Rule of Law and the Effectiveness of Privacy Protection in E-Government Networks

Pierre TRUDEL*

Introduction

The context in which information on individuals circulates has undergone significant change. Information systems are now designed as networks, in other words, inter-connected environments in which information circulates from one centre to another in a multi-directional, non-hierarchical manner. Such environments redefine the spaces in which information on individuals circulates. This is clear in the public sector, where there are growing plans to provide public services online and even e-government.

The spread of activities that can occur in environments such as the Internet requires a better analysis of the space in which personal information circulates, particularly with respect to virtual reality's growing role.[1] We have to review the notions that identify information that has to be protected because it is private and information that has to circulate because it is part of the public arena, contributes to the conduct of life in society or is needed for smooth delivery of public services.

A postulate of the present legal framework is that it is unusual for personal information to be shared without the consent of the individual

* Holder of the L. R. Wilson Chair in Information Technology and E-Commerce Law, Centre de recherche en droit public, Faculty of Law, University of Montréal. Email: pierre.trudel@umontreal.ca.

1 Vincent GAUTRAIS, "Le défi de la protection de la vie privée face aux besoins de circulation de l'information personnelle," *Lex electronica*, Vol 9 No. 2, winter 2004, <http://www.lex-electronica.org/articles/v9-2/gautrais2.htm>.

concerned. Yet, we have to admit that there is considerable sharing of personal information among some public agencies. In most countries, information sharing is authorized, but generally so as to increase the copying of one organization's data by another. This encourages duplication and, given information's persistency, increases the quantity of personal information held by governments.

A twofold phenomenon of personalization and pooling of information is characteristic of several trends accompanying the emergence of e-government. Circulation and sharing of information make it possible to improve service quality and speed. By reducing redundancy and limiting the situations in which people are required to resubmit the same information, we increase productivity, which should benefit everyone.

It is probable that people will expect to interact with the government in the same way that they are becoming accustomed to interacting with other online service providers. People will expect that information relevant to the relations they have with government will be available when needed, and that the information will be appropriate for the purposes in question. For example, when people move, they could send the change-of-address information only once and to a single place, and from there it could be relayed to all the departments and agencies that need to be informed.

In the first part of this paper, we will perform a critical review of a number of basic concepts underlying protection of personal information. We will show that the concepts have to be adapted to requirements flowing from the spread of networks. We will note how the notion of personal information oversimplifies the situation, and the perverse effects of the "surveillance paradigm" that underlies the dominant interpretation of current personal data protection law. This paradigm leads to global interpretations that cover the notion of personal information. It has favoured an inflexible interpretation of a number of notions, as well as a tendency to hinder or prohibit the circulation of information that has little to do with privacy. Too many expedients have had to be developed to make up for these problems. The result is needlessly complex and costly privacy protection.

In the second part, we will present the components of an updated framework able to provide effective protection for personal information in the network spaces used by public services[2].

I. Traditional approach for the protection of personal information

Legislation on protection of personal information has been around for nearly 30 years. It is primarily the result of a movement conveying concern about the perils of centralized computing, and has taken the form of a kind of defence against surveillance by government authorities. Its foundations have been little debated. One author even said that it was "symbolic legislation" with, in particular, weak roots in societal demand.[3] Ritual reference to a few surveys showing that people are concerned about their privacy is usually used to justify inflexible interpretations of personal data protection rules. In most countries, it has generally been taken for granted that the techniques used by legislators and regulatory bodies are appropriate. Yet, the legislation remains obscure and difficult to enforce.[4]

Growth in the circulation of information changes the scale of the risk to protection for individuals. The spread of networks has led to changes in the rationale behind the legislation. This explains why there are always demands for stronger privacy protection when information-processing environments are established. However, it is far from certain that we will be able to provide effective control over the production and circulation of personal information if we simply recycle approaches inherited from existing frameworks.

