Chapter 19
Privacy Protection on the Internet: Risk Management and Networked Normativity

Pierre Trudel

19.1 Introduction

In cyberspace's present form, particularly with respect to Web 2.0 applications, the conditions in which personal information circulates have changed. The Internet is now encompassing almost all aspects of social life. Yves Poullet observes that the Internet promotes dual globalisation: first, with respect to the international aspect of networks and their convergence and, second, with respect to the fact that all activities are transformed into digital information.[1]

Given such globalisation,[2] simple exegesis of state law will not suffice to describe the legal framework protecting privacy in cyberspace. Despite the global nature of the network, assessments and values are different in the various cultural milieus in which rules apply.[3] Some phenomena modulate accepted norms and prevent their application across the network. Such phenomena prevent application of rules that could be taken out of context with respect to the situation or cultural substrate in which they apply. One such phenomenon seems to be legal risk: stakeholders' assessment of the concrete possibility that a statute or other rule will be applied to their activities explains why, though the Internet is a global network, no one feels complied to obey all pieces of national legislation that could in theory apply.[4]

Philippe Amblard notes that a characteristic of Internet regulation is that the normative process is multifaceted, which tends to promote the social effectiveness of

P. Trudel (✉)
Faculty of Law, Centre de recherche en droit public, Université de Montréal, Montreal, QC, Canada
e-mail: pierre.trudel@umontreal.ca

[1] Yves Poullet, 'Mieux sensibiliser les personnes concernées, les rendre acteurs de leur propre protection,' [2005] 5 *Revue Lamy Droit de l'immatériel*, 47, note 66.

[2] Here, the word is used to refer to the growing interconnection of economies and societies resulting from the development of information technologies. Cynthia Ghorra-Gobin, *Dictionnaire des mondialisations*, (Paris: Armand Colin, 2006), p. 185.

[3] Jack Goldsmith and Tim Wu, *Who Controls the Internet? Illusions of a Borderless World*, (New York: Oxford University Press, 2006), Chapter 9, 'Consequences of Borders.'

[4] For a legal risk analysis methodology, see Franck Verdun, *La gestion des risques juridiques*, (Paris: Éditions d'organisation, 2006), pp. 39 ff.

S. Gutwirth et al. (eds.), *Reinventing Data Protection?*

DOI 10.1007/978-1-4020-9498-9_19,

living law in contrast with 'the positivist artificiality of state law.'[5] After describing various models of Internet regulation, Michel Vivant observes that 'it is indeed of regulations, in the plural, that we should speak, of forms of regulation that should be identified so as to combine them effectively.'[6]

According to a number of theorists, we need to speak of multi-regulation and of co-existence on the network of different types of regulation with different purposes and different methods but equal legitimacy.[7] Regulation of activities occurring on the Internet can be seen as a kind of network. Thomas Schultz notes that cyberspace is an interesting laboratory for contemporary legal phenomena.[8] Privacy regulation has to be examined with a view to the flows of normativity that underlie the law that is in fact applied in cyberspace.

Seen from the point of view of a network, privacy protection on the Internet can be expressed as active normativity resulting from risk management decisions made by regulators and stakeholders. In other words, on the Internet, users and other stakeholders manage risk. Through stakeholders' decisions and behaviour, norms created in nodes generate risks that are spread to stakeholders' counterparts and partners. Sources of norms cannot claim sovereignty over cyberspace but they have complete power to establish rules that generate risks for stakeholders.

The scope and effectiveness of privacy protection on the Internet result from risk management decisions. Users and other stakeholders have to decide whether they accept risks to privacy and how they will transfer them, if applicable. Governments can take measures to increase or limit risks facing cybernauts under their jurisdiction. However, for stakeholders on the Internet, government legislation appears as yet another risk to be managed. Legislation and other norms, such as technical standards, can both increase and decrease risks to stakeholders' privacy and other interests.

19.2 Privacy on the Internet

The Internet is a theatre of many situations in which invasion of privacy can occur.[9] Privacy has to be protected in accordance with users' legitimate expectations while at the same time we have to take into account the fact that users are necessarily

---

[5] Philippe Amblard, *Régulation de l'Internet l'élaboration des règles de conduite par le dialogue internormatif*, (Brussels: Bruylant, 2004), No. 80 [our translation].

[6] Michel Vivant, 'Internet et modes de régulation,' in Étienne Montero, *Internet face au droit*, (Brussels: Story Scientia, 1997), 215, p. 229 [our translation].

[7] Thomas Schultz, *Réguler le commerce électronique par la résolution des litiges en ligne*, (Brussels: Brulant, 2005), p. 162. Schultz reports on the points of views of the Mission interministérielle français sur l'Internet and the French Conseil supérieur de l'audiovisuel. He describes the findings of Marc Maesschalck and Tom Dedeurwaerdere, 'Autorégulation, éthique procédurale et gouvernance de la société de l'information,' in Jacques Berleur Christophe Lazaro and Robert Queck, *Gouvernance de la société de l'information*, (Brussels: Bruylant- Presses Universitaires de Namur, 2002), 77–103.

[8] Thomas Schultz, 'La régulation en réseau du cyberspace,' [2005] 55 *R.I.E.J.*, 31, p. 32.

[9] Paul M. Schwartz, 'Internet Privacy and the State,' [2000] 32 *Connecticut L. Rev*., 815–947; Fred H. Cate, 'Principles of Internet Privacy,' [2000] 32 *Connecticut L. Rev*., 877–896.

involved to various degrees in public life and therefore engage in activities that concern other people. Like the physical environment, cyberspace has both public and private spheres and legitimate expectations of privacy should therefore vary depending on the context.

