorizations; (4) limits on how long the data can be held; (5) a preference for domestic action (i.e., action by the host state intelligence services) wherever reasonable; and (6) the existence of a neutral body to authorize surveillance *ex ante* or review it *ex post*, in Deeks (n 10) 298. To read more on this see Part III of her article Ibid, 343 ss.

should rely mostly on data protection 'as a way to support a strong general right to privacy'[235]. According to him the advantages of using data protection as a regulatory tool for surveillance are multiple: it regulates in detail practices of data collecting, processing and exchange; substantive legal principles are already established in the field, it focuses on procedural justice and grant data subjects specific remedies; dedicated advisory supervisory bodies composed by experts are already in place.[236]

This last proposition, and the Necessary and Proportionate principles, illustrate clearly the influence of data protection principles on what is considered privacy protection should entail in the 21st century. Chapter III of this thesis developed the relationship of the right to privacy and data protection frameworks. Related, but conceptually different, the two regimes offer together a strong protection to individuals whose data is being processed by governmental authorities. Interestingly, data protection principles such a 'necessity' or 'purpose specification' are now being used to 'reinforce' the protection granted by the right to privacy. Data protection frameworks grant procedural rights to individuals, which is also the direction Ashley Deeks is promoting. It is interesting to see many voices calling for surveillance regulation through procedural means, rather than substantive. It allows to grant individuals guarantees while stepping away from the difficult conceptual baggage of privacy protection. As we have developed above, procedural data protection principles tend to refer to the paradigm of 'control': they empower individuals to control the way their private data is processed.

This highlights the conceptual complexity of the current debate on surveillance regulation: on one hand existing traditional frameworks still refer to an understanding of privacy protections as protecting individuals from unwarranted interference in their freedom to communicate, while new developments show the influence of data protection frameworks as supporting, almost 'fleshing out', what the general right to privacy means in the context of online surveillance in the 21st century. The conversation around international surveillance regulation seems therefore to mobilize the two paradigms of 'freedom from interference' and 'control' but is unaware of the conceptual baggage it carries.

Conclusion

Peacetime surveillance was a subject avoided for years in international law- to the point that its (il)legality is still subject to debate. States benefited from this unregulated status quo and never had any incentive to clarify their positions. The Snowden's disclosures of 2013 drastically changed the situation. Surveillance activities sponsored by governments were put under the limelight and the need for clearer regulation became obvious.

The outrage created by these revelations sparked a conversation on how to ensure these new surveillance practices were complying with international human rights standards, in particular with the right to privacy. The existing international provisions started to be interpreted to address these new threats to people's enjoyment of their right to privacy.

[235] Mitsilegas (n 182) 75.
[236] Ibid, 74.

However, the recent developments on surveillance regulation- mostly conducted by judicial bodies, but also at the UN level with the appointment of the Special Rapporteur on the right to privacy, mainly focus on 'technical issues'. There is no conversation around a common understanding of the types of interferences (and the correlated harm) caused by online surveillance, and no acknowledgment of the heavy conceptual baggage privacy protections carry. There is an increasing debate on the type of regulatory model that should be favoured in order to efficiently regulate surveillance and increase individual's protection from abusive practices, but no recognition of the different paradigms hidden in the different propositions. Being aware of the conceptual and substantive challenges present in the surveillance discourse is nonetheless essential to clarify the current situation and being able to move forward. A purely technical answer to the challenges raised by new surveillance technologies is not enough.

Legislating on surveillance activities mobilizes the two conceptual apparatuses identified in the first chapter of this dissertation. On one hand, their compliance with the provisions establishing a right to privacy is framed in a terminology belonging to the 'freedom paradigm'- even though as explained in the second chapter, there is no consensus on how these protections are conceptualized in general. The general reasoning behind assessing if a specific violation of the right to privacy occurred is to first consider if there was an interference to the individual's privacy and then to analyse whether such interference could be justified or not according specific criteria. Regardless of the exact scope of these protections, conceptually they are clearly understood as protecting the individual from an external, unjustified, interference. On the other hand, data protection principles have been increasingly used 'in support' of a general right to privacy when assessing the legality of data processing activities, including State-sponsored surveillance. Whether data protection principles are invoked to complement individual's protection to abusive data processing practices, 'side-by-side' with the right to privacy or to interpret the scope of privacy protection themselves- the legal regime of data protection represents a vision of control, of empowering individuals. Therefore, in order to move forward when discussing how to best tackle surveillance regulation at the international level, it is essential to be aware of the technical normative challenges these types of activities raise, but their conceptual implications.

The two paradigms of 'freedom from interference' and 'control' are currently present in the conversation on international surveillance regulation. Being aware of this is important for two reasons.

The first reason is that clarifying a debate is always, as such, useful. Navigating through complex privacy and data protection frameworks in the context of online surveillance is not an easy task. Understanding better the different conceptions behind the debate is helpful to explain the background on which the conversation is taking place and grasp different actors' motivations.

The second reason why it is important to be aware of the conceptual baggage is because the two paradigms represent different approaches to privacy regulation and therefore different choices for policymakers. On one hand the 'freedom from interference' paradigm refers to

a more restrictive, traditional, view to human right protection. The State is expected to take action to secure individuals' freedom from specific interferences (from its own authorities and private actors). The 'control' paradigm, on the other hand, illustrates a more 'hands on' approach to privacy regulation. As detailed supra, the protection is 'individual-orientated', it is detailed, and its main goal is to empower individuals to enhance their ability to control how their private interests are being handled. The protection often takes the shape of procedural rules. These rules are, by nature, not prohibitive.
Policy makers have the choice between these two approaches to privacy protection. They will make different choice depending on their political background, vision of government and how they reckon human rights can be best protected.

It is not surprising that the provisions in international instruments protecting privacy are framed under the paradigm of 'freedom of from interference'[237]. It refers to a more minimalistic approach to human rights protection and is therefore more conducive to consensus. But one wonders if the digital revolution has not tested the limits of that approach. There are reasons why data protection frameworks have emerged all over the world in the last 30 years, that judicial bodies are using data protection principles to interpret and give meaning to the general right to privacy in the context of online surveillance, and that scholars call for procedural rules to be enacted in order to respond to these new challenges. It is not enough to only protect a "zone free from interference" anymore. How long can the United States sustain the practice to enact a new regulation for every new abusive practice that comes up? International policymakers should not follow that path. In an highly complex, digital world, individuals need to be given the power to handle their own information. There is no doubt that online surveillance programs are part of our lives now, and they are not going to be prohibited. The question is how to best regulate them in order to make them comply to human rights standards. Procedural rules[238], and the paradigm of control they represent, are better equipped to deal with this new reality.

[237] Even though, as developed supra, there is no general conception of the protection itself.
[238] Because they are more detailed and not prohibitive by nature.

