Groningen Journal of International Law, vol 2(2): Privacy in International Law

Privacy as an International Human Right and the Right to Obscurity in Cyberspace

Alexandra Rengel*

DOI: 10.21827/5a86a81e79532

Keywords
RIGHT TO PRIVACY; HUMAN RIGHTS; RIGHT OF OBSCURITY; PRIVACY BY DESIGN; PERSONAL DATA; CYBERSPACE; INTERNET

Abstract
Fundamental rights are considered to be those which human beings have by the fact of being human and are neither created nor can be abrogated by any government absent extraordinary circumstances. They are fundamental in that the enjoyment of such rights is necessary to live a life with dignity. Fundamental rights are recognized by several international conventions and treaties such as the International Convention on Civil and Political Rights, and the International Convention on Economic and Social Rights and they include cultural, economic, and political rights, such as the right to life, the right to liberty, the right of association, and the right to freedom of religion. Privacy is an essential human need. Although the concept of privacy has a certain abstract quality to it that makes it difficult to define, instinctively, humans need to know that they can keep some things secret from others. Absent extraordinary circumstances the need for humans to have a certain degree of privacy is innate. Perhaps as a result of that intrinsic need, privacy as a concept has been recognized in a social as well as a legal sense in most cultures from time immemorial. Today, the right to privacy is considered to be an identifiable human right with universal qualities deserving legal recognition and protection, although the scope of such legal protection is still being determined.

In reviewing the concept of privacy, new technologies often make us wonder what level of protection of our right to privacy is possible in a world where personal information about us can be accessed not by infringing our physical space, but by invisible hands that can access our most private secrets just by pressing a button and looking at a screen. New technologies in the form of the Internet, social networks, remote access to information, etc., make it increasingly more difficult to maintain privacy rights in cyberspace such that online invisibility has become impossible. The quest for invisibility is the idea that individuals should be able to choose to remain invisible online. In order for that scenario to become a reality more emphasis needs to be made on the universal recognition of privacy principles in the context of cyberspace.

* Alexandra I. Rengel is the author of *Privacy in the 21st Century*, Martinus Nijhof Publishers. She is an attorney in private practice in the firm of Mercado & Rengel. Ms. Rengel received her B.A. from Mount Holyoke College and earned her JD from Boston University School of Law. Ms. Rengel is a *summa cum laude*, valedictorian graduate of the St. Thomas University School of Law LLM. Program in Intercultural Human Rights. She also obtained her JSD at St. Thomas University School of Law, writing her dissertation on the right to privacy in the international context, for which she was distinguished with *summa cum laude* honors. Ms. Rengel teaches at Suffolk University, Madrid campus; at Comillas Pontifical University in Madrid; and at the Instituto de Empresa in Madrid. She is also a frequent lecturer on human rights, international business law and arbitration. Ms. Rengel writes this article with special thanks to her husband, Ivan Mercado and her children Maria and Ivan.

Additionally, design based privacy solutions must be created to protect individuals' privacy in cyberspace.

I. The Law of Nations and Fundamental Human Rights

Before the Roman Empire, religion served as the paramount source of the law of nations.[1] During the Middle Ages, international, or universal, law merged with ecclesiastical law, and even treaty law was considered to have legal force only because treaties were confirmed by oath, which, being a "sacrament," subjected the obligation incurred to the jurisdiction of the Church.[2] Medieval legal scholars did not distinguish municipal from international law, instead viewing the law of nations as a universal law, binding upon all mankind.[3] Thus, in these early years, the public/private, domestic/international categories that later came to dominate classical international legal theory had not been developed, and were, in practice, unnecessary. The law of nations was thought to embrace private as well as public, domestic, as well as transborder, transactions, and to encompass not simply the "law of states," such as rules relating to passports and ambassadors, but also the law between states and individuals, including the "law maritime" (affecting shipwrecks, admiralty, prizes and the like) and the "law merchant" (*lex mercatoria*), applicable to transnational commercial transactions.[4] Throughout the eighteenth century, an increasing interdependence and interaction between nations called for a more uniform system of laws. Under the modern framework of international system of laws adopted, the scope of authority possessed by international organisations depends almost entirely upon the constitutional limitations in their charters as well as a nation's express consent to submit to the authority of those international organisations.[5] However, over time, international law has also benefitted from the

---

1 See generally Bederman, D. J., "Religion and the Sources of International Law in Antiquity", *in:* Janis, M. W. and Evans, C., eds., *The Influence of Religion on the Development of International Law*, Martinus Nijhoff Publishers, The Hague. 1999, (In his article, Bederman traces the role of religion in the Near East during the empires of Egypt, Babylon, Assyria, Hittites, Mittani, Israelites, Greek city-states, Indian states before 150 BC, and Mediterranean powers before 168 BC).

2 Nussbaum, A., *A Concise History of the Law of Nations*, Macmillan Co., New York, 1947, 58–59.

3 Dickinson, E. D., "The Law of Nations as Part of the National Law of the United States", *University of Pennsylvania Law Review*, vol. 101, ed. 1, 1952, 26–27.

4 Berman, H. J. and Kaufman, C., "The Law of International Commercial Transactions (Lex Mercatoria)", *Harvard International Law Journal*, vol. 19, ed. 1, 1978, 224–229 (explaining that law merchant was transnational private law based not on any single national law but on mercantile customs generally accepted by trading nations).

5 See United Nations, Charter of the United Nations, 24 October 1945, 1 UNTS 16, Articles 1–2 (detailing purposes of the UN and limits on the UN's international authority); Statute of the International Court of Justice, June 26 1945, 33 UNTS 993, Articles 34–38 (limiting competence of ICJ). The Charter of the United Nations declares itself to be an embodiment of positive law. See *ibid* (outlining the purposes and limits of the UN). The Charter states that its intent is to 'establish an international organization to be known as the United Nations', see UN Charter preamble, and specifically limits its membership to 'all other peace-loving States which accept the obligations' of the Charter. See UN Charter Article 4 (discussing the intent of UN Charter).
The UN Charter also constitutionally limits the scope of the organisation's function and purpose. UN Charter Articles 1–2. The Charter indicates that its purposes and principles are:

> 1. To maintain international peace and security; ...
> 2. To develop friendly relations among nations based on respect for the principle of equal rights and self-determination of peoples, and to take other appropriate measures to strengthen universal peace;

recognition of international custom as a source of law. The law of nations includes the Statute of the International Court of Justice (ICJ); [6] Article 38 of the Statute of the International Court of Justice lists the sources of international law and includes what is known as "customary international law." [7] Customary international law has equal authority with conventional laws, such as treaty law, and is relied upon for its important role in providing a rule of law in areas of international law in which there is no applicable conventional rule. Customary international law receives the status of "law" because the ICJ considers custom as 'evidence of a general practice accepted as law' and thus as 'part of the corpus of general international law.'[8] International customary law consists of the general practices or rules of behaviour that states observe and follow out of a sense of self-perceived legal obligation.[9] There is no minimum number of adhering states required to meet the generality requirement. The United States Supreme Court in *The Paquete Habana* case[10] and the Permanent Court of International Justice in The Case of the S.S. Wimbledon[11] and *The S.S. Lotus* case[12] deduced rules of customary international law from the practice of fewer than a dozen states.[13] Customary law gains decision-making value through state practice, which eventually develops into a legal norm through persistent use

---

3. To achieve international co-operation in solving international problems of an economic, social, cultural or humanitarian character, and in promoting and encouraging respect for human rights and for fundamental freedoms for all without distinction as to race, sex, language, or religion; and
4. To be a centre for harmonizing the actions of nations in the attainment of these common ends.

Ibid. Article 1 (discussing the intent of the UN Charter).

Further, the UN Charter expressly limits the ability of the United Nations to act in international matters without the express consent of the involved nations:

1. The Organization is based on the principle of the sovereign equality of all its Members.
7. Nothing contained in the present Charter shall authorize the United Nations to intervene in matters which are essentially within the domestic jurisdiction of any State or shall require the Members to submit such matters to settlement under the present Charter; ...

Id. Article 2 (discussing limitations on UN's authority to act in international matters).

6 Statute of the International Court of Justice, June 26 1945, 33 UNTS, 993.

7 *Id.*, Article 38(1)(b).

8 *Id.,* Article 38(1)(b); International Court of Justice, *North Sea Continental Shelf*, Judgment of 20 February 1969, ICJ Reports, 3, 28.

9 Restatement of the Law Third: The Foreign Relations Law of the United States, American Law Institute Publishers, 1987, Article 102.

10 The United States Supreme Court, 8 January 1900, *The Paquete Habana*, 175 US 677, (1900), 707–708.

11 Permanent Court of International Justice, *Case of the S.S. Wimbledon*, Judgment of 17 August 1923, PCIJ (ser. A) No. 1, 15, 25 and 28. In this case, the Court cited only the Suez Canal and Panama Canal regimes as "precedents" for the rule involving the Kiel Canal.