Police surveillance is often referred to as a possible threat to privacy on the Internet. Yet, in all countries with privacy legislation, the forces of law and order have powers authorizing them to obtain information likely to prevent or solve crimes. Thus, privacy protection with respect to possible abuses by the police is not an issue specific to cyberspace. Certainly, the accumulation and persistency of information on the Internet make it possible to create directories that could be made available to the police. This is one of the web's risks. However, the police's right to exact such information is essentially a problem that has to be solved by regulating the police not the Internet.

Some Internet interactions are public while others presuppose privacy. In order to establish protection that balances all basic rights, we have to take into account the fact that public and private situations lie along a continuum. In cyberspace, nothing is purely public or strictly private, just as nothing is completely black or white. The degree to which a situation is public or private varies according to the context and circumstances. This is how we have to approach the right to privacy. However, the approach flowing from personal data protection law is far from sufficiently shaded to ensure the balance that has to be maintained between the public and private spheres.

19.2.1 Personal Data Protection

Privacy protection on the Internet is often confused with personal data protection law. Nicola Lugaresi notes that 'protection of privacy is often adjusted to meet the needs of personal data protection.'[10] Certainly, personal data protection law is a facet of privacy protection[11] but privacy has many hues and covers both more and less than the notion of personal data.

The all-encompassing nature of the notion of personal data has its origin in a need for a simple definition of information about people that should be protected. In order to circumvent problems involved in teasing out what has to remain secret in order to respect the right to privacy, a notion was chosen that conflates 'information that identifies an individual' with 'information about an individual's private life' and personal data protection law has been structured around the principle that the whole set is confidential. This has resulted from a desire to get around the difficulties flowing from the contextual nature of privacy. While it is clear that some data concerning individuals is private, it is also clear that not all is. Apparently in

---

[10] Nicola Lugaresi, 'Principles and Regulations about Online Privacy: 'Implementaion Divide' and Misunderstanding in the European Union,' TPRC 2002 Working Paper No. 42, online at: < http://papers.ssrn.com/sol3/papers.cfm?abstract_id=333440 >

[11] Raymond Doray, 'Le respect de la vie privée et la protection des renseignements personnels dans un contexte de commerce électronique,' in Vincent Gautrais, Ed., *Droit du commerce électronique*, (Montréal: Éditions Thémis, 2002), p. 303–361.

the quest for standards guaranteeing fair[12] personal data collection and processing practices, the nuances that had until then described the concept of privacy were left behind and instead measures were adopted that prohibit the circulation of any data on individuals. This slide has obscured the fact that the right to privacy is not the only right relating to the Internet. It has to be weighed against other rights and freedoms.[13]

It is well-known that public figures have less privacy than other people. Public figures are people who, through their own free will or owing to special circumstances, participate in activities that take place in public or who seek to win public trust or attention. Such figures include government representatives, artists, athletes, leaders of organizations and professionals who intervene in the public space. Though it is essential to democracy, this distinction is often ignored in application of personal data protection laws.

For example, if one participates in a public sports competition, it is supposed that one agrees to comply with the rules. Information relevant to ensuring the probity of sports competitions should be public. Unfortunately, strict application of some principles of personal data protection law tends to favour a conception of privacy that leaves little room for transparency and accountability. For example, in an opinion rendered in June 2005, the CNIL criticized the publication of a directory of over 1000 racing cyclists who had admitted to or tested positive for doping.[14]

The case of a list of notaries published on the Internet is another illustration of the excessiveness of some applications of personal data protection law. A blacklist of notaries was published but the targeted notaries were not given the opportunity to object to publication of their names and addresses. This was found to contravene the French statute on data protection. In a January 11, 2007 decision, the Bourges Court of Appeal upheld the criminal court of Bourges' July 5, 2006 conviction of the European Defence League for the Victims of Public Notaries. The League, which has now been disbanded, had authorized its Secretary-General to create and publish a web site on its behalf. The site was critical of some notaries and on the home page it said that the profession of a public notary 'puts clients at great risk.' This statement was accompanied by a list of 2500 notaries and a note to the effect that 'the fact of appearing in the European Defence League for the Victims of Public Notaries' list implies no prejudice or pre-judgment. It simply means that the League has a file concerning one or more of the notary's clients.' Some public notaries who objected to having their competency and honesty questioned wrote to the site to have

---

[12] Joel R. Reidenberg, 'Setting Standards for Fair Information Practice in the U.S. Private Sector,' [1995] 80 *Iowa L. Rev*., 497; Spiros Simitis, 'Reviewing Privacy in an Information Society,' [1987] 135 *U. Pa.L.Rev*., 707.

[13] Pierre Trudel, 'La protection de la vie privée dans les réseaux: des paradigmes alarmistes aux garanties effectives,' [2006] 61 *Annales des télécommunications*, 950–974, p. 957.