CONCLUSION AND OUTLOOK

'One of the biggest challenges for international law is ensuring it keeps pace as the world changes'.[1] It is with these words that the Attorney General started a speech on the United Kingdom's position on applying international law to cyberspace in May 2018. He continued by stating that:

> There are few areas in which the world has moved faster than in the development of cyber technology. […] Until a few years ago, the international community had yet to agree whether there were any applicable rules in cyber space at all. The academic community has been quick to fill the gap and academics have made valuable contributions to the debate, but States have remained relatively quiet. […] But the truth is, as authors and subjects of international law, States have a responsibility here. A responsibility to be clear about how our international law obligations bind us. A responsibility we fulfil through our treaty obligations, our actions and our practice, as well as through our public statements. And a responsibility I believe extends to cyberspace. […]
>
> Online as well as everywhere else, the principle of sovereignty should not be used by States to undermine fundamental rights and freedoms and the right balance must be struck between national security and the protection of privacy and human rights.[2]

This type of statement is extremely rare. States have not been clear on how international law regulates online surveillance activities. The absence of clarity on the subject has been described as '[a situation] where most States have either resisted legalization or have been ambivalent about prioritizing rights where national security threats are politically resonant'[3]. States have benefited from an unregulated status quo and had no real incentive to address such a complicated issue. Against this background, however, the revelations of Edward Snowden in 2013 had a massive impact on the approach of the States to online surveillance. All of a sudden, the lack of regulation on practices of online surveillance became evident, as well as the need to rectify this situation. The goal of this thesis was to contribute to these efforts towards a more adequate regulation of online surveillance by clarifying the different sources of confusion at play—and more specifically the broader conceptual, jurisdictional, and substantive implications that the general right to privacy and online surveillance activities imply.

1. Findings of the dissertation: Identifying and addressing the challenges to online surveillance regulation

[1] Jeremy Wright, 'Speech: Cyber and International Law in the 21st century' (Chatham House Royal Institute for International affairs, 23 May 2018) < https://www.gov.uk/government/speeches/cyber-and-international-law-in-the-21st-century> accessed 1 October 2019.
[2] Ibid.
[3] 'Working Draft Legal Instrument on Government-led Surveillance and Privacy v7' (28 February 2018) <https://www.ohchr.org/Documents/Issues/Privacy/SR_Privacy/2018AnnualReportAppendix7.pdf> accessed 3 September 2019.

The legal discourse regarding online surveillance is complex for two main reasons: one is related to the conceptual baggage behind privacy regulation, the second concerns the nature of surveillance activities themselves.

1.1. Confusion related to privacy conceptual baggage

When discussing about legislating on online surveillance activities, one of the main issues is their compliance with the right to privacy. The right to privacy is in itself a complex legal construct. The first part of this thesis looked in detail into this specific right: its different conceptualizations in domestic systems, its ambiguity and amorphous nature at the international level, and its complex relationship with data protection frameworks.

In Chapter I, a comparative analysis of the approaches to privacy regulation in the United States and in France highlighted that two main paradigms can be found behind the right to privacy: one that associates the legal protection with preserving a form of freedom from external interferences, and another that understands it as empowering individuals to have control over certain aspects of their private life. These two paradigms can be found both in the terminology used by various legal actors to qualify the right to privacy, but also by the types of legal constructs mobilized before the recognition of a distinct right to privacy to protect certain private interests such as the sanctity of the house, the confidentiality of letters or the ability to oppose unwarranted disclosure of private facts.

This domestic comparative analysis was done with the intention to clarify how international law understands the right to privacy. Therefore, Chapter II turned to the question of how the paradigms identified at the domestic level were interpreted at the international level. The right to privacy is established by many international human rights treaties. The wide ratification of such instruments by States have contributed to a clear solidification of an international right to privacy. But how international law actually conceptualizes this right is not clear. The scope of the provisions is still debated, and the drafting histories of the major instruments that are the UDHR, ICCPR and ECHR do not clarify the issue. The drafters were silent on their conceptualization of the concept of privacy, and the protection they were granting. No debate took place as to whether a protection should be established to protect privacy or not, as if there was an uncontested consensus between the drafters to do so. But what might have been seen as obvious was, in reality, far from being so. The complex conceptual baggage of privacy regulation was not discussed at all by these treaties' drafters—and barely so by their respective interpretative bodies. Even when they do so, the different Special Rapporteurs keep oscillating between the two paradigms of 'freedom from interference' and 'control'—illustrating the conceptual confusion surrounding the issue of private regulation. The second part of the 20th century did not raise any particular incentive to explore this complicated question, but the situation changed in the 21st century and the interest for international right to privacy was renewed. All of a sudden, international attention turned to the right to privacy granted by the major treaties: the ambiguity around its scope became problematic, the uncertainty started to be regarded as weakening the protection of individuals' right to privacy.

Alongside a general, but ambiguous, right to privacy emerged a new legal regime which was the focus of Chapter III: data protection frameworks. With the emergence of the computers and the Internet, the general right to privacy was not considered as sufficiently detailed to address the new capabilities these new technologies provided. Data protection frameworks regulating data processing started to emerge at the international level in the 80s and 90s, to progressively be adopted by many domestic jurisdictions. While international law and Europe seems to now distinguish data protection regulations from the right to privacy, the United States still considers it under the general "privacy umbrella". Most of the core principles of data protection are procedural rather than substantive, and clearly relates to the paradigm of control. The goal is to empower individuals to have a better understanding, access and control over his own personal data and the way they are being processed. These frameworks play an important role in the context of surveillance activities—not only because of the rules they put in place concerning data processing in general, but also because of the influence they have on the understanding of what privacy means in the 21st century, and consequently how the international right to privacy should be understood, and what it should entail.

1.2. Confusion related to the nature of surveillance activities

The second main source of confusion in the debate around online surveillance regulation relates to the nature of the surveillance activities and the second part of the dissertation therefore focused on this set of challenges.

The context in which online surveillance operates has its own challenges. Cyberspace challenges our traditional understanding of the territoriality principle—which currently underpins the jurisdictional system in public international law. While certain surveillance activities—such as the access to data—currently receive some international attention, others keep being conducted off the radar. Cyberspace also complexifies the already delicate question of extraterritoriality of human rights treaties: how is the ECtHR standard of effective control understood in cyberspace? Should the location of the individual whose communication is intercepted still matter? Or the location of the interception itself? The latter would make sense, as it is at the location of the interception that an interference with the right to privacy might occur (leading to its potential violation). This is where the State's power actually takes effect. In the 21st century world, an individual and its private information are not exclusively at the same location. New technologies have granted the possibility to States to interfere with privacy of individuals in new ways. How we assess that interference needs to take into account this new reality: when it comes to the right to privacy, an interference (and therefore a potential violation) might occur in another location than the concerned individual's. As Chapter IV demonstrates, these questions indicate the need for a broader reconceptualization of traditional principles, but are still unanswered.

Another complicated aspect to online surveillance, which is examined in Chapter V, is its substantive regulation and its compliance with human rights standards such as the right to privacy. Regulation of online surveillance is complicated because on one hand public international law has always been very quiet on the question of peacetime espionage, making its legal status quite uncertain. On the other hand, existing human rights standards are being

interpreted to address new types of surveillance. But there is a limit on how creative and dynamic judicial interpretation can be. This can be related to the experience of American and French judges at the end of the 18th and the 19th century: faced with new technologies and new concerns, they had to use the legal constructs at their disposal to grant relief to individuals complaining of violations of certain private interests. International and domestic courts are currently experiencing the same situation: in order to effectively protect individuals from new threats on their privacy, they have to interpret standards that were initially not established to deal with this kind of measures. The international right to privacy and its accepted limitations standards are being "stretched" to respond to the reality created by online surveillance, but they currently fall short of providing effective protection. Data protection principles are increasingly being mobilized in support of the more general right to privacy. The two paradigms highlighted in the first chapter can therefore be identified in the international legal discourse on online surveillance substantive regulation: on one hand, surveillance activities' compliance with international provisions on privacy is being assessed under the paradigm of 'freedom from interference'- even if, as detailed in the second chapter, there is no consensus on how these protections are conceptualized in general. On the other hand, data protection principles mobilize the paradigm of 'control'.