---

2 The examples are taken from the experience of Quebec legislation. This province was the first canadian jurisdiction to adopt comprehensive legislation on Freedom of information and Privacy in the '80.

3 Pierre SADRAN, "De l'efficacité des politiques symboliques: l'accès à l'information et la transparence administrative," in Pierre TRUDEL, Ed., *Accès à l'information et protection des données personnelles*, Montréal: P.U.M., 1984, p.29.

4 See Valérie SÉDALLIAN, La loi informatique et liberté: du mythe à la réalité, <europa.eu.int/comm/internal_market/privacy/docs/lawreport/paper/sedallian_en.pdf >.

In order to guarantee the effectiveness of privacy protection in open environments, we have to re-examine some of the premises underpinning the present regime. In a world where information is circulating more, the legal framework for privacy protection should no longer be focussed on surveillance, but rather on appropriate, controlled use of information about individuals. Hindering the circulation of information will no longer ensure privacy protection. Instead, we have to establish appropriate, effective controls over the collection, use, circulation and quality of information on individuals.

A. Foundations that have become inappropriate

Personal information protection law was designed to protect individuals' privacy against the danger that information technologies could be used for surveillance purposes. With experience, we have found that personal data protection legislation has been designed not so much to prevent surveillance as to ensure information quality in decision-making processes. However, the persistence of the surveillance paradigm has led the scope and interpretation of some notions to be extended to the point that what was supposed to protect only privacy has been converted into complete protection of personal life. This slide in the foundations of privacy protection law hinders efforts to refocus on ensuring effective privacy protection.

1. The right to privacy

The right to protection of personal information is a facet of privacy protection regimes. There is a close relation between rules on protection of personal information and a person's real ability to control the circulation of information about him or her. However, the notion of personal information is born out of a desire for simplification. In order to circumvent the difficulty of identifying what should remain secret in the name of the right to privacy, we have opted for a notion that confuses "information that identifies a person" with "privacy information." Thus, in the name of privacy protection, a set of rules has been established that target not information on private life, but all information that could identify an individual.

The right to privacy varies depending on the context, epoch, moeurs and, especially, individual's position in society. In order to establish whether there has been an invasion of privacy, we have to determine whether a disclosure of information or invasion concerns an aspect of private life. Private information includes certain kinds of information that are, in principle, related to one another. What is considered private also depends on a person's position and situation. Traditionally, privacy is considered to have two main components. First, it includes the facts about and aspects of the life of a person that are included in a protected sphere. This makes it possible to identify elements that are considered to belong to a person's private life at a given time. However, the concrete content of the sphere varies depending on the person, the position he or she has in society and other circumstances. This component takes the individual and context into consideration, and makes it possible to assess the content of the sphere in accordance with the circumstances, in particular, the individual's participation in the community.[5] Very little of this is maintained when we resort to the all-embracing notion of "information that could identify an individual," which is at the heart of most legislation on protection of personal information.

An all-embracing notion of personal information was adopted in order to provide a clear definition of information that concerns individuals and should be protected. The goal was to eliminate problems flowing from the changing, contextual nature of the notion of private life. Clearly, a desire for simplification was at play here. While there was agreement that much personal information about an individual was private, there was also consensus that this was not true of all information on an individual. Yet, these nuances have frequently been overlooked.

The result of this slide has been the conflation of information on individuals in general and private information. The whole class of information thus constituted has been protected by censuring without distinction all information on individuals. Fear of surveillance has accentuated the distortion that was introduced into the legislation out of

---

5 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," in Barreau du Québec, Formation permanente, *Application des chartes des droits et libertés en matière civile*, Cowansville, Éditions Yvon Blais, 1988, 197 p. 211.

convenience. We have come to see all data on an identifiable individual as being related to his or her private life. The legitimacy associated with privacy protection and human dignity has been used to justify mechanisms that do not always concord with the balance that has to exist among the various rights brought into play by circulation of information.