[14] CNIL, Suite à l'information donnée sur son site par l'intéressé lui-même, la CNIL confirme qu'elle a mis en demeure le responsable de ce site de cesser la publication d'un annuaire du dopage, News Release, June 30, 2005, < http://www.cnil.fr/index.php?id=1843&news[uid]=271&cHash=a9b6482b22 >.

their names withdrawn. However, the League's Secretary-General refused because the publication was meeting the objectives for which it was designed. The case was submitted to the French *Commission nationale sur l'informatique et les libertés* (CNIL), which introduced an action against the League. The CNIL considered that the League had violated the right to object for legitimate reasons to having one's personal information processed, as set out in section 38 of the statute on informatics and freedoms. The Bourges criminal court and Appeal Court both ruled in favour of the Commission's point of view.[15]

Clearly, as it is now applied, personal data protection law can oppose legitimate criticism of individuals with respect to their public activities and restrict circulation of information not related to an individual's private life.[16] Yet, privacy protection on the Internet should reflect the social dimensions of activities that take place there, rather than favour an approach incompatible with transparency and public criticism. Human dignity is not protected by *de facto* prohibiting criticism of people's actions and behaviour.

19.2.2 The Right to Privacy

It is important to identify approaches able to provide regulations that protect privacy effectively in network spaces. Unlike the all-encompassing notion of personal data or information, the concept of privacy includes recognition of reference points reflecting the constraints of life in society. It is thus better equipped to deliver concepts that can ensure a balance among all of the basic rights that have to be protected.

Web 2.0 applications require greater user involvement as producers and suppliers of information. They make it all the more necessary to seek a theory that can situate privacy protection in a cyberspace environment that is slipping further and further away from prefabricated categories and theories inherited from a time when computer technology was seen by a certain elite as the realm of surveillance.

The right to privacy is sometimes depicted as an overriding right to be protected from an infinity of constraints flowing from social life. This has been taken to such an extreme that, in order to evade the requirements of balance that flow from the right to privacy, we have come to use the notion of 'protection of personal life' to justify regulations inspired by people's desires to control information that displeases them.

Yet, unless it is seen as the right that eclipses all others, the right to privacy is simply a rampart guaranteeing human dignity in infinitely variable contexts. Understood

---

[15] *Gisèle N., Ligue européenne de défense des victimes de notaires / Ministère public*, Cour d'appel de Bourges 2ème chambre Arrêt du 11 janvier 2007, < http://www.legalis.net/jurisprudence-imprimer.php3?id_article=1903 >

[16] Flora J. Garcia, '*Bodil Lindqvist*: A Swedish Churchgoer's Violation of the European Union's Data Protection Directive Should Be a Warning to U.S. Legislators,' [2005] 15 *Fordham Intell. Prop. Media & Ent. L.J.,* 1206–1244.

in this way, the right to privacy is a fuzzy notion that refers to shifting thresholds of compatibility depending on time and location.[17]

The meaning of the right to privacy varies depending on the era and culture. Its content varies according to the circumstances, the people concerned and the values of the society or community.[18] Generally, private life includes things relating to love and sex, health, family life, one's home and even religious, political and philosophical opinions. Private information may also include an individual's sexual orientation, anatomy and intimate life. Private life is presented as an area of activity that is specific to a person and that he or she can close off from others.[19] It is also generally accepted that a public figure's personal life can in some circumstances be more restricted than that of an average citizen.[20] However, on the Internet, there are situations when one is in a public situation. You cannot publish your profile on the Internet and expect to run no risks.

In order to establish that there has been a violation of privacy, it has to be determined whether the disclosure of information or intrusion concerns an aspect of private life. Private life covers certain types of information that are, in principle, related but it can also vary depending on the person's position and circumstances. The concrete content of private life varies from person to person, according to the position they have in society and other circumstances. Taking the context into account is inherent to the notion of private life. It makes it possible to identify the borders of private life according to the circumstances, particularly in relation to an individual's participation in community life.[21]

19.2.2.1 Areas of Varying Degrees of Privacy

Privacy varies depending on the context. On the Internet, as elsewhere, the degree of privacy varies according to many factors. There are different situations that delimit the extent of privacy and weighing the requirements of human dignity against the legitimate information needs of others leads to recognition that some spaces and information are public. Indeed, this is taken into account in legal systems through various concepts and standards. For example, in Canadian criminal law, notions such as reasonable expectation of privacy are used to circumscribe situations in which the right to privacy and other imperatives apply.[22]

---

[17] Jean-Louis Halperin, 'L'essor de la 'privacy' et l'usage des concepts juridiques,' *Droit et Société*, 61/2005, 765, p. 781.

[18] Pierre Trudel and France Abran, *Droit du public à l'information et vie privée: deux droits irréconciliables?*, (Montréal: Thémis, 1992).

[19] Bernard Beignier, 'Vie privée et vie publique,' Sept. 1995 124 *Légipresse* 67–74.

[20] André Bertrand, *Droit à la vie privée et droit à l'image*, (Paris: Litec, 1999).

[21] Patrick A. Molinari and Pierre Trudel, 'Le droit au respect de l'honneur, de la réputation et de la vie privée: aspects généraux et applications,' Barreau du Québec, *Application des chartes des droits et libertés en matière civile*, (Cowansville: Éditions Yvon Blais, 1988), 211.

[22] *Regina* v. *Dyment*, [1988] 2 S.C.R. 417. The *Dyment* decision recognized that the right to privacy has an information-based aspect. See Karim Benyekhlef, *La protection de la vie privée dans les échanges internationaux d'information*, (Montréal: Éditions Thémis, 1992), p. 29.

Thus, depending on the context, there are different spheres of privacy. The spheres vary over time, space and circumstances. The relationships in which people are involved mean that those they interact with have different interests in different information. For example, one's spouse has a legitimate interest in knowing some aspects of one's private life but the next door neighbour does not. Likewise, employers have an interest in knowing some kinds of information about their employees for certain purposes but not for others.

The different interests in knowing are limits on privacy. When there are legitimate interests or when conditions exist that open the way to such interests, the right to privacy must give way. Legitimate interests to know what is going on restrict the right to privacy.