To summarize, the conversation around online surveillance regulation at the international level is complicated because it is at the crossroads of many broader conceptual issues: different paradigms of privacy regulation at the domestic level, and no clarity at the international level; the complex relationship between privacy and data protection frameworks (and the different conceptualization of protection they imply); the jurisdictional challenges brought about by cyberspace under public international law and international human rights law; and finally the need to develop our current human rights standards—either through interpretation or by enacting new ones.

2. The need for further research and regulation

There is no doubt that the field of online surveillance needs more clarity. This is needed to ensure that the current measures comply with international law, but also to anticipate the future ones: AI surveillance is, for example, already being conducted in many countries.[4]

As mentioned in Chapter II, the Special Rapporteur on the right to privacy is currently working on the international legal instrument that would substantively regulate online surveillance practices:

> Due to its complexity, the right to privacy requires a comprehensive legal framework in order to operationalize it in a number of different contexts. […] Each context brings with it the need of a detailed and constantly up-dated understanding of how privacy could be threatened within that particular context […] The devil, literally, is in the detail, and privacy requires very

[4] Steven Feldstein, 'The Global Expansion of AI Surveillance' (*Carnegie Endowment for International Peace,* 17 September 2019) <https://carnegieendowment.org/2019/09/17/global-expansion-of-ai-surveillance-pub-79847> accessed 29 September 2019.

> detailed rules which spell out the level and modes of protection that privacy may be accorded in a particular context.[5]

Others have called for procedural standards to be enacted, drawing on internationally accepted data protection principles.[6]

Whichever way these new developments take form, simply adapting current standards to new surveillance activities is only part of the answer. Detailed substantive rules and dynamic procedural standards might be useful, but one cannot avoid the need to take into account important conceptual questions. Regulating online surveillance activities mobilizes the two conceptual paradigms identified in the first chapter of this thesis. Their compliance with the international right to privacy usually refers to the paradigm of "freedom from interference", the assessment of their compliance being framed in these terms. But the paradigm of control is also present in the legal discourse on online surveillance not only because it regulates data processing activities, but also because it has increasingly been used to support the general right to privacy, and is increasingly shaping our understanding of what the latter should mean and include. The only productive way forward to address online surveillance regulation is to take into consideration the broader conceptual implications these types of measures involve. A reconceptualization of traditional principles of international law is necessary. These conceptual and normative challenges need to be straightforwardly addressed to understand how to regulate effectively surveillance and consequently enhance individuals' enjoyment of their right to privacy. The aim of this dissertation was to take a step towards addressing this need by examining the conceptual baggage behind privacy regulation and the normative challenges of regulating privacy and online surveillance.

[5] Joseph Cannataci, 'Paper presented at Expert Workshop on the Right to Privacy in the Digital Age' (Office of the High Commissioner for Human Rights, Geneva, 19-20 February 2018) UN Doc A/HRC/37/62, Annex A, para 2.
[6] See Chapter V.

BIBLIOGRAPHY

Books

Colin J Bennet, *Regulating Privacy: Data Protection and Public Policy in Europe and the United States* (Cornwell University Press, 1992)

William Blackstone, *Commentaries on the Laws of England,* vol 4 (William Draper Lewis 1922) 168.

William Blackstone, *Commentaries on the Laws of England* (1769) reedited in (The University of Chicago Press, 1979).

Boitsel, *Philosophie du Droit*, vol I (1889).

Eva Brems/Janneke Gerards (eds), *Shaping Rights in the ECHR: The Role of the European Court of Human Rights in Determining the Scope of Human Rights* (CUP 2013).

Lee A Bygrave, *Data Privacy Law: An International Perspective* (OUP, 2014).

Iain Cameron, *The Protective Principle of International Criminal Jurisdiction* (Dartmouth Publishing Co, 1994).

Cannataci Joseph, *Privacy & Data Protection Law* (Norwegian University Press, 1987).

Joan Cocks, *On Sovereignty and Other Political Delusions* (Bloomsbury, 2014).

Brainerd Currie, *Selected Essays in the Conflict of Laws* (CUP, 1963).

Martin Dixon, *International Law* (7th edn, OUP, 2013).

Demogue, *Traite des obligations en general*, vol IV (1924)

Graham Greenleaf, *Asian Data Privacy Laws* (OUP, 2014).

Daniel Gutmann, *Le sentiment d'identité – Etude de droit des personnes et de la famille* (L.G.D.J. 2000).

John P Humprey, *Human Rights & The United Nations: A Great Adventure* (Dobbs Ferry: Transnational Publishing, 1984).

Sarah Joseph/Melissa Castan, *The International Covenant on Civil and Political Rights: Cases, Materials and Commentary* (3rd edn, OUP 2013).

Pierre Kayser, *La Protection de la vie privée* (2 edn, Economica, 1990).

Jan Klabbers, *International Law* (CUP, 2013).

Uta Kohl, *Jurisdiction and the Internet* (CUP, 2007).

Christopher Kuner, *Transborder Data Flows and Data Privacy Law* (OUP, 2013).

Lord Lester and D. Pannick (eds) *Human Rights Law and Practice* (Butterworth, 2004).

James Michael, *Privacy and Human Rights- An International and Comparative Study, with special reference to developments in information technology* (Darmouth Unesco Publishing, 1994).

Marko Milanovic, *Extraterritorial Application of Human Rights Treaties* (OUP, 2011).

Johannes Morsink, *The Universal Declaration of Human Rights- Origins, Drafting and Intent*, (University of Pennsylvania Press,1999).

Stoufflet, *Le droit de la personne sur son image*, vol I (J.C.P 1957).

Roger O'Keefe, *International Criminal Law* (OUP, 2015).

Priscilla M Regan, *Legislating Privacy: Technology, Social Values, and Public Policy* (University of North Carolina Press, 1995).

Cedric Ryngaert, *Jurisdiction in International Law* (OUP, 2008).

Michael Schmitt (ed.), *Tallinn Manual on the International Law Applicable to Cyber Warfare* (CUP, 2013).

Paul Sieghart, *Privacy and Computers* (Latimer, 1976).

Daniel Solove, *Understanding Privacy* (Harvard University Press 2008).

Paul Voigt and Axel von dem Bussche, *The EU General Data Protection Regulation – A Practical Guide* (Springer, 2017).

Judith Wagner DeCew, *In Pursuit of Privacy- Law, Ethics, and the Rise of Technology* (Cornell University Press, 1997).

Rolf H Weber and Dominic Staiger, *Transatlantic Data Protection in Practice* (Springer, 2017).

Alan F Westin, *Privacy and Freedom* (IG Publishing, 2015).

Books Chapters

Ed Bates, 'History' in Daniel Moeckli, et al. (eds), *International Human Rights Law* (2dn, OUP, 2014).

Paul de Hert and Serge Gutwirth, 'Privacy, Data Protection and Law Enforcement. Opacity of the Individual and Transparency of the Power' in Erik Claes, Antony Duff and Serge Gutwirth (eds), *Privacy and the Criminal Law* (Intesentia, 2006).

Oliver Dorr/Kirsten Schmalenbach, 'Article 32' in id (eds), *Vienna Convention on the Law of Treaties: A Commentary* (Springer 2012).

Richard Falk, 'Foreword' in *Essays on Espionage and International Law* (Roland J Stanger ed, 1962).

Helen Keller/Leena Grover, 'General Comments of the Human Rights Committee and their Legitimacy' in Helen Keller/Geir Ulfstein (eds), *Human Right Treaty Bodies: Law and Legitimacy* (CUP 2012).

Bernard H Oxman, 'Jurisdiction of States' in Rudolf Bernhart (ed), *Encyclopedia of Public International Law*, vol. 3 (Elsevier, 1997).