2. Apocalyptic Extrapolations

A number of claims about the risk of circulating personal information are based on alarmist extrapolations. Generally, the warnings invoke the potential for misuse flowing from the power of information technologies. It is taken for granted that misuse will necessarily and universally occur, and there are calls for *a priori* mechanisms to prohibit operations that are perceived as potentially dangerous.

Yet this is not the approach taken with respect to many other types of technological and social risks. For example, the use of cars on roads is not prohibited even though some drivers use such tools inappropriately or even dangerously.

To date, all cases of surveillance flowing from the processing of personal information are anecdotal. Most concern police surveillance operations that for all practical purposes fall outside the scope of legislation on the protection of personal information. There have been a few incidents that have resulted in inappropriate circulation of personal information, but in a number of cases, it seems the problems resulted from a lack of resources or will to apply existing legal provisions. However, unless we expand the meaning of the word 'surveillance,' a search for widespread surveillance of individuals will be in vain.

Faced with the theoretical possibilities offered by information technologies, people have invoked the fear of surveillance not in reference to surveillance activities that actually occur, but with respect to those that could become possible if information were used in a harmful manner. Thus a self-justifying cycle begins: having proclaimed great danger, people then cite surveys that indicate that other people have believed the alarming predictions and are concerned about threats to privacy that could follow from increased processing of personal information.

Despite the fact that there have been few attempts to ascertain its real applicability, the surveillance paradigm has resulted in constantly growing inflexibility and bureaucratization of personal data protection measures. In order to prevent surveillance, information, no matter whether it is sensitive or not, has now to be confined to the organization that collected it, and may circulate only if the person concerned has given informed consent. An individual's medical records thus have the same status as his or her email address! From this point of view, in order to prevent surveillance, information must not circulate. Thus, redundancy is preferred over re-use of the same information. It does not matter that people have to perform the same operations again and again or that there are numerous databases containing the same personal information. All that matters is that the information is contained in separate administrative modules and used for only one purpose.

This approach overlooks the way that networks work and increases the overall possession of personal information. Since it is in principle prohibited to obtain personal information other than by asking for it from the person concerned, the same data has to be collected and recollected, thereby accumulating and over-accumulating personal data in always more databases that are increasingly difficult to monitor.

As use of information technologies spreads, we need stronger, better-targeted foundations. We cannot continue living indefinitely with the fears of a time when all technology use was associated with the misuses that could be made of it. Such poorly designed measures could weaken privacy protection.

3. Misplaced Fears

A number of interpretations of legislation on personal information are based essentially on apprehensions and extrapolations. Daniel J. Solove has noted that fears concerning databases containing personal information have not been well articulated.[6] The media, political decision-makers and jurists all describe problems stemming from personal

---

[6] Daniel J. SOLOVE, "Privacy and Power: Computer Databases and Metaphors for Information Privacy," [2001] 53 *Stanford L. R.,* 1393, p. 1395.

information processing based on the Big Brother metaphor in George Orwell's novel *1984*. There is a flourishing supply of writings arguing for the need for personal data protection legislation based on the possibility of a surveillance society similar to that described by Orwell in his famous novel.[7]

Fear of technology is characteristic of the clear majority of analysis and discourse on the dangers and risks that technologies present for people. However, since information processing is seen as invariably leading to surveillance, the conclusion is that the spread of tools that can be used for such purposes will necessarily engender greater dangers. Lucas, Devèze and Frayssinet write that

> ...new technologies are a powerful bureaucratic and technocratic tool that have become essential for increasing the efficiency of government, police services, the justice system, public policy implementation (health, employment, public assistance, etc.), fraud prevention and projections. Virtually all administrative actions require records.[8]

Their analysis reflects what Daniel J. Solove calls the "Big Brother metaphor." However, when we look at it carefully, personal data protection does not counter the danger of surveillance. Instead, it is designed to ensure that information on people is accurate.