This can be illustrated by thinking about the information protected by the right to privacy as being located in concentric circles. Such circles delimit the information that can remain private and thereby also identify which information can circulate legitimately. Such information may not necessarily match what we consent to make available. Kayser shows that consent is not an appropriate concept for explaining the legitimacy of circulation of personal information. He writes that it is inaccurate to postulate that people tacitly consent to investigation and disclosure since 'a person who leaves private life to engage in a public activity does not think about consenting to disclosure of the activity. He or she thinks even less about authorizing research into his or her public activities.' He adds:

"The explanation has the greater defect of being inaccurate because, if it described reality, people would be able to express opposition to investigation and disclosure of their public activities. They would even be able to oppose the production and publication of images showing them engaged in such activities. However, they do not have that power."[23]

Doctrine has focused on describing the circle of privacy in relation to public life.[24] There is abundant case law examining the criteria for determining whether a situation is public or private.[25] Thus, as soon as one engages in a public activity, one leaves private life behind. Unless we completely abandon freedom of expression, we cannot extend privacy protection to claim a veto over information relating to public life.

---

[23] *Pierre Kayser,* La protection de la vie privée par le droit, *3rd Edition, (Paris: Economica-Presses universitaires d'Aix-Marseille, 1995), No. 134 [our translation].*

[24] See in particular Frederick Schauer, 'Internet Privacy and the Public-Private Distinction,' [1998] 38 Jurimetrics, 555–564; Daniel Solove, Marc Rotenberg and Paul M. Schwartz, *Information Privacy Law,* 2nd Edition, 2006; François Rigaux, *La protection de la vie privée et des autres biens de la personnalité*, (Brussels: Bruylant; Paris: LGDJ, 1990); Emmanuel Dreyer, 'Le respect de la vie privée, objet d'un droit fondamental,' *Communication commerce électronique*, May 2005, pp. 21–26.

[25] The French case law is analysed by Pierre Kayser, *La protection de la vie privée par le droit*, 3rd Edition, (Paris: Economica-Presses universitaires d'Aix-Marseille, 1995). See also Nathalie Mallet-Poujol, 'Vie privée et droit à l'image: les franchises de l'histoire,' *Légicom*, 1994/4, 51.

There are also situations that do not belong to public life but involve a third party's interest in knowing. For example, the right to privacy can be limited by children's right to know their origins, which can extend to knowing the identity of their biological parents. Owing to the imperatives of a job, an employer can have a legitimate interest in knowing some information that would otherwise belong to an employee's private life. However, for people located outside of the family circle or employment relationship, the information remains confidential.

An individual's choices also determine whether a piece of information is public or private. Choices differ from person to person and according to the context. For example, it may be considered natural to confide more in an intimate friend than in an employer. This explains why a piece of information can circulate legitimately inside a family or circle of friends, or even among co-workers, though a violation of privacy would occur if it circulated more broadly.

On the Internet, it is possible to make some information available to some people but not to others, for example, various functionalities make it possible to authorize different levels of disclosure of information on social networking sites.

Thus, the scope of privacy can be seen as composed of public, semi-public and semi-private spaces. This reflects the multiplicity of information-sharing circles associated with different areas of life, such as family and work. In the circles, information is public or private to varying degrees.

The way privacy is delimited is also determined by information-sharing circles flowing from specific events. Even when they have no public position, people can find themselves in the public eye when they are involved in public events. Such limited time-dependent circles make it possible to establish a 'right to social oblivion.'[26]

Violation of the right to social oblivion illustrates the relationship between the right to privacy and other people's right to know. The violation involves disclosing information that used to be known in the past but giving it a temporal and spatial scope different from that flowing from the initial disclosure. What is considered a violation and punished is disclosing it again, which is seen as unjustified in the context. Thus, the legitimacy of a right to social oblivion is dependent on assessment of the context in which the information is disclosed. Social oblivion is a right when it is judged unreasonable to disclose the information. In such cases, disclosure is found to be a violation, in other words, something that a reasonable person would not have done in similar circumstances. Context of disclosure is thus a very important factor in determining whether disclosure is legitimate.

The scope of the right to privacy is thus a function of the interest in disclosure. The purposes and interest in disclosure have to be identified. The premise is that the mere existence of a piece of information is not sufficient to making its disclosure legitimate. This shows the importance of the process of determining the interest in

[26] Catherine Costaz, 'Le droit à l'oubli,' *Gazette du palais*, 26 and 27 July 1995, p. 2; See also Roseline Letteron, 'Le droit à l'oubli,' *Revue de droit public*, 1996, 385 and François Petit, 'La mémoire en droit privé,' *Revue de la recherche juridique*, 1997-1, 17.

knowing. The scopes of the right to privacy and the right to disclose are determined by that process.

19.2.2.2 Interest in Knowing

Logically, not everything about an individual belongs to his or her private life. The right to privacy concerns information that affects an individual's independence and ability to exercise control over information concerning intimate relationships and life choices. However, as soon as an individual does things that concern others, his or her private life is necessarily constrained by their legitimate interests.

The democratic conception of privacy postulates that people holding public office or doing jobs that solicit public trust generally have a greater duty of transparency. People involved in public events, whether of their own free will or involuntarily, also have to expect a more restricted private life, at least as long as the event in question lasts. On the Internet there are public places and events. Visiting such places and participating in such events bring benefits but there are also accompanying risks and drawbacks.