12 Permanent Court of International Justice, *The Case of the S.S. Lotus*, Judgment, of 7 September, PCIJ (ser. A) No. 10 1927, 4 and 29. The Court cited, as decisive precedents, cases involving only five states: France, Italy, Great Britain, Germany, and Belgium. On 2 August 1926 there was a collision between the S.S. Lotus, a French steamship (or steamer), and the S.S. Boz-Kourt, a Turkish steamer, in a region just north of Mytilene. As a result of the accident, eight Turkish nationals aboard the Boz-Kourt drowned when the vessel was torn apart by the Lotus. The main issue in the Lotus case was jurisdiction. The issue at stake was Turkey's jurisdiction to try Monsieur Demons, the French officer on watch duty at the time of the collision.

13 Some scholars have argued for the rule of generality to be relaxed. For example, D'Amato rejects the view that there must exist "broad participation" of states in the creation of the rule to be consistent with principles of customary international law. His standard for a valid claim based on a rule of customary law would require only that an 'objective claim of international legality be articulated in advance of, or concurrently with, an act which will constitute the quantitative elements of custom.' D'Amato, A., *International Law: Process and Prospect*, Cornell University Press, New York, 1971, 191–192.

and final acceptance by domestic and international jurists and commentators.[14] In the context of human rights, the notion that there is a "higher" type of law that can be enforced internationally without the express consent of the sovereign is well recognised. Based partly on treaty law as well as customary international law, human rights law provides a set of universal standards that transcend particular cultural and historical circumstances, making it possible for trained observers to judge the conduct of both individuals and nations.[15] International human rights law attempts to adapt the practices of local cultures in order to bring them in line with certain universal principles of human rights.[16] As such, international human rights law is based on the idea that there are universal standards of human rights that supersede local and cultural customs that are not necessary to life itself, but which are considered necessary for human beings to live a dignified life. The Universal Declaration of Human Rights, which was the first document to enumerate a list of rights, represents the ideal that there are certain rights that ought to be universally protected.[17]

The Universal Declaration of Human Rights was not meant to impose legal obligations on states at the time of its adoption by the General Assembly in 1948. The status of the Declaration as described by the United Nations was that of 'a manifesto with primarily moral authority,' the first of four stages in the generation of the documents the General Assembly has collectively called the International Bill of Human Rights.[18] In contrast to the more political or hortatory Declaration, the subsequent three documents: the International Covenant on Civil and Political Rights, its Optional Protocol, and the International Covenant on Economic, Social and Cultural Rights were consciously adopted as legally binding treaties open for ratification or accession by states.[19]

Subsequent to the ratification of what is called the International Bill of Rights, international human rights law has continued its development. The creation of international tribunals, which are capable of judging the conduct of states, and even individuals, who might have committed human rights violations, was possible because of a belief that there were certain basic principles that could be universally recognised despite variations in cultures and customs around the world, and despite the lack of a universal legislative body creating a set of laws applicable to all.[20] Today, it is well

---

[14] Simma, B. and Alston, P., "The Sources of Human Rights Law: Custom, Jus Cogens, and General Principles", *in:* Alston, P., ed., *Human Rights Law,* New York University Press, New York, 1996*,* 3–8.

[15] Stanlis, P. J., *Edmund Burke and the Natural Law*, University of Michigan Press, Michigan, 1958, 7: ´Natural Law was an eternal, unchangeable, and universal ethical norm or standard, whose validity was independent of man's will; therefore, at all times, in all circumstances and everywhere it bound all individuals, races, nations, and governments.´); Verdross, A., "Jus Dispositivum and Jus Cogens in International Law", *American Journal of International Law*, vol. 60, ed. 1, 1966, 55.

[16] Koh, H. H., "How is International Human Rights Law Enforced?", *Indiana Law Journal,* vol. 74, ed. 4, 1999, 1416–1417.

[17] UN General Assembly, Universal Declaration of Human Rights, 10 December 1948, 217 A (III).

[18] The four instruments referred to as the International Bill of Human Rights are as follows: Universal Declaration of Human Rights; The Charter of the United Nations; The International Covenant on Civil and Political Rights, 16 December 1966, 171 UNTS 999; The International Covenant on Economic Social and Cultural Rights, 16 December 1966, 3 UNTS 933.

[19] *Ibid*.

[20] Such claims attached in particular to influential United Nations Documents such as the Universal Declaration of Human Rights, *supra* nt. 17.

established that there are certain human rights that are fundamental to human dignity and must be legally protected by all nations.[21]

II. Privacy as a Fundamental Human Right

References to the concept of individual privacy have been prevalent since the inception of civilisation. The concept of privacy is mentioned in the Code of Hammurabi,[22] the Bible,[23] the Qur'an,[24] Jewish law,[25] and was present in classical Greece and ancient China.[26] The need for privacy is not limited to certain cultures, and most societies regard some areas of human activity as being unsuitable for general observation and knowledge.[27] However, despite the recognition of the need for privacy in the abstract, providing a concrete definition of the notion has eluded social scientists, jurists, philosophers, and others seeking singular clarity on the subject.[28] Robert Post stated that: '[p]rivacy is a value so complex, so entangled in competing and contradictory dimensions, so engorged with various and distinct meanings, that I sometimes despair whether it can be usefully addressed at all.'[29] Arthur Miller declared that privacy is 'difficult to define because it is exasperatingly vague and evanescent.'[30]

---

[21] For a critique of the "universalist" and "relativist" views of human rights see generally Weston, B.H., "Human Rights and Nation-Building in Cross-Cultural Settings", *Maine Law Review*, vol. 60, ed. 2, 2008, 318, Professor Weston concludes as follows

> In any event, one thing is certain: if one is to take seriously the proposition that respect is "the core value of all human rights," there is no escaping that cross-cultural decision-making about relativist-universalist controversies cannot be a simpleminded affair. Necessarily, it must reflect the complexity of life itself, implicating a whole series of interrelated activities and events that are indispensable to effective inquiry and therefore to rational and respectful choice in decision.

[22] The Code of Hammurabi is a Babylonian law code dating back to about 1772 BC which details a set of principles meant to guide citizens of Babylonia with various activities such as agriculture, commerce, land rights, and contractual agreements. Article 21 of the Code of Hammurabi states: '[i]f a man makes a breach into a house, one shall kill him in front of the breach and bury him in it.' Article 21, *Code of Hammurabi*, 1750–1700 BC as quoted *in:* Lasson, N. B., *The History of the Development of the Fourth Amendment to the United States´ Constitution*, John Hopkins Press, Baltimore, 1937, 14–15.

[23] Hixson, R., *Privacy in a Public Society: Human Rights in Conflict*, Oxford University Press, New York, 1987, 3; Moore, B., *Privacy: Studies in Social and Cultural History*, Random House, New York, 1984.

[24] *Sahih Bukhari*, Volume 1, Book 10, Number 509; *Sahih Muslim*, Book 020, Number 4727; *Sunan Abu Dawud*, Book 31, Number 4003.

[25] Rosen, J., *The Unwanted Gaze: The Destruction of Privacy in America*, Random House, New York, 2000, 16.

[26] Moore, *supra* nt. 23; Jingchun, C., "Protecting the Right to Privacy in China", *VUW Law Review*, vol. 36, ed. 3, 2005, 646–647 (the author states that privacy was protected, to some extent, in ancient China and an awareness of privacy may be found in the Warring States Period, referring to the era of about 475 BC to 221 BC).

[27] Mead, M., *Coming of Age in Samoa: A Psychological Study of Primitive Youth for Western Civilization*, American Museum of Natural History, New York, 1973, 219. (Margaret Mead studies of Samoan culture which revealed that children were raised by village members and exposed to all aspects of life in the public arena).

[28] See, e.g., Young, J. B., "Introduction" *in:* Young, J. B., ed., *Privacy 2,* 1978: '[P]rivacy, like an elephant, is perhaps more readily recognized than described.'; Krotoszynski, R.J., "Autonomy, Community, and Traditions of Liberty: The Contrast of British and American Privacy Law*", Duke Law Journal*, vol. 1990, ed. 6, 1398–1454, 1401.

[29] Post, R. C., "Three Concepts of Privacy*"*, *Georgetown Law Journal*, vol. 89, ed. 6, 2001, 2087–2098, 2087.

[30] Miller, A. R., *The Assault on Privacy: Computers, Data Banks and Dossiers*, University of Michigan Press, Michigan, 1971, 25; see also Gormley, K., "One Hundred Years of Privacy", *Wisconsin Law Review*, vol.

The basic need for privacy at a personal level and for society as a whole also translates into the expectation that our governments will protect our privacy from unwanted intrusions. However, in order to determine the behaviours that cause a breach of the right to privacy and what level of protection is warranted, it is essential to clarify what the term privacy means, and to distinguish between the concept of privacy and the right to privacy.[31] The concept of privacy involves a definition of what it entails as well as how is it valued, while the right to privacy refers to the recognition that privacy should be legally protected. It is understood, however, that the concept of privacy and the right to privacy are intertwined, because without a definition of privacy, or at a minimum, a concrete way to conceptualise privacy, it would be impossible to formulate the appropriate legal framework for the protection of the right to privacy.