Y Poullet/Serge Gutwirth, 'The Contribution of the Article 29 Working Party to the Construciton of a Harmonised European Data Protecitonk System: An Illustration of 'Reflexive Governance'?' in Marie Pérz-Asinari and Pablo Palazzi (eds), *Challenges of Privacy and Data Protection Law* (Bruylant, 2008).

Ariadna Ripoll Servent, 'Protecting or Processing? Recasting EU Data Protection Norms' in W.J. Schunemann and M-O Baumann (eds), *Privacy, Data Protection and Cybersecurity in Europe* (Springer, 2017).

Stefano Rodotà; 'Data Protection as a fundamental right', in Serge Gutwirth et al., *Reinventing Data Protection?* (Springer, 2009).

Christopher Staker, 'Jurisdiction' in Malcom D Evans (ed), *International Law* (4dn, OUP, 2014).

John Tobin/Sarah M Field, 'Article 16' in John Tobin (ed), *The UN Convention on the Rights of the Child: A Commentary* (OUP 2019).

Judith Jarvis Thomson, 'The right to privacy', in Ferdinand David Schoeman, *Philosophical Dimensions of Privacy* (CUP, 1984).

Bart van der Sloot, 'Is the Human Rights Framework Still Fit for the Big Data Era? A Discussion of the ECtHR's Case Law on Privacy Violations Arising from Surveillance Activities' in Serge Gutwirth et al. (eds), *Data Protection on the Move* (Springer, 2016) Law, Governance and Technologies Series 24.

Bart van der Sloot, 'Legal Fundamentalism: Is Data Protection Really a Fundamental Right?' in Ronald Leenes et al. (eds), *Data Protection and Privacy: (In)visibilities and Infrastructures* (Springer, 2017).

Ian Walden, 'Accessing Data in the Cloud: The Long Arm of the Law Enforcement Agent' in Siani Pearson and George Yee (eds), *Privacy & Security for Cloud Computing* (Springer-Verlag, 2013).

Eliza Watt, 'The Role of International Human Rights Law in the Protection of Online Privacy in the Age of Surveillance' (2017) In: *9th International Conference on Cyber Conflict: Defending the Core*, 30 May (Tallinn, Estonia, 2 Jun 2017).

Quincy Wright, 'Espionage and the Doctrine of Non-Intervention in Internal Affairs', in *Essays on Espionage and International Law* (Roland J. Stanger ed, 1962).

Articles and Papers

'Notes' (July-August 1902) 36 American Law Review 580.

'Recent Important Decisions', Michigan Law Review 3 (May 1905) at 559-63.

Repertoire de Droit civil, Dalloz, Titre 1. Notion et identification des droits de la personnalite, 4.

'Right of Privacy Note' Virginia Law Register 12 (June 1906).

'Standing, Surveillance and Technologies Companies' Chapter 2, Developments in the Law, (2018) 131 Harvard Law Review 1742.

'The Right to Privacy in Nineteenth Century America' (1981) 94 Harvard Law Review 1892.

Mahir Al Banna, 'The Long Arm US Jurisdiction and International Law: Extraterritoriality against Sovereignty' (2017) 60 J.L. Pol'y & Globalisation 60.

Edward R Alo, 'EU Privacy: A Step Towards Global Privacy" (2014) 22 Mich. St. Int'l L. Rev. 1095.

William C Banks, 'Cyber Espionage and Electronic Surveillance: Beyond the Media Coverage' (2017) 66 Emory Law Journal 513.

Badinter, 'Le droit au respect de la vie privée' (1968) J.C.P.I. 2136.

Stephan Balthazar, 'Vérité et Secret: la Protection de la 'vie privée' dans l'ancien droit allemande, français et anglais' (2006) 74 Tijdschrift voor Rechtsgeschiedenis 337.

Christopher D Baker, 'Tolerance of International Espionage: A Functional Approach' (2004) 19 Am. U. Int'l L. Rev. 1091.

Alberto Bernabe, 'Giving Credit Where Credit is Due: A Comment on the Theoretical Foundation and Historical Origin of the Tort Remedy for Invasion of Privacy' (2012) 29 John Marshall J Inf Technol Priv Law 493.

M D Blecher, 'Aspects of privacy in civil law' (1975) 43 Tijdschrift voor Rechtsgeschiedenis 279.

Benjamin E Bratman, ‘Brandeis and Warren’s Right to Privacy and the Birth of the Right to Privacy’ 69 Tenn. L. Rev. 623.

Lee A Bygrave, ‘Data Protection Pursuant to the Right to Privacy in Human Rights Treaties’ (1998) 6 International Journal of Law and Information Technology 247.

Adrien Chaze, ‘La violation du domicile et du droit pénal’ 8 June 2011Le Petit Juriste. <https://www.lepetitjuriste.fr/non-classe/la-violation-de-domicile-et-le-droit-penal/accessed> 15 June 2017.

Simon Chesterman, ‘The Spy Who Came in From the Cold War: Intelligence and International War’ (2006) 27 Mich. J. Int’l L. 1071.

McKay Cunningham, ‘Complying with International Data Protection Law’ (2016) 84 U. Cin. L. Rev. 421.

Jennifer Daskal, ‘The Un-Territoriality of Data’ (2015) 125 Yale L. J. 326.

Lothar Determann/Karl Gutenberg, ‘On War and Peace in Cyberspace: Security, Privacy, Jurisdiction’ (2014) 41 Hastings Const. Law Q. 875.

Ashley Deeks, ‘An International Legal Framework for Surveillance’ (2015) 55 Virginia Journal of International Law 291.

Ingrid Delupis, ‘Foreign Warships and Immunity for Espionage’ (1984) 78 Am. J. Int’l L. 53.

Geoffroy Desmaret, ‘Espionage in International Law’ (1996) 24 Denv. J. Int’l L. & Pol’Y 321.

Oliver Diggleman and Maria Nicole Cleis, ‘How the Right to Privacy Became a Human Rights’ (2014) 4 Human Rights Law Review, Issue 3, 441.

Robert G Dixon, ‘The Griswold Penumbra: Constitutional Charter for an Expanded Right of Privacy?’ [1965] Mich. Law Rev. 197.

Craig Forcese, ‘Spies Without Borders: International Law and Intelligence Collection’ (2011) 5 Journal of National Security Law & Policy 179.

Manuel R Garcia-Mora, ‘Treason, Sedition and Espionage as Political Offenses Under the Law of Extradition’ (1964) 26 U. Pitt. L. Rev. 65.

David J Garrow, ‘Privacy and the American Constitution’ (2001) 68 Soc Res 55.

Raphaël Gellert and Serge Gutwirth, ‘The Legal Construction of Privacy and Data Protection’ (2013) 29 C.L.S.R. 522.

Ilina Georgieva, ‘The Right to Privacy under Fire – Foreign Surveillance under the NSA and the GCHQ and Its Compatibility with Art. 17 ICCPR and Art. 8 ECHR’ (2015) 31 Utrecht J. Int. Eur. Law 104.

Graham Greenleaf, ‘Sheherezade and the 101 data privacy laws: Origins, significance and global trajectories’ (2014) 23 JL Inf. & Sci.

Hyman Gross, ‘The Concept of Privacy’ [1967] N Y Univ. Law Rev 34.

Jean-Louis Halperin, ‘Protection de la vie privée et privacy : deux traditions juridiques différentes ?’ (2015) 48 Nouveaux Cahiers du Conseil Constitutionnel.

Augustus N Hand, ‘Schuyler against Curtis and the Right to Privacy’ (1897) 45 *U. Pa. L. Rev.* 745.