The right to privacy varies in scope depending on the weight given to human dignity and other values in different relational contexts. For example, the right to privacy in the workplace depends on factors such as work requirements, confidentiality and level of trust.

As a legal standard, the notion of an interest in knowing has more than one meaning. Legal standards require us to examine what is acceptable in the context in which the decision applies. A standard is a flexible norm based on an intentionally underdetermined criterion.[27]

The various meanings of standards are established through different processes ranging from courts and professional fora to more fuzzy channels, such as common sense and ethical reflexes. Every meaning given to the notion can be seen as legitimate in some way. This is why it becomes the focal point when different interest groups in civil society come into conflict. It is rare that there is consensus on a definition. When there is unanimity, it is often easier to define the scope and limits of rights and duties in a more detailed manner a priori. However, when there is no unanimity, it is easier to state a rule by referring the interpreter to an assessment of the interest in knowing. This supposes recourse to a standard that can guide decision-makers. Thus, the meaning of the notion of interest in knowing emerges out of the history of concrete situations.[28]

The meaning of the notion of the interest in knowing is also defined through loose systems such as morals, ideology, common or generally accepted beliefs, ideas and fantasies more or less widespread in civil society, in short, through the common

---

[27] André-Jean Arnaud, Ed., *Dictionnaire encyclopédique de théorie et de sociologie du droit*, 2nd Edition, (Paris: LGDJ, 1993), p.581.

[28] Pierre Trudel, 'L'intérêt public en droit français et québécois de la communication,' in Emmanuel Derieux and Pierre Trudel, *L'intérêt public, principe du droit de la communication*, (Paris: Éditions Victoire, 1996), 179–189.

sense of the time and morality revealed in the body social as a whole. No source of law, not even legislation, can have a definitive effect on the conceptions and points of view that spontaneously combine, conflict and merge. Refining the arguments, concepts and views involved in determining what the public has a right to know or legitimate interest in knowing requires maintaining a healthy environment in which different ideas can challenge one another.

Seen in this way, the right to privacy is an individual's right to exercise control over information concerning something that does not belong to public space or that others do not have a legitimate right to know. It does not have universal scope. Its extent and meaning necessarily flow from examination of the limits entailed when there is an interest in knowing.

19.2.2.3 The Diversity of Circles of Friends on the Internet

The Internet is not uniform: it contains spaces of many different kinds. Some are more risky than others for the privacy of people who visit them. For example, social networking web sites make it possible for people to meet and connect through social networks. Sites such as *MySpace* (http://www.myspace.com) and *LinkedIn* (http://www.linkedin.com/) offer online services that allow people to get together. Such sites can be used to make friends, create professional relationships, publicize music groups, meet people who share the same interests, find old classmates, etc. One need only choose the site that meets one's needs and register to be potentially linked with millions of people.

The registration form generally enables users to create a basic profile containing their name, home town and occupation. Next, users can add more details, photographs, résumés and information on their interests. The information is located in a personal space.

In order to be linked with other people, users enter contact information into their address books. This requires searching for people who are already members of the site and inviting them to contact you. Users can also contact people who are not members, suggest they register and invite them to become friends. Some sites let you import a list of contacts from an existing email address so that you can send invitations to all the people on the list. When people join the site, they in turn bring in their friends and so the network grows.

The different circles of friends are protected in various ways, such as through technical barriers and a priori security. However, since this type of activity exists on the Internet, in other words, since users can decide to display certain pieces of personal information, we have to postulate that on the Internet there is information belonging to collective life in addition to that belonging to private life. In contrast, what we do on the Internet, our connection data and key words we have used are a priori private and generally should not be made public.

The different places on the Internet and the power of some information processing functions mean that cyberspace engenders greater risks that have to be managed. For example, the danger of information compiling and search engine capacities has

often been noted.[29] Information, even public information, can be found more easily and then compiled so as to deduce private information. This changes the scale of threats to privacy on the Internet.

19.2.3 The Internet Changes the Scale of Risk

On the Internet, spatial and temporal reference points change and those applying in a less networked world are inadequate. Stakes unknown in the physical world arise with great acuity in networked space.[30] The OECD's *Report on the Cross-Border Enforcement of Privacy Laws* notes that increased circulation of information, particularly on the Internet, increases risks to privacy.

Larger volumes of cross-border flows at higher speeds, reaching broader geographical areas, transferring alpha-numeric, voice and image data among an ever-greater multiplicity of actors is likely to increase the number and cost of privacy breaches borne by individuals and organizations.[31]

Risk to human dignity occurs on different scales. Circles of privacy are redrawn, shifted and re-centred.

There is a spatial shift: physical space seems to dissolve in cyberspace. The location where information is situated now has little impact on its accessibility. As soon as a document is available on a server, it can be found using general Internet search tools or other specialized tools. Distance in space and the passage of time seem to have much less impact on the real availability of information.

The Internet makes publication routine and information can easily be published outside of legitimate circles, thus the increased risk. Naturally, cyberspace is made up of both public and private spaces but the reference points that distinguish between private and public have been blurred. Belgum notes that:

"Personal data, such as address, phone number, income, property value and marital status have always been available to those willing to dig. The Internet can make it possible for a much wider class of persons – essentially all Internet users – to gain access to similar types of personal information at little or no cost."[32]

The Internet changes the spatial scale used to assess privacy risks. Outside the networked world, gaining access to a piece of information can be very difficult. On the Internet, it seems that much information is within the reach of a simple search engine query. Solove observes:

---

[29] Daniel J. Solove, 'Access and Aggregation: Public Records, Privacy and the Consitution,' [2002] 86 *Minn. L. Rev.,* 1137–1218.