As for those who have attempted to provide an all-encompassing working definition of privacy, the definitions are varied. Privacy has been defined in the context of personal autonomy or control over the intimacies of personal identity.[32] Some define privacy as focusing on control over information about oneself. [33] Alan Westin described privacy as a 'claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others'.[34] According to Hyman Gross, 'privacy is the condition of human life in which acquaintance with a person or with affairs of his life which are personal to him is limited'.[35] Philosopher Sissela Bok states that 'privacy is the condition of being protected from unwanted access by others – physical access, personal information, or attention'.[36] Daniel Solove, after studying the concept of privacy in great depth, has classified the different conceptions of privacy into six general types: (1) the right to be let alone; (2) limited access to the self – the ability to shield oneself from unwanted access by others; (3) secrecy – the concealment of certain matters from others; (4) control over personal information – the ability to exercise control over information about oneself; (5) personhood – the protection of one's personality, individuality, and dignity; and (6) intimacy – control over, or limited access to, one's intimate relationships or aspects of life.[37] Although there is clearly an overlap of the different conceptions, this classification reflects the various theories on privacy. After examining the six categories, Solove finds that if the purpose of

---

1992, ed. 5, 1992, 1335, 1339: '[L]egal privacy consists of four or five different species of legal rights which are quite distinct from each other and thus incapable of a single definition.'; Mc Carthy, J. T., *Rights of Publicity and Privacy*, Clark Boardman Callaghan, New York, 1999, section 5:59: 'It is apparent that the word "privacy" has proven to be a powerful rhetorical battle cry in a plethora of unrelated contexts .... Like the emotive word "freedom", "privacy" means so many different things to so many different people that it has lost any precise legal connotation that it might once have had.'; Gross, H., "The Concept of Privacy", *New York University Law Review*, vol. 42, ed. 1, 1967, 34, 34–35: 'stating that, we can readily recognise a threat to privacy 'yet stumble when trying to make clear what privacy is'.

31 Solove, D. J., "Conceptualizing Privacy", *California Law Review*, vol. 90, ed. 4, 2002, 1087–1156, 1088.

32 Gerety, T., "Redefining Privacy", *Harvard Civil Rights-Civil Liberties Law Review*, vol. 12, ed. 2, 1977, 236.

33 Parent, W., "Privacy, Morality and the Law", *Philosophy and Public Affairs*, vol. 12, ed. 4, 1983, 323–333.

34 Westin, A. F., *Privacy and Freedom*, Atheneum, New York, 1970, 330–364. The author further explained that: '[v]iewed in terms of the relation of the individual to social participation, privacy is the voluntary and temporary withdrawal of a person from the general society through physical or psychological means, either in a state of solitude or small-group intimacy, or, when among larger groups, in a condition of anonymity or reserve.

35 Gross, *supra* nt. 30, 35–36.

36 Bok, S., *Secrets: On the Ethics of Concealment and Revelation*, Pantheon, New York, 1983, 10–11.

37 Solove, D., *Understanding Privacy*, Harvard University Press, Cambridge, 2009, 13.

conceptualising privacy is to define its unique characteristics, the classifications fall short of achieving that task because they are either too narrow, thereby failing to include some aspects of life generally viewed as private, or too broad and fail to exclude matters not generally viewed as private.[38] Solove's own theory of privacy is that

> The value of privacy must be determined on the basis of its importance to society, not in terms of individual rights. Moreover, privacy does not have a universal value that is the same across all contexts. The value of privacy in a particular context depends upon the social importance of the activities that it facilitates.[39]

In effect, Solove contends that we should explore what privacy means for individuals by looking at real privacy problems. He advances a pragmatic approach to conceptualising privacy, by looking at how practices involving privacy have changed throughout history and by advocating a contextual analysis of privacy.[40]

As a right, privacy has been defined as the general 'right to be left alone',[41] and a 'generic term encompassing various rights recognized ... to be inherent in the concept of ordered liberty.'[42] The right to privacy is related to the right to secrecy, to limiting the knowledge of others about oneself.[43] As such, the right to privacy could be described as the right to keep a sphere of our lives away from government intrusion, and away from the intrusion of others with whom we do not want to share certain aspects of our lives. In that sense, the right to privacy would mean a myriad of different things such as, control over personal information, freedom from surveillance, protection from invasions into one's home, personal autonomy, control over one's body and a series of other things.[44]

Some scholars have argued that the right to privacy is a necessary requirement for life in modern democratic society.[45] Political scientist Priscilla Regan states that privacy interests are not individual interests but the interests of society. She explains how individual perceptions fail to appreciate the importance of privacy for individuals fails to recognise its importance as common, public and collective values. According to Regan, '[m]ost privacy scholars emphasize that the individual is better off if privacy exists; I argue that society is better off as well when privacy exists. I maintain that privacy serves not just individual interests but common, public, and collective purposes.'[46] In the abstract, the moral value placed on the concept of privacy varies. Most argue that privacy

---

38 *Ibid.*

39 *Id.* 39–77.

40 *Ibid.*

41 See S. Warren and L. Brandeis, "The right to Privacy"*, Harvard Law Review* vol, 4, ed. 5, 1890, 193.

42 US Supreme Court, *Katz v. U. S.*, 389 US 347, at 350 (1967*);* Texas Supreme Court, *Industrial Foundation of the South v. Texas Industrial Accident Board*, 540 SW 2d 668, 679(1976).

43 Cavoukian, A. and Tapscott, D., *Who Knows: Safeguarding Your Privacy in a Networked World,* McGraw-Hill, New York, 1997.

44 See Newell, P. B., "Perspectives on Privacy", *Journal of Environmental Psycholo*gy, vol. 15, ed. 2, 1995, 87–105. In this comprehensive review of literature, published in 1995, psychologist Patricia Brierley Newell identified at least seventeen discrete concepts of privacy. These included describing privacy as a phenomenal state or condition of the person, a quality of place, a space of refuge, a goal, a descriptor of personal space or territoriality, a level of close personal intimacy, a behaviour, a process, a legal right, a descriptor of an interactive condition (such as an attitude, solitude, anonymity, and secrecy) and the ability to control information, among others.

45 Westin, A. F., *Privacy and Freedom*, The Bodley Head Ltd, London, 1970, 330–364.

46 Regan, P., *Legislating Privacy: Technology, Social Values, and Public Policy*, University of North Carolina Press, Chapel Hill, 1995.

as a concept is an intrinsic good,[47] and that privacy is closely implicated in the notions of respect for others and oneself, as well as love, friendship and trust.[48] Jeffrey Reiman states that privacy functions 'as a means of protecting freedom, moral personality, and a rich and critical inner life.'[49] Edward Bloustein wrote that privacy is an interest of human personality, and to protect an individual's privacy is to protect the individual's personality, independence, dignity and integrity.[50] Others defend it as a broader concept necessary for the development of varied and meaningful relationships.[51] Thus, privacy can be viewed not only as a personal value intrinsically beneficial to preserving our sense of self, but also an essential value for society.

The right to privacy has been long recognised by the international community. A review of the basic international conventions of international human rights reveals that privacy is mentioned in most of them.[52] Pursuant to article 28 of the International Covenant on Civil and Political Rights, (ICCPR), a committee of 18 independent experts, known as the Human Rights Committee, was formed to oversee implementation of the ICCPR within the States Parties to that treaty.[53] Although, the text of the ICCPR is ambiguous about what is intended by the "general comments". According to article 40(4), the Human Rights Committee may issue "general comments," to be distributed to States Parties and which are deemed to be "authoritative interpretations" of the relevant part(s) of the ICCPR that the particular comments address.[54] The Human Rights Committee issued a General Comment on article 17 of the ICCPR, which embodies the right to privacy, discussing and clarifying concepts such as: "arbitrary interference", "family", "home" and "correspondence".[55] The General Comment sheds light on how the ICCPR should interpret the right to privacy within the realm of international law.[56]

---

47 Schoeman, F. D., "Privacy and Intimate Information"*, in:* Schoeman, F.D., ed., *Philosophical Dimensions of Privacy: An Anthology*, Cambridge University Press, Cambridge, 1984, 403.

48 Fried, C., "Privacy", *Yale Law Journal*, vol. 33, ed. 3, 1968, 475–493.

49 Reiman, J., "Driving to the Panopticon: A Philosophical Exploration of the Risks to Privacy Posed by the Highway Technology of the Future", *Santa Clara High Tech. Law Journal*, vol. 11, ed. 1, 1995, 27–44.

50 Bloustein, E., "Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser", *New York University Law Review*, vol. 39, 1964, 962–1007, 971.

51 Gerstein, R. S., "Intimacy and Privacy", *Ethics,* vol. 89, ed. 1, 1978, 76–81; Innes, J., *Privacy, Intimacy and Isolation*, Oxford University Press, New York, 1992.