In arguments justifying measures for controlling personal information, the possibilities offered by technology are noted and then a conclusion is immediately drawn about the possibility of misuse. Supposed surveillance dangers, dramatic identity thefts and other fantasies from literature and films are automatically invoked. Yet, when we

---

[7] It is interesting that so little attention is paid to another aspect of the society described by Orwell in *1984*. The novel describes a society where officials from the "Ministry of Truth" spend their time rewriting history and erasing the names and photographs of those whom the state has eliminated! This resembles the tendency of those who demand that public data, such as that in databases of legal decisions and probably newspapers, be purged of their names. Thus, historical archives would be censured in the name of a totalitarian conception of privacy protection!

[8] André LUCAS, Jean DEVEZE and Jean FRAYSINNET, *Droit de l'informatique et de l'Internet*, Paris PUF coll. Thémis Droit privée, 2001, p. 10 [our translation].

document the dangers really threatening individuals owing to the circulation of personal information, we do not find surveillance but rather problems generated by information quality in decision-making processes. We thus find that the

> …danger comes from the inadequacy, ambiguousness, inaccuracy and inappropriateness of information that is sometimes gathered in bad faith and for dubious ends, which may be hidden behind an attractive veneer of argumentation.[9]

From this point of view, there is no "innocuous information." Lucas, Devèze and Frayssinet note that

> …experience shows that there is no innocuous information and that the notion of sensitive data (on health, opinions on politics and unions, private matters) *a priori* defines what has to be considered in context. After all, mail-order companies do not ask customers for their ages because that would be viewed poorly, but thanks to INSEE's tables on the popularity of given names, they can estimate people's ages quite accurately.[10]

According to this line of reasoning, even a person's given name could be private information because it would make it possible to know the person's age by extrapolation. However, the age that would be attributed to an individual in such a situation would be based cross-references with historical documents, namely the annual tables of popular first names. Thus, it might be likely that a person named Nathalie was born between 1965 and 1972. Clearly, what poses a problem is not so much the threat to privacy, for the individual's real age will not be disclosed. What is in question is rather probable data based on the fact that individuals born in certain years are very likely to have certain first names. Naturally, it would be absurd to use such information in order to make a significant decision with respect to the individual. Thus this is not

---

9 André LUCAS, Jean DEVEZE and Jean FRAYSINNET, *Droit de l'informatique et de l'Internet*, Paris PUF coll. Thémis. n° 18 [our translation].

10 André LUCAS, Jean DEVEZE and Jean FRAYSINNET, *Droit de l'informatique et de l'Internet*, Paris PUF coll. Thémis n° 19 [our translation].

an invasion of privacy. It is rather a problem of information quality. While the information on age obtained using this kind of linking is sufficient for targeting with respect to marketing, it is clearly insufficient for making any decisions about the person in question.

The example is extreme, but illustrates the usefulness of basing personal information protection not on surveillance risks but on information quality guarantees. The example also illustrates the pitfalls of confusing all information on an individual with his or her private life. Finally, it sheds light on the fact that the problems targeted by personal information legislation rarely concern surveillance operations, but often the accuracy of information used in making decisions about individuals.

4. A Slide from Privacy to Personal Life

Many uses of personal information do not violate privacy. Privacy is a weak justification for taking measures with respect to information that must circulate in society. This is probably why some people have resorted to an extremely vague notion with an as yet undetermined scope: the notion of personal life. This notion seems to result from an attempt to resolve conceptual difficulties flowing from the fragility of the foundations of controls on personal information that is not related to privacy.

Fear that information could be used inappropriately leads to a search for protection for all information concerning an individual. As soon as one postulates that there is no innocuous information and that cross-referencing makes it possible to establish profiles using the most ordinary clues, one can no longer make the distinction between private information and that in the public domain. Accordingly, it becomes impossible to base personal data protection regimes on privacy protection alone. Given the perceptions of the risks likely to flow from cross-referencing information, we have come to find it natural that legislation prohibits all circulation of information *a priori*, with no regard to wrongdoing, or whether individuals' privacy has been violated, or whether harm has in fact been caused.