[30] Frederick Schauer, 'Internet Privacy and the Public-Private Distinction,' [1998] 38 *Jurimetrics* 555.

[31] OECD, *Report on the Cross-Border Enforcement of Privacy Laws,* (Paris: OCDE, 2006), p. 8, <http://www.oecd.org/dataoecd/17/43/37558845.pdf>.

[32] Karl D. Belgum, 'Who Leads at Half-time?: Three Conflicting Visions of Internet Privacy Policy' [1999] 6 *Rich. J.L. & Tech*. 1.

"Until recently, public records were difficult to access. For a long time, public records were only available locally. Finding information about a person often involved a treasure hunt around the country to a series of local offices to dig up records. But with the Internet revolution, public records can be easily obtained and searched from anywhere."[33]

Access to court records is emblematic of the quantitative and qualitative changes generated by the Internet. As Natale M. Gome-Velez says:

"Providing Internet access to court records increases exponentially the availability of court records, including any sensitive information they contain. Examples of sensitive information that might be found in court records include: social security numbers, home addresses, names of minor children, financial account numbers and medical information."[34]

There is also a temporal shift. The persistency of information entails that it can last longer than the circle in which it was legitimate. For example, it may be legitimate for a piece of information to be available to the public owing to a current event but archiving and virtual permanent availability on the Internet could go beyond what is necessary to report the news.

Information compiling capacities make it possible to create deposits of information on people and those deposits can be used by both the police and wrongdoers. In short, now that information can be found effortlessly, there is no default privacy protection. This means we have to reassess the arguments used to determine whether one is in public or private.

All of these changes to the scope of what is at stake in terms of privacy show that the level of risk entailed by networked circulation of information has also changed. The scope of the new risks to privacy transforms the reasons underlying laws. While it used to be taken for granted that the level of risk to privacy remained low or easy to control, as the Internet has spread, qualitative and temporal changes to the scale mean that there are greater threats. This explains the calls for stronger privacy protection when information processing environments are set up.

19.3 Risk Management Through Networks

Faced with the quantitative and qualitative changes in risks to privacy, there is a big temptation to call for stronger legislation. There is even a tendency to want to give the right to privacy such priority that other rights, such as the right to transparent public process, are limited. However, regulators have to deal with cyberspace's

---

[33] Daniel J. Solove, 'Access and Aggregation: Public Records, Privacy and the Constitution,' [2002] 86 *Minn. L. Rev.,* 1137–1218, p. 1139.

[34] *Natalie M. Gomez-Velez, 'Internet Access to Court Reports- Balancing Public Access and Privacy,' [2005] 51* Loyola L.Rev., *365–438, p. 371.*

special characteristics. The most effective way to ensure better privacy protection is to increase the risks to those who endanger it.

The normative framework of the Internet can be viewed in relation to the risks that the technology seems to entail. Internet privacy regulation is a set of decisions pertaining to management of risks that are perceived by stakeholders in the network.

Risk as a social construction is assessed differently depending on the time and cultural, political and social context.[35] Ideas about the dangers and potential of technologies help construct collective perceptions of their risks and benefits. Perceptions vary over time; they are not always the same. They are also dependent on the social context and law and other norms flow largely from varying perceptions reflecting social and historical contexts.

Internet stakeholders assess the risks that a measure or rule presents for their activities. The decision to comply with one rule but not others flows from an assessment of legal risks. The risk potential of laws of different legal orders is assessed by stakeholders in relation to various factors, such as real possibility of legal action, ownership of assets in the country in question, the desire to win trust and the concern to behave like a 'good citizen.' These factors are components in analyses used by stakeholders to orient their risk management strategies.

19.3.1 Risk

Regulation of the Internet is justified largely by the perceived risks of poorly regulated use. Maryse Deguergue points out that risk can be classified as an axiological notion describing reality while at the same time passing a value judgment on it, which makes it possible to establish legal rules.[36]

The diverging and converging perceptions of Internet risks help to construct reasons that form the foundations for legal rules designed to provide a framework for how the Internet operates. Risk forecasting, management, sharing and transfer are among the primary concerns of legal systems. Ulrich Beck explains:

"Modern society has been transformed into a risk society [. . .] because the fact of discussing risks produced by society itself, the fact of anticipating and managing them, has gradually become one of its main concerns."[37]

With respect to the Internet, normativity is motivated largely by the desire to reduce, manage and spread risk flowing from availability of information. Generally, risk is seen as a social object. Yvette Veyret says that 'risk as a social object is defined as the perception of danger. Risk exists only in relation to an individual, social or professional group, community or society that perceives it [. . .] and deals

---

[35] Christine Noiville, *Du bon gouvernement des risques*, (Paris: PUF, les voies du droit), 235 p.

[36] Maryse Deguergue, 'Risque,' in Denis Alland and Stéphane Rials, *Dictionnaire de la culture juridique*, (Paris: Quadridge, Lamy, PUF, 2003), p.1372.

[37] *Ulrich Beck, 'Risque et société,' in Sylvie Mesure and Patrick Savidan,* Le dictionnaire des sciences humaines, *(Paris: Quadrige, PUF, dicos poche, 2006), p. 1022 [our translation].*

with it through specific practices. Risk does not exist when there are no people or individuals who perceive or could be affected by it.'[38] Risk does not exist in a vacuum; it necessarily flows from a social context.