52 The main human rights instruments are as follow: Universal Declaration of Human Rights, Article 12; International Covenant on Civil Political Rights, Article 17 (1966); UN International Covenant on Economic Social and Cultural Rights, Article 11; UN International Convention on the Elimination of All Forms of Racial Discrimination, 660 UNTS 195 (1969), Article 5; International Conference of American States, The American Declaration of the Rights and Duties of Man, 9th Sess., UN Doc. E/CN.4/122 (1948), Article 9; Organization of American States, American Convention on Human Rights "Pact of San Jose, Costa Rica" (B-32), 22 January 1969, Article 11; Council of Europe, European Convention for the Protection of Human Rights and Fundamental Freedoms, as amended by Protocols Nos. 11 and 14, 4 November 1950, ETS 5, Article 8; Organization of the African Union, The African Charter on Human and People's Rights, Doc. CAB/LEG/67/3/Rev.5 (1981), 5, 21 ILM 58 (1982).

53 *Id.*, Article 28.

54 *Ibid.*

55 GA Report of the Human Rights Committee (43rd session) A/43/40, 1988.

56 *Id.*, para. 1. Here it states the following: 'Article 17 provides for the right of every person to be protected against arbitrary or unlawful interference with his privacy, family, home or correspondence as well as against unlawful attacks on his honour and reputation. In the view of the Committee this right is required to be guaranteed against all such interferences and attacks whether they emanate from State authorities or from natural or legal persons. The obligations imposed by this article require the State to adopt legislative and other measures to give effect to the prohibition against such interferences and attacks as well as to the protection of this right.'

According to the Human Rights Committee, the term "unlawful" as it appears in Article 17 explains that no one's privacy must be interfered with unless reasoned by law.[57] In the event that an intrusion into a person's privacy is necessary '[t]he 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.'[58] The gathering of personal information is also addressed in the General Comment providing that law must regulate such collection.[59] Likewise, states are under an obligation to provide adequate legislation for the protection of personal honour and reputation.[60] The General Comment also clarifies that under Article 17 of the ICCPR that privacy rights are not absolute.[61] In addition to the General Comment, the European Convention of Human Rights and the Universal Declaration of Human Rights limit the scope of protection, recognising offsetting interests to which the right to privacy must yield.[62] Thus, states may lawfully restrict an individual's rights in order to protect the rights of others, the general welfare, public order, morality and the security of all.[63] However, these restrictions may not result in rendering the right a nullity.

Gradually, the right to privacy has become universally recognised as a fundamental human right. In addition to being addressed in the most important international and regional human rights treaties, some aspect of the right to privacy is incorporated into almost every constitution in the world, and into the general laws and jurisprudence of

---

[57] *Id.,* para. 3.

[58] *Id.*, para. 7.

[59] *Id.*, para. 10.

[60] *Id.,* para. 11.

[61] *Id.,* paras. 7–9.

[62] See Convention for the Protection of Human Rights and Fundamental Freedoms, 1953, 213 UNTS. 222, Article 8 (European Convention on Human Rights). It states the following:

> (1) Everyone has the right to respect for his privacy and family life, his home and 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.

See Article 29 Universal Declaration of Human Rights. The Universal Declaration of Human Rights imposes a general restriction in Article 29 upon the rights recognised in the instrument:

> (1) Everyone has duties to the community in which alone the free and full development of his personality is possible. (2) In the exercise of his rights and freedoms, everyone shall be subject only to such limitations as are determined by law solely for the purpose of securing due recognition and respect for the rights and freedoms of others and of meeting the just requirements of morality, public order and the general welfare in a democratic society.

Article 4 of the International Covenant on Civil and Political Rights specifically states that derogation is possible in time of an emergency. Although Article 4(2) also notes some articles from which derogation is not possible. Since article 17, on the right to privacy, is not mentioned under that provision, it should be assumed that derogation is possible on the right to privacy.

> 1. In time of public emergency which threatens the life of the nation and the existence of which is officially proclaimed, the States Parties to the present Covenant may take measures derogating from their obligations under the present Covenant to the extent strictly required by the exigencies of the situation, provided that such measures are not inconsistent with their other obligations under international law and do not involve discrimination solely on the ground of race, colour, sex, language, religion or social origin.
> 2. No derogation from articles 6, 7, 8 (paragraphs I and 2), 11, 15, 16 and 18 may be made under this provision.

Articles. 4 and 17 International Covenant on Civil and Political Rights.

[63] *Id.*, Article 32(1); Universal Declaration of Human Rights, Article 29(2).

those countries without written constitutions.[64] Countries that have no written constitutions extend privacy protections through their other legal norms such as procedural rules, evidentiary codes, and statutory protections,[65] so that the protection of privacy has become a common component of the laws of nearly every country.[66] Given the recognition of the right to privacy in the most important international treaties, the legal acknowledgment of the right to privacy in the majority of legal systems, and the generalised belief among jurists and scholars of the importance of privacy, it can be concluded that this right has become part and parcel of customary international law. Although the right to privacy is not absolute, and must yield when other societal interests are at stake, a balancing test must take into account the universality of the right and the acts it protects,

International law recognises privacy as an important aspect of human dignity. The need to implement adequate protections is exacerbated by the development of new technologies that facilitate the invasion and interference with an individual's privacy.[67] To determine the effect of new technologies on the right to privacy, and provide adequate solutions, a contextual analysis of the potential infringements that technology facilitates and the resources available for protection is essential. Such analysis requires first, an examination of how technological progress has changed individuals' behaviour and affected society as a whole regarding privacy, and then, finding the adequate solutions to address privacy concerns in a manner that embraces the benefits of technological advancement while balancing the individual's right to privacy.

III. The Effect of Information Technologies and the Internet on the Right to Privacy

It is indisputable that the capacity, power, speed, and impact of information technology has been, and continues to be, accelerating rapidly. With these advancements there is also a corresponding increase in the risks to privacy.[68] The demands of a democratic society and its obligations towards protecting individual rights must be balanced against the need and appetite for electronic commerce and information technology. The reality is that technologies that might be invasive of one's privacy also have the potential for unprecedented opportunities for enlightenment, prosperity and security. Traditionally, privacy law has developed in the footsteps of technology constantly reshaping itself to meet the privacy threats embodied in new technologies.[69] The information revolution,

---

[64] Edwards, G. E., "International Human Rights Law Challenges to the New International Criminal Court: The Search and Seizure Right to Privacy", *Yale Journal of International Law*, vol. 26, 2001, 323–412, 327.

[65] One example is the United Kingdom, which lacks a written constitution but has statutory laws and other protections for privacy in place. See Krotoszynski, R. J., "Autonomy, Community, and Traditions of Liberty: The Contrast of British and American Privacy Law", *Duke Law Journal*, vol. 39, ed. 6. 1990, 1398–1454, 1401.

[66] See Rengel, A. I., *Privacy in the 21st Century*, Martinus Nijhof Publishers, Leiden, 2013, 205–255. The author addresses specific aspects of the right to privacy that have become part of customary international law by looking at treaties, international court decisions, opinions by jurists, commentators and state practice.

[67] Froomkin, A. M., "The Death of Privacy?", *Stanford Law Review*, vol. 52, no. 5, 2000, 1461–1543, 1468.

[68] See Solove, D. J., "Privacy and Power: Computer Databases and Metaphors for Information Privacy", *Stanford Law Review*, vol. 53, ed. 6, 2001, 1393–1462, 1394.

[69] See Hernandez, D. F., "Litigating the Right to Privacy: A Survey of Current Issues", *446 PLI/Pat* 425, 1996, 429.

however, has been taking place at such speed and affecting so many areas of privacy law that the orthodox, adaptive legislative and judicial process has failed to address digital privacy problems adequately and swiftly. The last generation has seen technological change on a scale matching or exceeding that of the industrial revolution.[70] Three relatively recent major digital developments have affected our concept of privacy greatly. The first of which is the increase in data creation and the resulting collection of vast amounts of personal data—caused by the electronic recording of almost every transaction; secondly, the globalisation of the data market and the ability of anyone to collate and examine this data; and lastly the lack of control mechanisms for digital data which existed to protect analogue data.[71] These three developments all concern the changes wrought by digital technology on the ability to manipulate, store and disseminate information.[72] Every interaction with the Internet and with social networks, every credit card transaction, every bank withdrawal, and every magazine subscription is recorded digitally and linked to specific users.[73] All of this information, once it is collected in networked databases, can be sent instantly and cheaply around the globe.[74] Individuals have little ability to control this collection or manipulation of their data. Most people are not even aware of what information has been collected about them or for what purpose it is being used.[75]

While all of these changes affect information, not only informational privacy has been affected, autonomy is also imperilled from the interference with one's daily life by digital technology and the Internet.[76] When almost every activity leaves a digital trail, government and private monitoring become less about analogue surveillance or human intelligence gathering and more a matter of "data mining," defined as: 'the intelligent search for new knowledge in existing masses of data.'[77] Additionally, when the Internet stores and makes available all types of information previously collected and without any type of filter, individuals' privacy is inevitably affected. The well-documented problem with the current state of privacy law is that it does not factor new advancements in technology or reflect societal and individual notions of privacy.[78]

---

[70] See Quinn, Jr., E. R., "Tax Implications for Electronic Commerce over the Internet", *Journal of Technology Law and Policy*, vol. 4, ed. 3, 1999.