This explains the demand for acknowledgement of a "right to personal life." For example, Frayssinet argues that "violation does not concern private life but all aspects of personal life."[11]

The result is a stream of demands that looks like a general quest for a veto over all information on individuals, including information the disclosure of which was not long ago seen as one of the normal inconveniences of living in society. For example, the right not to receive advertizing or email solicitation has been invoked. Fear of such annoyances is partly justified and leads to demands to establish controls over all kinds of situations in which personal information is concerned. In many ways, the demands to strengthen personal data protection have sometimes become demands not for privacy protection but for protection from the inconvenience inherent to living in society. This approach is incompatible with the requirements of a democratic society because it prevents the exercise of other basic rights, such as freedom of expression and accountability.

The notion of protection for personal life does not have hard edges; it essentially seems to refer to individual preferences, and it is difficult to see where it stops. While the notion is intended to provide a protected space where individuals can have some intimacy and control over their lives, it is confused with the notion of privacy, which is delimited by the imperatives of life in society. "Personal life" has a greater extension than "privacy" and establishes as a right anything that could upset an individual, depending on his or her sensibilities. The notion is not recognized in any legislation or constitutional texts. It would be dangerous to base a law on a notion so closely connected to the various, and sometimes even arbitrary, sensibilities of individuals.

Moreover, the notion of personal life leaves little space for the requirements of life in society, for the fact that information has to be able to circulate in the name of the interests of the community or for the fact

---

[11] Jean FRAYSSINET, "La protection des données personnelles est-elle assurée sur Internet?," Text presented at the international conference, *Droit de l'Internet, approches européennes et internationales*, September 2001, http://droit-internet-2001.univ-paris1.fr/pdf/vf/Frayssinet.pdf. See also André LUCAS, Jean DEVEZE and Jean FRAYSINNET, *Droit de l'informatique et de l'Internet*, Paris PUF coll. Thémis droit privé, 2002, n° 50.

that such circulation is, in practice, rarely harmful. If everything depends on personal choice, then there remains little room for circulation of information in order to meet the needs of the community.

Finally, now that all significant human activities depend on the use of networks, we need a legal framework sophisticated enough to ensure a balance among the various rights that come into play in social interactions. In this context, the notion of personal life is too rudimentary to be useful as a framework for reflection. Even worse, by contradicting other values inherent to the democracy that it necessarily conveys, this notion tends to force the rule of law to take a step backwards.

This drift has diverted many resources into the protection of individual desires that are usually determined by moods, and left the way open to practices that are much more of a threat to privacy. In the name of protection of personal life, we have increased the censure of public information, but done little to monitor surveillance activities, in particular those of private investigation and credit rating agencies.

For example, in Québec, a company that gathers and sells information on the credit of individuals is sued several times every year but this has apparently escaped the attention of the *Commission d'accès à l'information*. Yet, the Commission has expressed concerns about the dangers of genealogical research and publicized worst-case scenarios concerning functionalities designed to facilitate online transactions between government and individuals. It is surprising that such zeal is displayed with respect to projects that are designed to ensure a high degree of privacy, while at the same time such apparent disinterest is shown in the activities of companies that do not seem to put much effort into ensuring the accuracy of information they distribute about individuals' credit history.

B) Increasingly Laborious Enforcement

Conceptual slips and drifts have made protection of personal information more and more difficult to enforce. The malfunctions are even more visible in situations where information has to circulate in order to perform services that are generally in the interest of individuals living in society.

1. The Illegitimacy of Public Space

The wide scope given to the notion of personal information has sometimes turned public information into data that has to be treated as if it were confidential. This has resulted from the destruction of the balance that a number of legal systems had nonetheless been careful to establish between privacy and the need to allow some information on people to circulate. The following examples taken from application of Québec legislation illustrate this disturbing phenomenon.