Naturally, protection of information belonging to private life depends on relationships between risks. The consequences of information circulation are not necessarily known by stakeholders when information is put into circulation. It is often the agglomeration of information that is considered dangerous. For example, a harmless piece of personal information can be published and then combined with other information and this can lead to disclosure of something private about an individual. In such a situation, the person concerned has consented to the disclosure or the public nature of the situation has brought the information out of the field of private information but there is nonetheless a violation of privacy.

Once acknowledged, risk entails an obligation to take precautions. Indeed, legal risk flows from situations in which there could be a violation of the rights of others. Even though they are different, there is a close link between technological and legal risk. When technological risk is proven, it almost always entails an obligation to take it into account and behave accordingly. Likewise, legal risk can result from non-compliance with laws or other obligations. Hypothetically, legal risk arises in situations in which individuals can be blamed.

Those who take part in cyberspace activities do so to a greater or lesser degree depending on the amount of risk to which they are aware of exposing themselves.

19.3.2 Networked Normativity

Risk management is part of a networked regulation process.[39] Networks are the result of interactions among people who find themselves linked. Networking supposes interconnected environments uniting stakeholders, regulators and the bodies playing a role in governance of the Internet.[40] In the spaces created by networks, namely, cyberspace, normativity is developed and applied according to a network

---

[38] Yvette Veyret, 'Les risques,' *Dossier des images économiques du monde*, FEDES, cited by Franck Verdun, *La gestion des risques juridiques*, (Paris: Éditions d'organisation, 2006), p. 11 [our translation].

[39] Katherine J. Strandburg, Gabor Csardi, Jan Tobochnik, Peter Érdi and Laszlo Zalanyi, 'Law and the Science of Networks: An Overview and an Application to the 'Patent Explosion,' [2006] 21 *Berkeley Technology L.J.*, 1293–1351; Andrea M. Matwyshyn, 'Of Nodes and Power Laws: A Network Theory Approach to Internet Jurisdiction through Data Privacy,' (2003) 98 *Nw.U.L.Rev.*, 494–544; Avitai Aviram, 'Regulation by Networks,' [2003] *Brigham Young U. L.Rev.*, 1180–1238; Lior Jacob Strahilevitz, 'Asocial Networks Theory of Privacy,' [2005] 72 *U. Chi.L.Rev.*, 919–988.

[40] Manuel Castells, *La société en réseaux. L'ère de l'information*, (Paris: Fayard, 1998); François OST and Michel de Kerchove, *De la pyramide au réseau: pour une théorie dialectique du droit*, (Brussels: Publications des facultés universitaires Saint-Louis, 2002).

model.[41] Renaud Berthou sees the Internet as 'a factor for development of a multiplicity of network processes.' While it is not the only cause of network development in law creation in post-modern times, it is a major instrument of change.[42]

In a network, stakeholders manage risks and seek to limit them or transfer them to others. For example, operators of social networking sites publish warnings so that users will consciously accept the risks flowing from putting their personal profiles online. Other stakeholders may consider establishing mechanisms to obtain consent for personal data processing so as to limit risk entailed by enforcement of national personal information protection laws.

Regulations can flow from technological standards, management norms and legal rules. There is no reason to consider that legal or other norms are always dominant. In fact, various sets of regulation-producing norms compete with one another: technological, market and legal standards are not always consistent. In some situations, legal references are absent from debates over what are seen as essentially management or technological issues. In other contexts, technology is bridled by law.

Government and other players can increase the risks involved in some forms of behaviour and activities, or reduce the risk associated with safe action. For example, when strict legislation is adopted against certain practices, the risk associated with those practices increases. In the case of legitimate activities, the government can signal and even limit risks to stakeholders. While government seems to have lost power in cyberspace, it generally still has strong influence over bodies located on its territory as well as over those that could be targeted by legislation indirectly.

In a network, every stakeholder able to set conditions has the ability to increase the risk of others. Thus, a government can impose duties on citizens living on its territory. The latter then have to manage the resulting risk. They will seek to ensure that their partners comply with the obligations that they themselves are required to fulfil and for which they are responsible.

In sum, the system of regulation is designed to re-establish balance between risks and precautions. It has to encourage all stakeholders to minimize the risks flowing from situations over which they have some control and to maximize the risk incurred by stakeholders who choose to behave in ways that are harmful or unduly increase risks to legitimate users. Privacy protection on the Internet belongs to this approach.

19.3.2.1 The Many Relations Among Norms

The Internet can be seen as a world made up of normativity nodes and relays that influence one another. What is at stake is not whether law, technology or self-regulation provides the best protection for privacy. Effective normativity results

---

[41] Pierre Trudel, 'Un 'droit en réseau' pour le réseau: le contrôle des communications et la responsabilité sur internet,' in INSTITUT CANADIEN D'ÉTUDES JURIDIQUES SUPÉRIEURES, *Droits de la personne: Éthique et mondialisation,* (Cowansville: Éditions Yvon Blais, 2004), pp. 221–262.

[42] Renaud Berthou, *L'évolution de la création du droit engendrée par Internet: vers un rôle de guide structurel pour l'ordre juridique européen*, PhD thesis, Université de Rennes I, Rennes, July 2, 2004, p. 373 [our translation].

from dialogue among stakeholders and their ability to relay norms and principles. In order to learn which norms govern an environment connected to the Internet, we have to identify the nodes in which they are stated.[43] For example, a state sets out legislation that is obligatory on its territory. Relays both connect and separate nodes. For example, to manage risk adequately, a company governed by the laws of Québec has to require parties with whom it signs contracts to protect personal data in accordance with Québec law. In virtue of other legal relationships, the same company may have to comply with European legislation. Co-contractors also have to comply with contract terms and technical standards.