Jeanne M Hauch, ‘Protecting Private Facts in France : the Warren and Brandeis Tort is Alive and Well and Flourishing in Paris’ (1993-1994) 68 Tul. L. Rev. 1219.

Mireille Hildebrandt, ‘Extraterritorial jurisdiction to enforce in cyberspace? Bodin, Schmitt, Grotius in cyberspace’ (2013) 63 U.T.L.J. 196

Ziemele Ineta, ‘Privacy, Right to, International Protection’, *Max Planck Encyclopedia of Public International Law*.

Michael James, ‘A comparative analysis of the right to privacy in the United States, Canada and Europe’ (2013) 29 Conn. J. Int’l L. 257.

David Johnson/David Post, ‘Law and Borders – The Rise of Law in Cyberspace’ (1996) 48 Stanford Law Review 1367.

Paul G Kauper, ‘Penumbras, Peripheries, Emanations, Things Fundamental and Things Forgotten: The Griswold Case’ [1965] Mich. Law Rev. 235.

Pierre Kayser, ‘Les droits de la personnalité : Aspects théoriques et pratiques’ (1971) 69 *Rev. Trim Dr. Civ.* 30.

Juliane Kokott and Christoph Sobotta, ‘The distinction between privacy and data protection in the jurisprudence of the CJEU and the ECtHR’ (2013) 3 International Data Privacy Law 222.

Irwin R Kramer, ‘The Birth of Privacy Law: A Century Since Warren and Brandeis’ (1989) 39 *Cath. UL Rev.* 703.

Christopher Kuner, ‘An International Framework for Data Protection: Issues and Prospects’ (2009) 25 *Computer L. & Security Rev.* 314.

Philip Kuning, ‘Intervention, Prohibition of’ (April 2008) *Max Planck Encyclopedias of International Law*

Hannfried Leisterer/Julian Staben, ‘International Cross-Surveillance: Global IT Surveillance Arbitrage and the Principle of Proportionality as a Counterargument’ (2017) 15 *Surveillance and Society* 108.

Agathe Lepage, ‘Repertoire de Droit civil’ (*Recueil Dalloz*, September 2009, last update November 2017) 41.

Asaf Lubin, ‘A Principled Defence of the International Human Right to Privacy: A Response to Frédéric Sourgens’ 42 Yale J. Int’l L. Online, 1.

Peter Margulies, ‘The NSA in Global Perspective: Surveillance, Human Right, and International Counterterrorism’ (2014) 82 Fordham L. Rev 2137.

L Martin, ‘Le secret de la vie privée’ (1959) Rev. Trim. Dr. Civ. 227.

W Archibald McClean, ‘The Right of Privacy’ (1903) 15 Green Bag 494.

Marko Milanovic, ‘Human Rights Treaties and Foreign Surveillance’ (2015) 56 *Harvard International Law Journal* 81.

Valsamis Mitsilegas, ‘Surveillance and Digital Privacy in the Transatlantic War on Terror: The Case for a Global Privacy Regime’ (2016) 47 Colum. Hum. Rts. L. Rev. 1.

NA Moreham, ‘Unpacking the reasonable expectation of privacy test’ (2018) 134 Law Quarterly Review 651.

Lauren Movius and Nathalie Krup, ‘US and EU Privacy Policy: Comparison’ (2009) 3 *International Journal of Communication* 169.

Afsheen John Radsan, ‘The Unresolved Equation of Espionage and International Law’ (2007) 28 *Mich. J. Int’l L.* 595.

Joel R Reidenberg, ‘The simplification of international data privacy rules’ (2006) 29 Fordham Int’l L.J. 1128.

Jeffrey B Ritter, Benjamin S Hayes, and Henry L Judy, 'Emerging Trends in International Privacy Law' (2001) 15 *Emory Int'l L. Rv.* 87.

Alan Z Rozenshtein, 'Surveillance Intermediaries' (2018) 70 Stanford Law Review 99.

Cedric Ryngaert, 'An Urgent Suggestion To Pour Old Wine into New Bottles- Comment on 'A New Jurisprudential Framework for Jurisdiction' (2015) *AJIL UNBOUND* 81.

Richard A Posner, 'The Uncertain Protection of Privacy by the Supreme Court' (1979) 1979 *Supreme Court Rev*. 173.

Roger Nerson, 'La protection de la vie privée en droit francais' (1971) 23 *RIDC* 737.

Denis O'Brien, 'The Right of Privacy' (1902) 2 Columbia Law Rev. 437, 437–38.

M E H Perreau, 'Des droits de la personnalité' (1909) Rev. Trim Dr. Civ. 501.

William L Prosser, 'Privacy' (1960) 48 California Law Review 383.

Paul M Schwartz, 'Privacy and Participation: Personal Information and Public Sector Regulation in the United States' (1995) 80 Iowa L. Rev. 553.

Paul M Schwartz, 'Regulating Data Mining in the United States and Germany: Constitutional Courts, the State, and New Technologies' (2011) 53 Wm & Mary L. Rev. 351.

Paul M Schwartz/Karl-Nikolaus Peifer, 'Transatlantic Data Privacy Law' (2017) 106 Geo. L. J. 115

Paul Schwartz, 'Global Data Privacy: the EU Way' (forthcoming 2019) 94 NYU Law Review, 3.

Roger D Scott, 'Territorially Intrusive Intelligence Collection and International Law' (1999) 46 A.F.L. REV. 217.

Jeffrey H Smith, 'Symposium: State Intelligence Gathering and International Law: Keynote Address' (2007) 28 Mich J. Int'l L. 543.

Frédéric Gilles Sourgens, 'The Privacy Principle' (2017) 42 Yale J. Int'l L. 345.

Yuko Suda, 'Transatlantic Politics of Data Transfer; Extraterritoriality, Counter-Extraterritoriality and Counter-Terrorism' (2013) 51 JCMS 773.

Dan Jerker Svantesson, 'A New Jurisprudential Framework for Jurisdiction Beyond the Harvard Draft' (2015) 109 AJIL BOUND 69.

Wencelas J Wagner, 'The right to one's own linkess in French law' (1970) 46 Indiana Law Journal 1.

Wencelas J Wagner, 'The development of the theory of the right to privacy in France' (1971) 1971 Wash. U. L. Q. 45.

Wencelas J Wagner, 'Photography and the right to privacy : the French and the Americnan approaches' (1979-80) 25 Cath. Law. 195.

Kate Westmoreland/Gail Kent, 'International Law Enforcement Access to User Data: A Survival Guide and Call for Action' (2015) 13 Canadian Journal of Law and Technology 225.

F P Walton, 'The comparative law of the right to privacy' (1931) 47 L. Q. Rev. 219.

Samuel D Warren and Louis D Brandeis, 'The Right to Privacy' (1890) 4 Harvard Law Review 193.

Eliza Watt, 'The Right to Privacy and the Future of Mass Surveillance' (2017) 21 The International Journal of Human Rights 773.

Horatia Watt, 'A Private (International) Law Perspective Comment on a 'New Jurisprudential Framework for Jurisdiction' (2015) 109 AJIL UNBOUND 75.

James K Weeks, 'Comparative Law of Privacy' (1963) Clev. Marshall L. Rev. 484.

James Q Whitman, 'The Two Western Cultures of Privacy: Dignity versus Liberty' (2004) 113 The Yale Journal 1151.

Leon R Yankwich, 'Right of Privacy: Its Development, Scope and Limitations' (1951) 27 Notre Dame Lawyer 499.

Monika Zalnieriute, 'An International Constitutional Moment for Data Privacy in the Times of Mass-Surveillance' (2015) 23 International Journal of Law and Information Technology 99.