[71] Berman, J., and Mulligan, D., "Privacy in a Digital Age: Work in Progress" *Nova Law Review*, vol. 23, 1998, 551–582, 553–54.

[72] Froomkin, A. M., "The Death of Privacy?", *Stanford Law Review*, vol. 52, no. 5, 2000, 1461–1543, 1462.

[73] As compared to old-fashioned cash commerce today's "e-commerce" allows merchants to track your "clickstream" through the use of "cookies," and are able to track your interests based on what you view as well as your purchase, while credit companies are able to record your purchase. See United States Court for the Southern District of New York, *In re DoubleClick, Inc. Privacy Litigation*, 154 F. Supp. 2d 497, 501–05, SDNY (2001).

[74] Berman and Mulligan, *supra* nt. 71, 554.

[75] Solove, "Conceptualizing Privacy", *supra* nt. 31, 1095.

[76] See generally Cohen, J. E., "A Right to Read Anonymously: A Closer Look at "Copyright Management" in Cyberspace", *Connecticut Law Review*, vol. 28, 1996, 981–1039.

[77] See generally Fulda, J. S., "Data Mining and Privacy", *Albany Law Journal of Science and Technology*, vol. 11, 2000, 105–113. In this article, Fulda defines and discusses the concept of data mining. Data mining shows how difficult it is to fully determine the various breaches of privacy because the technology allows the collection and potential for misuse of such vast amounts of data.

[78] See Nissenbaum, H., *Privacy in Context: Technology, Policy, and the Integrity of Social Life*, Stanford University Press, Stanford, Palo Alto, 2010, 104–126; Solove, *Understanding Privacy*, *supra* nt. 37, 1–37; Nissenbaum, H., "Privacy as Contextual Integrity", *Washington Law Review*, vol. 79, ed. 1, 2004, 101–139, 119; Nissenbaum, H., "Protecting Privacy in an Information Age: The Problem of Privacy in Public", *Law and Philosophy*, vol. 17, ed. 5, 1998, 559–596; Solove, "Conceptualizing Privacy", *supra* nt.

The explosion in the availability and access to the Internet has made it one of the principal tools for communication, commerce and research. With the hyper development of new technologies and applications, the Internet is constantly evolving for ever more creative uses.[79] However, because of its relative youth in mass application, the Internet lacks many of the protections and control mechanisms utilised for systems like hard-wired telephony. Such things as the unauthorised collection and storage of information relating to Internet activities have emerged as significant threats to privacy on the Internet.[80] With each keystroke and page that is opened, database server's store and catalogue very precise information about the user and his or her use of the Internet. Many sites utilise what are commonly known as "cookies" which are placed on an Internet user's access device and facilitates detailed information about the user often without the user's knowledge or consent. Adding to the amount of personal data collected are the websites that require personal data before use and others that obtain information in connection with purchases, all of which are readily vulnerable to theft and abuse. Sites such as Google, Yahoo, Twitter, Facebook, and LinkedIn, accumulate personal data about users with alarming specificity. They are able to know such things as where individuals log on from, their use patterns and their personal and professional contact information. The collection and retention of this data is a source of great concern but has also been sought by governments and others for non-commercial purposes, such as hackers, businesses and simply the curious.

Social networks have had perhaps the greatest growth as well as the biggest impact on privacy because of the way they have affected how people interact on line. Today, there are some fourteen social media networks with over one hundred million registered users.[81] Most social networks share the common characteristic of 'visible profiles that display an articulated list of Friends who are also users of the system.'[82] As social networks have mushroomed, so has the amount of information and data that individuals are willing and able to post about themselves and others on these sites. Sites such as Facebook, MySpace, Google+, Instagram, etc., collect data on the interests of their users, their friends, and their preferences, for anything from travel information to the games they play. They also collect photographs, location, and many other pieces of information about the users using new technologies such as facial recognition technology. This information becomes the source of much concern from a privacy rights perspective

31; Strahilevitz, L. J., "A Social Networks Theory of Privacy", *University of Chicago Law Review*, vol. 72, 2005, 919–988.

79 Pikowsky, R. A., "Legal and Technological Issues Surrounding Privacy of Attorney Client Communications Via Email", *Advocate*, vol. 43, ed. 16, 2000.

80 See Simmons, R., "Technological Change and the Evolution of Criminal Law: Why 2007 is Not Like 1984: A Broader Perspective on Technology's Effect on Privacy and Fourth Amendment Jurisprudence", *Journal of Criminal Law and Criminology*, vol. 97, ed. 2, 2007, 531–568, 533. The author discusses the effect of technology on Fourth Amendment cases and argues for an appropriate balance between an individual's right to privacy and the government's interest in law enforcement. See Hornung, M. S., "Note Think Before You Type: A Look at Email Privacy in the Workplace", *Fordham Journal of Corporate and Financial L*aw, vol. 11, 2005, 115–159, 118.

81 *Facebook* 1+ billion, USA; *Tencent* 712 million, China; *Skype* 663 million, Denmark/Sweden; *Qzone* 536 million, China; *Twitter* 500+ million, USA; *Google*+ 400+ million, USA; *Windows Live* 330+ million, USA; *Sina Weibo* 368 million, China; *Tencent Weibo* 310 million, China; *Habbo* 273 million, Finland; *LinkedIn* 175+ million, USA; *Badoo* 162+ million, UK; *VK (VKontakte)* 140+ million, Russia; *Bebo* 117 million, USA. Wikipedia, *List of virtual communities with more than 100 million users*, available online at <en.wikipedia.org/wiki/List_of_virtual_communities_with_more_than_100_million_users> (accessed 4 November 2014).

82 *Ibid.*

because once the information is uploaded onto a social network, the site has broad latitude as to how long it can maintain the information, how to use the information, and for what purposes.[83]

In addition to identifying information that the users themselves disclose when they sign up for the service, such as their address, telephone number, date of birth, etc., the sites also collect information about the device that a user is using to access the site, track data about patterns of use of the service, record location information of the user when they access the site, and may collect other personal information stored in the user's computer using cookies and anonymous identifiers.[84] This ability to capture so much consumer information has not gone unnoticed and in some cases has led to a legal response from governments concerned about the privacy rights of their citizens.

In 2009, Germany passed amendments to the country's Federal Data Protection Act,[85] and has since then battled with United States (US) technology companies Apple, Facebook, and Google. The country launched investigations into how these companies collect and store personal data.[86] In one instance, German officials asked Google to turn over data from home wireless networks that were collected while the company compiled information for its Street View map.[87] German officials also questioned Apple about the duration and the type of personal information the company stores on its iPhone 4.[88] German data-protection officials launched legal proceedings in August 2010 because of how Facebook handles non-user information.[89] Facebook's social graph architecture allows any site to share information between the site and the Facebook platform, permitting readers of the German news magazine Spiegel Online[90] to see what stories their Facebook "friends" like, for example.[91] The Facebook privacy policy, however, suggests that Facebook receives an array of data when a user visits a website that connects to the Facebook Platform through such links as the "Like" button

---

83 Users grant Facebook, for example, 'a non-exclusive, transferable, sub-licensable, royalty-free, worldwide license to use any IP content that you post on or in connection with Facebook (IP License)…' limited only by Facebook privacy settings. Moreover, this "license" does not end upon deletion or closing on one's account. Facebook Statement of Rights and Responsibilities, available online at <facebook.com/legal/terms> (accessed 4 November 2014).

84 *Ibid.*

85 Bundesdatenschutzgesetz [BDSG] [Federal Data Protection Act], Germany, 1 January 2002, BGBl. I, last amended by Gesetz [G], 1 September 2009, BGBl. I.

86 Annual Activity Report 2009/2010 of the Federal Commissioner for Data Protection and Freedom of Information, 23 April 2010, available online at <bfdi.bund.de/SharedDocs/Publikationen/EN/AnnualReport/2009-2010.pdf?__blob=publicationFile> (accessed 1 December 2014). See also New York Times, O'Brien, K., *Despite Privacy Inquiries, Germans Flock to Google, Facebook and Apple*, 11 July 2010, at B8, available online at <http://www.nytimes.com/2010/07/12/technology/12disconnect.html?_r=0> (accessed 1 December 2014).

87 New York Times, O'Brien, K., *Google Balks at Turning Over Data to Regulators*, 27 May 2010, at B3, available online at <nytimes.com/2010/05/28/technology/28google.html> (accessed 4 November 2014).

88 *Ibid.*

89 Wall Street Journal, Lawton, C., and Fuhrmans, V., *Google Rouses Privacy Concerns in Germany—Mapping Service Sparks Debate as Nation Scarred by Authoritarian Past Grapples With Personal Data in Digital Age*,.17 August 2010, at B5.