Thus a way to strengthen privacy protection is to establish a set of measures designed to reinforce one another so as to limit risks to the privacy of cybernauts engaging in licit activities. The strategy has to be deployed in a network: stakeholders have to comply with rules and be encouraged to relay the requirements to those they influence.

In risk management, government measures will be more effective if they are accompanied by dynamic surveillance and enforcement policies wherever possible. Legislation that is notoriously not applied will be perceived as entailing lower risk.

For stakeholders in cyberspace, responsibility law that is set out and enforced by the state is an important part of the framework structuring actions and circumscribing obligations. Indeed, both collective and individual stakeholders adopt rules of conduct in order to manage risk and limit responsibility. This entails relaying the requirements set out in nodes of normativity. In every environment, the principles stated in such nodes, such as statutes and widely accepted principles, are relayed through micro- and self-regulation.

The network structure of cyberspace law makes it possible to describe the many relationships among the different orders of norms applying on the web. The risk management paradigm provides an explanatory hypothesis concerning the effectiveness of norms. Rules' effectiveness seems to be a function of their ability to promote optimal management of the risk that they permit stakeholders to identify, since the risk concerns both the danger justifying the norm itself and the sanctions and other constraints it engenders.

19.3.2.2 Norms are Proposed, Imposed and Relayed

In a network, many different relations can be seen between norms. Norms are proposed and even imposed in various nodes of normativity, which both compete with and complement one another. Relays between norms ensure rules are applied effectively because they make them explicit and disseminate the norms and their consequences.

---

[43] Pierre Trudel, 'Un 'droit en réseau' pour le réseau: le contrôle des communications et la responsabilité sur Internet,' in INSTITUT CANADIEN D'ÉTUDES JURIDIQUES SUPÉRIEURES, *Droits de la personne: Éthique et mondialisation*, (Cowansville: Éditions Yvon Blais, 2004), pp. 221–262.

A number of relationships can be identified among norms. In most cases, there is obligation: national legislation is compulsory for a person located in that country and that person necessarily has to relay the obligations flowing from the legislation or else suffer the consequences. This shows the degree of risk flowing from effective legislation. If legislation is not enforced, it will be perceived as generating negligible risk. This also shows how important it is to limit the number of laws. If legislation is adopted but enforcement resources are not provided, the law will be feeble.

In other situations, indirect application of norms flowing wholly or partially from other legal orders can be seen as a risk. For example, European directives affect not only member countries but also the obligations of stakeholders in countries with strong relationships with European nationals. This also applies in the case of American legislation: people running sites in other countries often consider that it is a good practice to comply with American laws because they hope to do business with Americans.

Regulation of Internet use thus often results from both the national law of the country where a site is based and the law of bodies that influence other sources of norms.

Some sources of normativity produce norms and coordination processes while others function like spaces of negotiation and balancing in which regulations are applied through a dialogue with other sources of normativity. For example, it is often following invitations from international organizations that states are led to spread norms contained in their legislation. This occurred in the case of the *Convention on Cybercrime*[44], which has been promoted by European Council and is open to signing by other countries.

Finally, when we engage in an activity on the Internet, we generally have to consider the possible risks entailed by failure to comply with many different kinds of norms. While the legislation of the country where we are located automatically applies, we may also have to cope with other legal, technical and customary rules that flow from the broad expanse of sources of norms.

19.4 Conclusion

On the Internet, users manage risks: they accept them or transfer them, limit or minimize them. It results that in practice, privacy protection on the Internet is regulated through risk management.

The risk management approach shows that what is at stake is not so much whether legislation or self-regulation should be used to protect privacy, as if one excluded the other. On the contrary, understood as a set of risks to be managed, Internet regulation has to be seen as a set of various kinds of norms that are necessarily relayed through many different networked processes. The incentive to relay

[44] COUNCIL OF EUROPE, *Convention on Cybercrime*, Budapest, 23 November 2001 < http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm >

the requirements of a rule so as to oblige others to comply depends on whether the rule generates risks that are seen as significant by those concerned.

Norms flowing from technical standards either increase or limit risks to privacy. Government and other regulators can also expand or shrink risk. Risk management decisions taken in nodes with enforcement capacity create norms that are in turn relayed to other actors. Governments can impose obligations that limit risks to privacy. On the Internet, such measures are generally treated by stakeholders as risks to be managed and transferred to co-contractors or other partners.

Cyberspace is an interconnected whole composed of interacting nodes of normativity. It is made up of spaces in which norms applying to users are enforced wholly or partly. A set of systems of norms are discussed and applied in cyberspace. In addition to government and private regulations, there are processes designed to provide frameworks for activities that cannot be regulated entirely by territory-based law. Technology and related constraints are also sources of norms in networks.

All of the norms on the Internet can be described according to a network model. Internet activities are thus governed by a networked normativity, the effectiveness of which is largely a function of norms producers' ability to create sufficient risk for other stakeholders so as to motivate them to manage the risk. It is as if the network were a vast environment in which stakeholders generate the risks that they perceive and then produce obligations that they spread to those with whom they are in virtual contact.

Privacy protection develops and functions according to a network model. Stakeholders can increase, transfer and limit risks. The effectiveness of regulation is a function of the real ability to increase the risk of those engaging in dangerous activities and to manage the risk of legitimate users. The more we understand about the relations between the various risk management processes, the greater our chances of achieving effective privacy regulation on the Internet.