Guobin Zhu, 'The Right to Privacy: An Emerging Right in Chinese Law' (1997) 18 Statute Law Rev. 208.

Reports

American Civil Liberties Union, 'Privacy Rights in the Digital Age: A Proposal for a New General Comment on the Right to Privacy under Article 17 of the International Covenant on Civil and Political Rights: A Draft Report and General Comment' (March 2014) <https://www.aclu.org/sites/default/files/assets/jus14-report-iccpr-web-rel1.pdf> accessed 3 September 2019.

Amnesty International, Privacy International, 'Two Years After Snowden, Protecting Human Rights in an Age of Mass Surveillance' (June 2015) <https://www.amnestyusa.org/wp-content/uploads/2017/04/ai-pi_two_years_on_from_snowden_final_final_clean.pdf> accessed 9 October 2017.

Berkman Klein Centre for Internet & Society, Tiffany Lin/Mailyn Fidler, 'Cross-Border Data Access Reform: A Primer on the Proposed U.S.-U.K. Agreement', Berklett Cybersecurity publication, 7 September 2017) <https://dash.harvard.edu/bitstream/handle/1/33867385/2017-09_berklett.pdf?sequence=1> accessed 15 October 2017.

International Bar Association, 'Report of the Task Force on Extraterritorial Jurisdiction' 2009, < https://www.ibanet.org/Document/Default.aspx?DocumentUid=ECF39839-A217-4B3D-8106-DAB716B34F1E> accessed on 18 Jan 2018

Privacy International, 'Fighting Mass Surveillance in the Post Snowden Era' <https://privacyinternational.org/impact/fighting-mass-surveillance-post-snowden-era> accessed 29 August 2019.

Privacy & C.L. Oversight Board, 'Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act' (2 July 2014) <https://www.pclob.gov/library/702-Report.pdf> accessed 22 September 2019.

Council of Europe

Committee of Ministers, Resolution 73(22) on the protection of the privacy of individuals vis-à-vis electronic data banks in the private sector (adopted 26 September 1973).

Committee of Ministers, Resolution 74(29) on the protection of the *privacy of individuals* vis-à-vis data banks in the public sector (adopted 20 September 1974).

Decision, Consultative Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108) (T-PD) – Abridged report of the 24th plenary meeting (Strasbourg, 13-14 March 2008) Item 10.2. (CM(2008)81).

Explanatory Report on the Convention on Cybercrime (2001) ETS No 185 <https://rm.coe.int/16800cce5b> accessed 22 September 2019.

Factsheet Extra-territorial jurisdiction of States Parties to the European Convention on Human Rights, February 2016, accessible at <http://www.echr.coe.int/Documents/FS_Extra-territorial_jurisdiction_ENG.pdf> (accessed 10 October 2017).

Factsheet Mass Surveillance, November 2017, accessible at <http://www.echr.coe.int/Documents/FS_Mass_surveillance_ENG.pdf> (accessed on 19 Jan. 2018).)

EU Agency for Fundamental Rights (FRA), Council of Europe, Registry of the European Court of Human Rights, and the European Data Protection Supervisor, *Handbook on European Data Protection Law* (2018).

'Guide on Article 8 of the European Convention on Human Rights: Right to respect for private and family life, home and correspondence' (last updated 30 April 2019) <https://www.echr.coe.int/Documents/Guide_Art_8_ENG.pdf> accessed 2 September 2019.

'Case Law of the European Court of Human Rights Concerning the Protection of Personal Data' 15 November 2017, <https://rm.coe.int/case-law-on-data-protection/1680766992> accessed 2 September 2019.

European Union

European Commission, Press Release 'Commission proposes a comprehensive reform of data protection rules to increase users' control of their data and to cut costs for businesses' (25 January 2012) <http://europa.eu/rapid/press-release_IP-12-46_en.htm> accessed 4 July 2019.

European Commission, Fact Sheets (21 December 2015) <http://europa.eu/rapid/press-release_MEMO-15-6385_en.htm> accessed 6 July 2019.

European Commission, 'Communication from the Commission to the European parliament and the Council: Data protection rules as a trust-enabler in the EU and beyond – taking stock' (24 July 2019), COM (2019) 374 final.

UN Docs

International Law Commission

'Report of the International Law Commission on the work of its 58th Session: Annex E – Extraterritorial Jurisdiction' (2006) 229

'Annex IV. Protection of Personal Data in Transborder Flow of Information' in Report of the International Law Commission on the work of its fifty-eight session (1 May to 9 June to 11 August 2006) UN Doc A/61/10, pp. 217-228.

UNHRC

‘General Comment No. 16: Article 17 (Right to Privacy): The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation’ (8 April 1988) UN Doc HRI/GEN/1/Rev.9.

‘General Comment No 31: The nature of the general legal obligation imposed on States Parties to the Covenant’ (26 May 2004) UN Doc CCPR/C/21/Rev.1/Add.13.

‘General Comment No 34 on Article 19: Freedoms of opinion and expression’ (12 September 2011) UN Doc CCPR/C/GC/34.

UNHRC Resolution: ‘The Right to Privacy in the Digital Age’ (24 March 2015) UN Doc A/HRC/28/L.27.

UNHRC Resolution, ‘The Right to Privacy in the Digital Age’ (1 April 2015) UN Doc A/HRC/RES/28/16.

UNHRC Resolution: The Right to Privacy in the Digital Age’ (23 March 2017) UN Doc A/HRC/RES/34/7.

‘Report of the Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms while Countering Terrorism, Martin Scheinin: Addendum: Mission to the United States of America’ (22 November 2007) UN Doc A/HRC/6/17/Add.3.

‘Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Martin Scheinin’ (28 December 2009) UN Doc A/HRC/13/37.

‘Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue’ (16 May 2011) A/HRC/17/27.

‘Report Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue’ (17 April 2013) A/HRC/23/40.

‘Report of Report Special Rapporteur on Promotion and protection of human rights and fundamental freedoms while counter terrorism, Ben Emmerson’ (23 September 2014) UN Doc A/69/397.

‘Report of Report Special Rapporteur on Promotion and protection of human rights and fundamental freedoms while counter terrorism, Joseph A Cannataci’ (30 August 2016) UN A/71/368.

‘Report of the Special Rapporteur on the right to privacy, Joseph A Cannataci’ (8 March 2016) UN Doc A/HRC/31/64.

‘Report of the Special Rapporteur on the right to privacy, Joseph A Cannataci – Note by the Secretariat’ (27 February 2017) UN Doc A/HRC/34/60.

‘Report of the Special Rapporteur on the right to privacy, Joseph A Cannataci – Note by the Secretariat’ (19 October 2017) UN Doc A/72/540.

Joseph A Cannataci Paper presented at Expert Workshop on the right to privacy in the digital age, (Geneva, 19-20 February 2018) UN doc A/HRC/37/62 Annex.

‘Report of the Special Rapporteur on the Right to Privacy – Note by the Secretariat’ (28 February 2018) UN Doc A/HRC/37/67.

‘Right to privacy: Report of the Special Rapporteur on the Right to Privacy’ (21 February 2019) UN Doc A/HRC/40/63.

‘Report of the Special Rapporteur of the Human Rights Council on the right to privacy (19 October) UN Doc A/HRC/72/540.

‘The Promotion, Protection and Enjoyment of Human Rights on the Internet’ (20 June 2012) UN Doc A/HRC/20/L.13.

‘The Right to Privacy in the Digital Age: Report of the Office of the United Nations High Commissioner for Human Rights’ (30 June 2014) UN Doc A/HRC/27/37, para 20.