90 An online magazine available online at <spiegel.de/international/> (accessed 4 November 2014).

91 In 2010, Facebook opened up its powerful platform, allowing any site in the world to connect to Facebook. The Guardian, Bell, E., Why *Facebook's Open Graph Idea Must Be Taken Seriously*, 26 April 2010, available online at <guardian.co.uk/media/pda/2010/apr/26/facebook-f8-emily-bell> (accessed 4 November 2014).

> We receive data whenever you visit a game, application, or website that uses Facebook Platform or visit a site with a Facebook feature (such as a social plug-in). This may include the date and time you visit the site; the web address, or URL, you're on; technical information about the IP address, browser and the operating system you use; and, if you are logged in to Facebook, your User ID.[92]

In early 2014, the District Court of Berlin ruled that Facebook has to comply with German data protection law. The Berlin court confirmed a 2012 verdict that found that Facebook's "Friend Finder" violated German law because it was unclear to users that they imported their entire address book into the social network when using it. The court also confirmed that several clauses of Facebook's privacy policy and terms of service violate German law.[93]

France has also seen legal battles involving the likes of social media. In *Hervé G. v. Facebook France*, the Paris Court of First Instance considered a claim brought by French Bishop Hervé Giraud of Soissons against Facebook.[94] Bishop Hervé Giraud of Soissons claimed that a Facebook page titled "Courir nu dans une église en poursuivant l'évêque" (running naked in a church after the bishop) incited hate and violence against Catholics and, thus, violated the French hate speech codes.[95] He also claimed that his photograph was used without his permission.[96] The French court ruled in the bishop's favour on both grounds.[97] Even though the photograph at issue was not at all scandalous, but rather simply a portrait of the bishop,[98] the French court ordered Facebook to remove the page, and to pay 2,000 Euros in damages, with a penalty for every day the page remained up.[99]

In the United States, many courts have attempted to define what the reasonable expectation of privacy in the context of the Internet is, with little success.[100] The case of *Lane v. Facebook*,[101] shows how easy it is for social network sites to have access and share user's information that should remain private. In 2007 Facebook launched the Beacon program where user records were released on the public for friends to see. Mr. Sean Lane bought a diamond ring from overstock.com, and it showed up on his news feed, which was visible to his wife. Along with other plaintiffs, Lane filed a class action suit against Facebook complaining that the Beacon program was causing publication of otherwise private information about their outside web activities to their personal profiles without their knowledge or approval. The parties eventually settled for USD9.5 million in damages, and Facebook ended the Beacon program.

---

92 Data Use Policy, Facebook, available online at <facebook.com/full_data_use_ policy> (accessed 4 November 2014).

93 District Court of Berlin, *In Re: Facebook*, 5 U 42/1216 0 551/10, 24 January 2014.

94 TGI Paris, 13 April 2010, *Hervé G. v. Facebook France@*.

95 *Ibid.*

96 *Ibid.*

97 *Ibid.*

98 La Vie, Bataille, J., *Condamné pour Outrage à un Évêque, Facebook Gagne en Appel*, 1 November 2011, available online at <lavie.fr/actualite/france/condamne-pour-outrage-a-un-eveque-facebook-gagne-en-appel-11-01-2011-13046_4.php> (providing an image of the Facebook page) (accessed 4 November 2014).

99 *Ibid.*

100 Solove, D. J., "Fourth Amendment Pragmatism", *Boston College Law Review*, vol. 51, 2010, 1511–12. The author explains that '[t]he reasonable expectation of privacy test has led to a contentious jurisprudence that is riddled with inconsistency and incoherence. Debates rage over whether particular government information activities invade "privacy"'.

101 US Court of Appeals 9th Circuit, *Lane v. Facebook Inc.,* 2012, 696 F.3d 811.

The case of *New York v. Harris* shows the difficulty in determining where the line lies between the private and the public in online communications. The case began in 2011 in the context of the "Occupy Wall Street" movement. After being arrested and charged with disorderly conduct during a particular march across the Brooklyn Bridge, Mr. Harris pled "not guilty" and claimed New York police led protesters on to the Brooklyn Bridge in order to make it easier to arrest them. The Prosecutor subpoenaed Mr. Harris' tweets saying they would reveal that he was "well aware of police instructions" ordering protesters not to block traffic. The New York City District Attorney's Office requested Twitter to turn over reams of information, including the content Harris's of tweets, IP addresses from where he accessed Twitter, and any email addresses it had on file. Harris contested the subpoena alleging that: '[T]he tweets are protected by the Fourth Amendment because the government admits that it cannot publicly access them, thus establishing that the defendant maintains a reasonable expectation of privacy in his communications…' However, the court ruled that Harris did not have legal standing to challenge it because the information—including all of his tweets—belonged to Twitter. The Judge stated

> If you post a tweet, just like if you scream it out the window, there is no reasonable expectation of privacy. There is no proprietary interest in your tweets, which you have now gifted to the world. This is not the same as a private e-mail, a private direct message, a private chat, or any of the other readily available ways to have a private conversation via the Internet that now exist. Those private dialogues would require a warrant based on probable cause in order to access the relevant information.[102]

The Court's decision allowed the government to obtain the content of communication—tweets—with simply a subpoena, and not a search warrant as required by the Fourth Amendment and the Stored Communications Act. Twitter was also ordered to give the keys to location information—IP addresses that could be used to determine where a person is when he logs into Twitter—without a search warrant. On September 13, Twitter turned the requested information over to the judge.

In the case of *Romano v. Steelcase*, another court in the State of New York held that information posted on the Plaintiff's MySpace page was public.[103] Kathleen Romano brought an action against Steelcase Inc. claiming that the defendant permanently injured her so severely that she was confined to misery and home. For the trial the defendant sought to introduce portions of Romano's Facebook and MySpace sites that showed her looking happy, traveling and portraying a lifestyle inconsistent with her litigation claims to the contrary. Defense counsel asked Romano about her Facebook and MySpace data, and sought not only the live private pages but also deleted pages. Romano refused, and the defendant pursued. The court found no reasonable expectation of privacy in social network sites and allowed disclosure information stating that:

When Plaintiff created her Facebook and MySpace accounts, she consented to the fact that her personal information would be shared with others, notwithstanding her privacy settings. Indeed, that is the very nature and purpose of these social networking sites else they would cease to exist. Since Plaintiff knew that her information may become publicly available, she cannot now claim that she had a reasonable expectation of privacy. [104]

---

[102] *Ibid*.
[103] New York Supreme Court, 2010, *Romano v. Steelcase, Inc.,* 907 N.Y.S.2d 650.
[104] *Id.,* 657.

The United States Supreme Court has been hesitant to issue definitive rulings about Fourth Amendment expectations of privacy pertaining to new technology in an apparent acknowledgement of the difficulty in determining where the public sphere ends the private sphere begins.[105] Cases involving privacy issues and new technologies raise questions about the private/public dichotomy in the context of current laws addressing privacy. Given that Twitter has a feature that allows a user to block a follower, does that feature give the user a sense of control over his messages regarding who has access to them? Are messages posted on Twitter "gifted to the world", or are those messages more like emails, and would require the government to obtain a warrant to have access to them? Is anything published in a MySpace or FaceBook "wall/page" public? What about posts that have been deleted?

In the context of information accessed through a search engine and consequently made available via the Internet through such means, a recent decision from the European Court of Human Rights judicially recognised the "right to be forgotten".[106] This "right" is little more than a long held feeling that an individual should have the ability to remove information from the internet at some point in time based on such reasons as it being incorrect, being unfairly placed on the internet, or simply being having occurred long ago and no longer relevant. The "right to be forgotten" was enshrined in the in the 1995 European Data Protection Directive (Directive 95/46 EC). Under Article 12 of the Directive private citizens in the EU were permitted to request removal of information from the Internet, however, only recently has the Court provided guidelines for the application of such right.

The case began in 2010 when a Spanish citizen presented a complaint against a Spanish newspaper and Google with the Data Protection Agency of Spain. Mr. Costeja alleged that a notice of auction in connection with a bankruptcy notice that appeared in Google's search results violated his right to privacy because the matter to which the notice related had been completely resolved for several years and was no longer relevant. He initially asked the Court to order that the newspaper either delete the information or change the pages at issue so that the personal data would cease to appear online, and also that Google Spain or Google Incorporated not make the information relating to him available through searches with his name.

The Spanish Audiencia Nacional decided to stay the proceedings and to refer the case to the Court of Justice of the European Union. The Grand Chamber found that

> a) Even in cases where the actual server is located outside of the EU, the laws and Directives of the EU are applicable to search engine providers if they maintain a physical presence in any Member State and carry out business intended toward garnering revenue within the EU;
>
> b) Search engines should be considered "controllers" of personal data. That by search engines qualify by "…exploring the internet automatically, constantly and systematically in search of the information which is published there, the operator of a search engine 'collects' such data which it

[105] See US Supreme Court, 17 June 2010, *City of Ontario v. Quon*, 130 S.Ct. 2619, where the Court found that changes in technology made it difficult to determine reasonable expectations of privacy and declined to issue a ruling about employee privacy expectations when using employer-provided communication devices.

[106] European Court of Justice, Grand Chamber, 13 May 2014, *Google Spain v. AEPD and Mario Costeja Gonzalez*, C-131/12.

> subsequently 'retrieves', 'records' and 'organises' within the framework of its indexing programmes, 'stores' on its servers and, as the case may be, 'discloses' and 'makes available' to its users in the form of lists of search results." As such the right to be forgotten as enshrined in 95/46 EC also applies to them.
>
> c) The Court concluded that the Right to be Forgotten arises not only in cases where the data is inaccurate but also in cases where the information is inadequate, irrelevant or excessive in relation to the purposes of the processing, in cases that the information is not kept up to date, or in cases where the information is kept for longer than is necessary unless they are required to be kept for historical, statistical or scientific purposes.

The European Court also stated that the right to be forgotten is not without limits and must be balanced against 'the legitimate interest of internet users potentially interested in having access to that information…'.[107] Interestingly, the Court made explicit that the party requesting removal need not establish 'that the inclusion of the information in question in the list of results causes prejudice to the data subject.'[108] The issuance of this ruling clarifies that the "right to be forgotten" is more than an aspirational right as may have been previously thought given its existence in the Directive 95/46 since 1995.

Current cases on privacy issues illustrate that in the current technological landscape it is virtually impossible to clearly differentiate the private from the public. The law seems to always be playing catch-up to technology that develops faster than the legal frameworks to regulate it. The impact of digital technology on privacy appears to follow the same pattern seen with older technologies, and one can foresee that the law will attempt to evolve in response to the privacy threats posed by the digital revolution.[109] However, the impact of the digital age is so deep and pervasive that expansion of a single area of privacy law is unlikely to adequately address all of the problems.[110] The response to the effect of new technologies on our concept of privacy has usually been greater governmental regulation.[111] However, greater regulation might not adequately address

---

[107] European Court of Justice, Grand Chamber, 13 May 2014, *Google Spain v. AEPD and Mario Costeja Gonzalez*, C-131/12

[108] *Ibid*.

[109] Cohen, J.E., "Examined Lives: Informational Privacy and the Subject as Object", *Stanford Law Review*, vol. 52, 2000, 1374.

[110] Challis, W.S., and Cavoukian, A., "The Case of a U.S. Privacy Commissioner: a Canadian Commissioner's Perspective", *The John Marshall Journal of Computer and Information Law*, vol. 19, 2000, 1. The author argues that the current regulatory system with regards to new technologies and their effect on privacy is insufficient. He makes the case for the creation of a specialised agency headed by a US Privacy Commissioner with the responsibility of establishing fair information practices and standards in the context of businesses and technologies.

[111] For examples of state regulation initiatives see: Directive 95/46/EC of the European Parliament and 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, 1995 OJ (L281/33), available online at <europa.eu/legislation_summaries/information_society/l14012_en.htm> (accessed 4 November 2014); Freedom of Information Act, United States of America, 5 USC Section 552 (2000), available online at <usdoj.gov/oip/foia_updates/Vol_XVII_4/page2.htm> (accessed 4 November 2014); Right to Financial Privacy Act, United States of America, 12 USC Section 3412 (2000), available online at <law.cornell.edu/uscode/text/12/3412> (accessed 4 November 2014); Privacy Protection Act, United States of America, 42 USC Section 2000 (2000), available online at <law.cornell.edu/uscode/42/2000aa.html> (accessed 4 November 2014); Employee Polygraph Protection Act, United States of America, 29 USCS Sections 2001 *et seq.* (2000), available online at

privacy violations on the part of governments and private parties that utilise the latest technologies. The demands of protecting the right to privacy in Cyberspace must take into account the easiness of access to personal information available online to virtually anyone with a computer, as well as the technological advancements that can facilitate protection. A problem-based approach seems to be the most appropriate approach to arrive at a feasible solution that addresses privacy concerns in Cyberspace. The concept of Obscurity in Cyberspace has been advanced as a way to provide effective and effective remedies to protect the right to privacy in the Internet.[112]

IV. The Right to Obscurity in Cyberspace

The concept of privacy includes the idea that even though human interactions might often take place in public spaces, individuals rely on a zone of privacy that is not open and accessible to others unless the owner agrees to share that space. Given the difficulties in defining an individual's actual zone of privacy, and in trying to design the appropriate safeguards to protect it, especially in the context of Cyberspace, it has been argued that "obscurity" is a more desirable goal.[113] Obscurity is defined as the state of unknowing or being unidentifiable online.[114] An individual is obscure when a casual observer does not possess sufficient information about an individual to decipher the fragments of data about that person that might be accessible in Cyberspace. For example, if two individuals are having a conversation in a restaurant, the casual observer, who has not been previously acquainted with them, and is not eavesdropping, does not possess sufficient information to readily identify the individuals or determine the content of their conversation. In the context of Cyberspace, an individual is obscure when critical information such as identity, social connections, and other personal information is not readily available or decipherable by others.[115] Online obscurity has been defined as information that 'exists in a context missing one or more key factors that are essential to discovery or comprehension.'[116]

<law.cornell.edu/uscode/29/usc_sup_01_29_10_22.html> (accessed 4 November 2014); Cable Communications Policy Act, United States of America, 47 USC Section 551(h) (2000) , available online at <law.cornell.edu/uscode/html/uscode47/usc_sec_47_00000551----000-.html> (accessed 4 November 2014); Financial Services Modernization Act, United States of America, Pub. L. No. 106-102, 113 Stat. 1338 (1999), available online at <gpo.gov/fdsys/pkg/PLAW-106publ102/content-detail.html> (accessed 4 November 2014); The Children's Online Privacy Protection, United States of America, 15 USC Sections 6501–6506 (1999), available online at <law.cornell.edu/uscode/html/uscode15/usc_sup_01_15_10_91.html> (accessed 4 November 2014); Personal Information Protection and Electronic Documents Act, Canada, S.C. ch. V (2000) (assented to Apr. 13, 2000), available online at <priv.gc.ca/information/guide_e.pdf> (accessed 4 November 2014); The Australian Privacy Commission, Australia's Privacy Amendment (Bill 2000), Australia, available online at <privacy.gov.au/law/act> (accessed 4 November 2014).

[112] Hartzog. W., and Stutzman, F., "The Case for Online Obscurity", *California Law Review*, vol. 101, 2013, 1–52.

[113] Hartzog, W. and Stutzman, F., "Obscurity by Design", *Washington Law Review,* vol. 88, ed. 2, 2013, 385. The authors juxtapose "privacy by design" as a universal approach to privacy which poses a set of significant challenges for implementers with "obscurity by design" as the optimal protection for most online social interactions. The authors propose that information in cyberspace can be plotted on a spectrum of obscurity that would allow regulators, designers, and organisational stakeholders to adopt guiding principles regarding the protection of online information.

[114] Hartzog and Stutzman, "The Case for Online Obscurity", *supra* nt. 112, 5.

[115] *Ibid.*

[116] *Id.*, 35.

The intrinsic need to keep certain areas of our lives private is evident when one looks at the actual content of the Internet. It has been estimated that 80-99 percent of the World Wide Web is completely hidden from general-purpose search engines and only accessible by those with the right search terms, URL, or insider knowledge.[117] Other pieces of online information are obfuscated by the use of pseudonyms, multiple profiles, privacy settings, or encryption.[118] The constant effort made by many to keep certain information obscure from the casual Internet user shows the need for humans to maintain a sphere of privacy. On the Internet, information that is obscure has very little chance of being understood by unintended recipients. Consequently, although a user might choose to make some information public, they also want the prerogative to limit the recipients of certain information that he/she might wish to remain private. Such user control provides adequate protection from online privacy infringement.

Obscurity can be achieved by the creation of design-based solutions for new technologies that would benefit from increased attention to user interaction, with a focus on the principles of "obscurity" rather than the expansive and vague concept of "privacy".[119] Obscurity in cyberspace, in part, is achieved by requiring the protection of access to identifying information related to users. Access protection covers a variety of technology and methods to manage access to content.[120] Obscurity can also be achieved through regulation that protects an individual's information mandating that information that a user wishes to remain private be kept secure and unidentifiable. To the extent that a fundamental right to privacy has been internationally recognised, and given that the Internet has become an extension of our social sphere, it can be argued that a right to "obscurity" in Cyberspace is an indispensable corollary to the right to privacy. Hartzog and Stutzman have made a good case for Online Obscurity and Obscurity by Design as alternatives to creating other frameworks for privacy protection on the Internet.[121] They have convincingly argued that the "right to obscurity" in Cyberspace should be easier to implement than the difficult to define right to privacy and the behaviours that might constitute breach of the right to privacy in Cyberspace. Obscurity could serve as a compromise protective remedy: instead of forcing websites to remove sensitive information, courts could mandate some form of obscurity.[122] Internet "companies"

---

[117] 'Since they are missing the deep Web when they use such search engines, Internet searchers are therefore searching only 0.03%—orone in 3,000—of the pages available to them today', Bergman, M. K., "The Deep Web: Surfacing Hidden Value", *The Journal of Electronic Publishing*, vol. 7, ed. 1, 2001, available online at <quod.lib.umich.edu/cgi/t/text/textidx?c=jep;view=text;rgn=main;idno=3336451.0007.104> (accessed 27 October 2014); Medeiros, N., "Reap What You Sow: Harvesting the Deep Web", *OCLC Systems and Services*, vol. 18, ed. 1, 2002, 18–20.