‘Summary of the Human Rights Council Panel Discussion on the Right to Privacy in the Digital Age’ (19 December 1014) UN Doc A/HRC/28/39, para 44.

Human Rights Committee

‘*Concluding Observations on the Russian Federation’* (1995) UN Doc CCPR/C/79/Add.54.

‘Concluding Observations: Jamaica’ (19 November 1997) UN Doc CCPR/C/79/Add.83

‘*Concluding observations on the fourth periodic report of the United States of America’* (23 April 2014) UN Doc CCPR/C/USA/CO/4.

‘*Concluding observations on the fifth periodic report of* Belarus’ (22 November 2018) UN Doc CCPR/C/BLR/CO/5.

UN Commission on Human Rights

Commission on Human Rights, 2nd Session, Summary Record of the 28th Meeting, 4 December 1947, E/CN.4/SR/28.

Commission on Human Rights, 2nd Session, Summary Record of the 29th Meeting, 8 December 1947, E/CN.4/SR/29.

Commission on Human Rights, 3rd Session, Summary Record of the 55th Meeting, 15 June 1948, E/CN.4/SR.55.

Commission on Human Rights, Report on its 3rd Session, 28 June 1948, E/800 at Annex A (‘Commission Report 800’).

Drafting Committee on an International Bill of Human Rights, Documented Outline, 11 June 1947, E/CN.4/AC.1/3/Add.1.

Drafting Committee on an International Bill of Rights, Report on its 1st Session, 1 July 1947, E/CN.4/21.

Australia: Draft of Additional Articles for the Draft International Covenant on Human Rights, 6 May 1948, E/CN/4/AC.1/21 (‘Australian Proposal’).

Drafting Committee on an International Bill of Human Rights, Report on its 2nd session, 21 May 1948, E/CN.4/95 at Annex A.

Drafting Committee on an International Bill of Human Rights, 2nd Session, Summary Record of the 29th Meeting, 20 May 1948, E/CN.4/AC.1/SR.29.

Drafting Committee on an International Bill of Human Rights, 2nd Session, Summary Record of the 36th Meeting, 17 May 1948, E/CN.4/AC.1/SR.36.

Working Group on the Declaration on Human Rights, Report to the Commission on Human Rights, 10 December 1947, E/CN.4/57.

Draft International Bill of Right (Document E/600) with United States’ Recommendations, 5 May 1948, E/CN.4/AC.1/20.

Comments on Governments on the Draft International Covenant on Human Rights and Measures of Implementation, 16 January 1950, E/CN.4/353/Add.3

Observations of Governments of Member States on the Draft International Covenant on Human Rights, 26 February 1951, E.CN.4/515/Add.6

Commission on Human Rights, Report on its 6th Session, 29 May 1950, E/CN.4/507.

Commission on Human Rights, Report on its 9th Session, 6 June 1953, E/CN.4/689.

OHCHR

'United States Response to OHCHR Questionnaire on 'the Right to Privacy in the Digital Age' <https://www.ohchr.org/Documents/Issues/Privacy/United%20States.pdf> accessed 23 September 2019.

Working Draft Legal Instrument on Government-led Surveillance and Privacy v7 (28 February 2018) <https://www.ohchr.org/Documents/Issues/Privacy/SR_Privacy/2018AnnualReportAppendix7.pdf> accessed 3 September 2019.

'The right to privacy in the digital age' (3 August 2018) UN Doc A/HRC/39/29.

UNGA

'Draft Universal Declaration of Human Rights, Report of the Third Committee' to the 3rd Session of the General Assembly (7 December 1948) A/777.

'Draft International Convenants on Human Rights, Annotations, prepared by the Secretary General' (1 July 1955) UN Doc A/2929.

Third Commission Report to the 15th Session of the GA (8 December 1960) UN Doc A/4625 (reproduced in Bossuyt, Guide to the Travaux Preparatoires of the International Covenant on Civil and Political Rights (Dordrecht: Martinus Nijhoff Publishers, 1987).

H.E. Dilma Rousseff, 'Statement at the Opening of the General Debate of the 68th Session of the United Nations General Assembly' (New York, 24 September 2013) <https://gadebate.un.org/sites/default/files/gastatements/68/BR_en.pdf> accessed 19 August 2019.

'Right to Privacy: Note by the Secretary General transmitting the Report of the Special Rapporteur of the Human Rights Council on the Right to Privacy, Joseph A Cannataci' (19 October 2017) UN Doc A/72/540.

UN Other

United Nations Economic and Social Council Resolution 9 (II): Commission on Human Rights (21 June 1946) UN Doc E/RES/9(II).

United Nations Economic and Social Council Resolution 46(IV): Human Rights (28 March 1947) UN Doc E/Res/46(II).

United Nations Economic and Social Council 151(VII): Report of the third session of the Commission on Human Rights' (26 August 1948) UN Doc E/RES/151(VII).

'Statement of Essential Human Rights presented by the Delegation of Panama' (26 April 1946) UN Doc E/HR.3.

Report of the Secretary-General, Respect for the Privacy of Individuals and the Integrity and Sovereignty of Nations in the Light of Advances in Recording and Other Techniques, 29 U.N. ECOSOC 10 n6, UN Doc. E/CN.4/1116 (Jan. 23, 1973); Id. U.N. Doc. E/CN.4/1116/Add.1 (March 5, 1973); U.N. Doc. E/CN.4/1116/Add.2 (March 19, 1973); Id. U.N. Doc. E/CN.4/1116/Add.3 (Feb 23, 1973); Id. U.N. Doc. E/CN.4/1116/Add.4 (Jan. 8, 1974).

Report of the Secretary-General, Uses of Electronics which may affect the rights of the Person and the Limits which should be Placed on such Uses in a Democratic Society, 30 U.N. ECOSOC, U.N. Doc. C/CN.4/1142 (Jan 1974).

OAS - Inter-American Commission on Human Rights

'Freedom of Expression and the Internet', The Office of the Special Rapporteur for Freedom of Expression of the Inter-American Commission on Human Rights (31 December 2013).

Inter-American Judicial Commission, 'Draft Declaration of the International Rights and Duties of Man and Accompanying Report' (1946) 40 *American Journal of International Law*, 93.

Inter-American Juridical Committee 'Right to Information: Access to and Protection of Information and Personal Data in Electronic Form' (27 February 2007) CJI/doc.25/00

Inter-American Juridical Committee 'Principles on the Right of Access to Information' (7 August 2008) CJI/RES.147 (LXXIII-O/08).

Committee on Juridical and Political Affairs, 'Recommendations on Access to Information' (21 April 2008) CP/CAJP-2599/08.

Inter-American Juridical Committee 'Proposed Statement of Principles for Privacy and Personal Data Protection in the Americas' (9 March 2012) CJI/RES. 186 (LXXX-O/12).

Inter-American Juridical Committee, 'Report by David P. Stewart: Privacy and Data Protection' (25 February 2014) CJI/doc. 450/14; Inter-American Juridical Committee, 'Report by David P. Stewart: Privacy and Data Protection' (26 July 2014) CJI/doc. 465/14.

Inter-American Juridical Committee, 'Privacy and Data Protection' (26 March 2016) CJI/doc. 474/15 rev.2. 3.

Other

APEC 'Privacy Framework' (December 2015) APEC#205-SO-01.

APEC 'Cross Border Privacy Rules' Official Website, <http://cbprs.org/> accessed 20 May 2019).

OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data adopted by OECD Council Recommendation on 23 September 1980 (updated in 2013).

OECD Privacy Guidelines 2013, C(80)58/FINAL, as amended on 11 July 2013 by C(2013)79.

UNESCO, Global Survey on Internet Privacy and Freedom of Expression, Unesco Series on Internet Freedom, Unesco Publishing, 2012.

Memo by Former Legal Adviser of the Department of State H. KOH., Memorandum Opinion on the Geographic Scope of the International Covenant on Civil and Political Rights 19 October 2010, < https://www.justsecurity.org/wp-content/uploads/2014/03/state-department-iccpr-memo.pdf > accessed 19 October 2017.

White House, 'Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy' (February 2012) <https://obamawhitehouse.archives.gov/sites/default/files/privacy-final.pdf> accessed on 1 Oct 2019.

Necessary and Proportionate, International Principles on the Application of Human Rights to Communications Surveillance (March 2014) <https://necessaryandproportionate.org/principles> accessed 29 August 2019.

Review Committee on the Intelligence and Security Services, Joint Statement: Strengthening Intelligence Oversight Cooperation,

<https://english.ctivd.nl/documents/publications/2018/11/14/index> accessed 4 September 2019.

News Articles

'Washington – Secrets of the Telegraph' (*New York Times*, 24 June 1876) p.4, col.7, col. 2.

Julian Borger, 'GCHQ and European spy agencies worked together on mass surveillance' (*The Guardian*, 1 November 2013 <https://www.theguardian.com/uk-news/2013/nov/01/gchq-europe-spy-agencies-mass-surveillance-snowden> accessed 20 October 2017.

Max Ehrenfreund, 'Google, responding to Edward Snowden's leaks, challenges gag order on NSA' (*The Washington Post*, 19 June 2013) <https://www.washingtonpost.com/world/national-security/google-responding-to-edward-snowdens-leaks-challenges-gag-order-on-nsa/2013/06/19/e6bdea0a-d8ef-11e2-a9f2-42ee3912ae0e_story.html?noredirect=on> accessed 19 August 2019.

Ewen Macaskill, et al., 'GCHQ taps fibre-optic cables for secret access to world's communications' (*The Guardian,* 21 June 2013) <https://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa> accessed on 9 October 2017.

James G Meeks et al., 'Intel Heads: Edward Snowden Did 'Profound Damage' to U.S. Security' (*ABC News*, 29 January 2014) <https://abcnews.go.com/Blotter/intel-heads-edward-snowden-profound-damage-us-security/story?id=22285388> accessed 2 September 2019.

Barack Obama, 'Speech on National Security Agency Data Collection Programs' (*The New York Times*, 17 January 2014) <https://www.nytimes.com/2014/01/18/us/politics/obamas-speech-on-nsa-phone-surveillance.html> accessed 15 August 2019

Alan Travis, 'UK-US surveillance regime: statements by political figures before the ruling' (*The Guardian*, 6 February 2015) <https://www.theguardian.com/uk-news/2015/feb/06/mass-surveillance-gchq-key-statements-political-figures> accessed 15 August 2019.

Christopher York, 'Barak Obama Justifies PRISM NSA Surveillance Programme Saying it Has Saved Lives' (*The Huffington Post*, 19 June 2013) <https://www.huffingtonpost.co.uk/2013/06/19/prism-obama-germany-merkel_n_3464613.html> accessed 3 September 2019.

'FISA court ruling on illegal NSA e-mail collection program' (*Washington Post*, 21 August 2013) <https://www.washingtonpost.com/apps/g/page/national/fisa-court-ruling-on-illegal-nsa-e-mail-collection-program/409/> accessed 30 October 2017.

UN News, 'UN official welcomes ASEAN commitment to human rights, but concerned over declaration wording' (19 November 2012) <https://news.un.org/en/story/2012/11/426012> accessed 20 May 2019.

Blogs

Theodore Christakis, 'A Fragmentation of EU/ECHR Law on Mass Surveillance: Initial Thoughts on the Big Brother Watch Judgment' (*European Law* Blog, 20 September 2019) <https://europeanlawblog.eu/2018/09/20/a-fragmentation-of-eu-echr-law-on-mass-surveillance-initial-thoughts-on-the-big-brother-watch-judgment/> accessed 5 September 2019.

Ashley Deeks, 'Does the ICCPR Establish an Extraterritorial Right to Privacy?' (*Lawfare Blog*, 14 November 2013) <https://www.lawfareblog.com/does-iccpr-establish-extraterritorial-right-privacy> accessed 4 October 2017.

Tomaso Falchetta, 'Intelligence Sharing and the Right to Privacy after the European Court Judgment in Big Brother Watch v. UK' (*EJIL: Talk!*, 24 September 2018) <https://www.ejiltalk.org/intelligence-sharing-and-the-right-to-privacy-after-the-european-court-judgment-in-big-brother-watch-v-uk/> accessed 24 September 2019.

Steven Feldstein, 'The Global Expansion of AI Surveillance' (*Carnegie Endowment for International Peace,* 17 September 2019) <https://carnegieendowment.org/2019/09/17/global-expansion-of-ai-surveillance-pub-79847> accessed 29 September 2019.

Alex Lakatos, 'The USA Patriot Act and the Privacy of Data Stored in the Cloud' (*Mayer and Brown Online*, 18 January 2012) <https://www.mayerbrown.com/publications/the-usa-patriot-act-and-the-privacy-of-data-stored-in-the-cloud-01-18-2012/> accessed 18 October 2017.

Christopher Kuner, 'Extraterritoriality and the Fundamental Right to Data Protection' (*EJIL: Talk! Blog Post*, 16 December 2013) <https://www.ejiltalk.org/extraterritoriality-and-the-fundamental-right-to-data-protection/> accessed 20 October 2017.

Marko Milanovic, 'ECtHR Judgment in Big Brother Watch v. UK' (*EJIL Talk!,* 17 September 2018) <https://www.ejiltalk.org/ecthr-judgment-in-big-brother-watch-v-uk/> accessed 29 September 2019.

Anne Peters, 'Surveillance Without Borders: the Unlawfulness of the NSA Panopticon, Part II' (*EJIL: TALK!*, 1 November 2013) <https://www.ejiltalk.org/surveillance-without-borders-the-unlawfulness-of-the-nsa-panopticon-part-ii/> accessed 10 October 2017.

Laura Pitter, 'Comments of Human Rights Watch to Privacy and Civil Liberties Oversight Board Hearings' (19 March 2014) <https://www.hrw.org/news/2014/03/19/comments-human-rights-watch-privacy-and-civil-liberties-oversight-board-hearing> accessed 19 October 2017.

David J Seipp 'The Right to Privacy in American History' (Harvard University: Program on Information Resources Policy, 1978) 2. <http://pirp.harvard.edu/pubs_pdf/seipp/seipp-p78-3.pdf> accessed 16 September 2019.

Brad Smith, 'Time for an International Convention on Government Access to Data' (*Microsoft Blog*, 20 January 2014) <https://blogs.microsoft.com/on-the-issues/2014/01/20/time-for-an-international-convention-on-government-access-to-data/> accessed 21 October 2017.

Kate Westmoreland, 'Jurisdiction over user date – What is the ideal solution to a very real world problem?' (*CIS Blog*, 24 July 2014) <http://cyberlaw.stanford.edu/blog/2014/07/jurisdiction-over-user-data-what-ideal-solution-very-real-world-problem> accessed 15 October 2017.

Kate Westmoreland, 'A New International Convention on International Legal Cooperation?' (ACS Blog, 2 September 2015) <https://www.acslaw.org/acsblog/a-new-international-convention-on-international-legal-cooperation> accessed 21 October 2017.