[118] 'Most people believe that security through obscurity will serve as a functional barrier online. For the most part, this is a reasonable assumption.', Boyd, D., "Why Youth Heart Social Network Sites: The Role of Networked Publics in Teenage Social Life", *in:* Buckingham, D., ed., *MacArthur Foundation Series on Digital Learning – Youth, Identity, and Digital Media Volume*, MIT Press, Cambridge, 2007, 16; 'People also have a sense that their social-network information will be kept private because they feel anonymous amidst the millions of social-network users.', Keats Citron, D., "Fulfilling Government 2.0's Promise with Robust Privacy Protections", *George Washington Law Review,* vol. 78, ed. 4, 2010, 835; Gelman, L. A., "Privacy, Free Speech, and "Blurry-Edged" Social Networks", *Boston College Law Review*, vol. 50, ed. 5, 2009, 1317–18; Grimmelmann, J., "Saving Facebook", *Iowa Law Review,* vol. 94, ed. 4, 2009, 1160–63.

[119] Hartzog and Stutzman, "The Case for Online Obscurity", *supra* nt. 112.

[120] *Id.*, 37–38.

[121] Hartzog and Stutzman, "The Case for Online Obscurity", *supra* nt. 112; Hartzog and Stutzman, "Obscurity by Design", *supra* nt. 113.

[122] Hartzog and Stutzman, "The Case for Online Obscurity", *supra* nt. 112, 3.

bound by a "duty to maintain obscurity" would be allowed to further disclose information online, so long as they kept the information generally as obscure as the form in which they received it.[123] Finally, obscurity could replace confidentiality as a term in some contracts, particularly those involving the Internet.

Similarly, the right to obscurity in Cyberspace, requiring certain providers to allow for users to keep their information obscure, and allowing greater certainty for courts and administrative bodies in determining what information should be considered private would be beneficial for all. There are four factors which when found diminish obscurity (and their absence enhances it) and that could be used by judges and others to determine whether certain information on the Internet is private or public, these are: (1) search visibility, (2) unprotected access, (3) identification, and (4) clarity.[124] Having clear guidelines as to what constitutes private versus public information from a legal standpoint would benefit users by providing some degree of clarity and expectation regarding what information about them is considered to be legally private. Likewise, courts would have a uniform framework to establish privacy protections in Cyberspace. When a judge is faced with a situation where the sphere of privacy must be determined, looking at the above factors can facilitate a determination on whether the information should be considered to be public or private. These factors can also be applied uniformly to provide standard guidelines that may be universally adopted to protect privacy online.

The right to obscurity should also place the burden on service providers and technology manufacturers to create technology that provides users with the possibility to maintain the obscurity of certain information if they choose to do so. These guidelines should take into account the available tools for users to indicate their intentions regarding the information that they want to keep private. The four factors should become guidelines for the manufacturing of appropriate technology as well as the necessary regulation to achieve such ends.

Whether the right to obscurity is an extension of the right to privacy is an argument based on the importance that individuals place on privacy, the acknowledged legal recognition of a right to privacy in the international context, the need to adapt our concept of privacy to new technologies, and the lack of current legal guidelines that provide appropriate safeguards to protect users from privacy infringements on the internet. The right to privacy as an abstract concept is insufficient to protect individuals' privacy given the technology available to infringe it. However, if the right to privacy is an internationally recognised right, the right to obscurity might serve to give substance to the right for individuals who are concerned about the effect of current communications on their privacy. Additionally, using the four factors to determine whether certain information was meant to remain obscure online, courts should be able to identify a clear line that divides the private from the public eliminating the current confusion regarding the right to privacy online.

V. Conclusion

The concept of privacy has been discussed for centuries by philosophers, anthropologists, sociologists, and legal scholars. The importance that individuals place on privacy is beyond question and transcends geographical, cultural and racial boundaries. Individuals' need for secrecy and private space is so fundamental to forging relationships

---

[123] *Ibid*.

[124] Hartzog and Stutzman, "Obscurity by Design", *supra* nt. 113, 397.

with others and to preserving our sense of self, that a society with a complete lack of individual privacy would be unimaginable. Given that a desire for privacy is a fundamental human characteristic, the idea of a right to privacy follows from our ingrained need for a life of dignity.

At the international level there is evidence of an existing appreciation for the existence of some universal basic principles that merit international legal protection. The concept of a human right can be described as a claim of a higher order than other legal relationships, such as contractual rights or statutory entitlements.[125] Today, the right to privacy has been recognised as a '…[f]undamental human 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.'[126] The argument that the right to privacy has risen to the level of international law can be made and is bolstered by the inclusion of the right in numerous international and regional human rights treaties and its recognition as customary international law. Although the right to privacy is not an absolute right, and must be balanced against state interests, the notion of necessity implies that the interference corresponds to a pressing social need and that it is proportionate to the legitimate aim pursued.[127]

The importance that the right to privacy has for individuals is evidenced in the manner in which the right continues to expand and evolves to adapt to society's needs. The legal definition as well as the contours of what the individual right to privacy encompasses is still and will continue developing as society advances and as technology provides new ways in which individual privacy is affected. The advent of new technologies capable of easily infringing our private affairs has forced us to recognise the pressing need to establish with clarity what level of protection we can expect from governments with respect to our right to privacy. The technologies and ease of communication in today's world have helped individuals recognise that the concept of privacy is more than an abstract notion, and that we must actively seek its protection in order to enjoy the type of freedom that society strives to reach.

Technology brings about innovation and progress for civilisation, but it also brings the potential to harm society and the principles we cherish as individuals. Privacy becomes more of a concern in response to events and advancements that facilitate its infringement. As technology has made the collection, distribution, and transfer of information faster and more efficient, the legal protections available for private personal data have become a necessity. The main problem with establishing a workable framework to determine what is private versus public information on the Internet is that the new communication systems and technologies breach the barrier of what used to be recognisable as private. As technology advances it becomes easier to access individuals' personal information without much effort or training, merely by pressing a button on a computer terminal.

---

[125] Dworkin, R., *Taking Rights Seriously,* Harvard University Press, Cambridge, 1977.

[126] United Nations Human Rights Council, Scheinin, M., *Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism*, 28 December 2009, available online at <ohchr.org/english/bodies/hrcouncil/docs/13session/A-HRC-13-37.pdf> (accessed 27 October 2014).

[127] In *Olson v. Sweden*, the Court stated that, 'the notion of necessity implies that the interference corresponds to a pressing social need and, in particular, that it is proportionate to the legitimate aim pursued; in determining whether an interference is "necessary in a democratic society", the Court will take into account that a margin of appreciation is left to the Contracting States'. European Court of Human Rights, *Olson v. Sweden,* 24 March 1988, 11 EHRR 259, para. 67.

Today that data protection appears to be at the forefront of privacy concerns, people are worried about losing their privacy and governments are responding to people's demand for privacy by enacting laws that protect privacy in this digital era. However, the current legal framework of privacy protection in the context of online technologies is unclear and insufficient to deal with the current technology in this area, with its potential to infringe on privacy rights. Fortunately, while there is technology available capable of infringing on online privacy, there is also technology available to help users to keep their digital information private.[128] Perhaps the answer is to require that online users be allowed to decide what information they desire to keep public and what information they want to make public.

The concept of obscurity provides a potential bedrock for protecting privacy in Cyberspace. The proposition that there might be a developing right to obscurity in Cyberspace is related to the fundamental need "to be left alone" even in the context of online communications. As a legal concept it may go hand in hand with the recognition of the sanctity of an individual's right to privacy. In the quest for real and verifiable measures that guarantee a level of protection to safeguard privacy in the digital age, obscurity may be an indispensable part of reaching that goal. While the concept of privacy might be difficult to define, the concept of obscurity and the four factors that determine whether information is obscure, might facilitate the creation of standard legal guidelines to make the distinction between public and private and thereby offer real protection for privacy rights in the context of online communications. Society must find a way to adapt to new developments in order to preserve its values and its humanity. It is difficult to predict, or even to imagine future technologies, but positive strides are being made in the recognition that the protection of privacy is everyone's concern and everyone should be involved in protecting the human values it represents.

*

[128] See, e.g., PrivacyFix, which is a programme that helps set up a user's privacy settings on Facebook and Google, and control cookie activity. PrivacyFix is available online at <privacyfix.com/start> (accessed 27 October 2014); See (reviewing and explaining the benefits of Privacy), Fix: Cnet, Whitney, L., *Privacy Fix helps protect your privacy on the Web,* 10 October 2012, available online at <news.cnet.com/8301-1009_3-57529655-83/privacyfix-helps-protect-your-privacy-on-the-web/> (accessed 27 October 2014).