For example, in Québec, section 55 of the Act respecting Access[12] stipulates that "Personal information which, by law, is public is not nominative information." The topic in question is information governed by a principle of free circulation, yet the *Commission d'accès à l'information*, which is responsible for enforcing the protection of personal information aspect of the legislation, has not shied from setting limits on the circulation of data that the legislators were careful to exempt from the nominative information regime.

An opinion on public keys infrastructures (PKI) by the Québec Commission[13] illustrates the extent of the slide. The opinion does not take into account the public nature[14] of information kept in directories associated with public key infrastructure. The *Avis de pertinence sur la solution intérimaire de l'infrastructure à clés publiques gouvernementales du secrétariat du Conseil du Trésor* asserts emphatically that "use of PKI implies that additional information will be gathered on individuals and organizations and that their actions will be monitored" (our emphasis). It is of course possible that this kind of infrastructure could result in risks to

---

12 *An Act respecting Access to documents held by public bodies and the Protection of personal information*, R.S.Q., c. A-2.1, hereinafter the "Act respecting Access."

13 COMMISSION D'ACCÈS À L'INFORMATION, *Avis de pertinence sur la solution intérimaire de l'infrastructure à clés publiques gouvernementale du secrétariat du Conseil du trésor*, August 2001, < http://www.cai.gouv.qc.ca/fra/docu/a011107.pdf > [our translation].

14 Section 50(2) of the *Act to establish a legal framework for information technology* asserts the public nature of the directory.

privacy protection. However, postulating *a priori* that surveillance is a necessary consequence of PKI is simply an unfounded assertion.

In its *Avis relatif à la diffusion sur Internet de renseignements contenus dans les demandes de permis de construction,*[15] the Commission takes it upon itself to restrict the notion of public information for the reason, which is however not included in the legislation, that if public information were on the Internet, it could become available to millions of Internet users, and this could make Québec a "paradise for direct marketing." Of course, we may have prejudices against direct marketing and find it unpleasant to receive unsolicited advertising. However, this has so far been a matter of personal preference. Direct marketing is not illegal in Québec. It is surprising that a public agency responsible for enforcing legislation would indulge in making value judgments about an activity that is in itself legal.

Moreover, the Commission sets requirements on the purposes of public information. It states that "even though the legislation is mute on this subject, we can nonetheless identify the objective of such a provision." The Commission thus adds to the legislation by including a kind of intangible limitation on the public nature of information based on the purpose for which it is to be used. This procedure is very disturbing. Value judgments are being made on a whole set of possible uses of public information. Is it illegitimate to consult the assessment roll to find out how many buildings an individual owns in a city? There is nothing that says that the fact that someone owns a building, or even several, is information belonging to his or her private life. However, legislation already, and rightly, prohibits inappropriate publication of such information if it is harmful or not in the public interest.

Fears about possible misuses of public information have led to drastic restrictions on how information can be accessed. Access to data now depends on the real or supposed purposes underlying their public nature. Thus, public information is censured because there is a risk (most often hypothetical) that it could be misused.

---

[15] COMMISSION D'ACCÈS À L'INFORMATION, *Avis relatif à la diffusion via intranet et Internet par la ville de Gatineau des renseignements contenus dans les demandes de permis de construction, mai 1999*, < http://www.cai.gouv.qc.ca/fra/docu/a990534.pdf > [our translation].

This aberration has even been included in the *Act to establish a legal framework for information technology,*[16] which establishes a mechanism to censure public documents containing personal information. Section 24 reads as follows:

> The use of extensive search functions in a technology-based document containing personal information which is made public for a specific purpose must be restricted to that purpose. The person responsible for access to the document must see to it that appropriate technological means are in place to achieve that end. The person may also set conditions for the use of such search functions, in accordance with the criteria determined under paragraph 2 of section 69.

This provision applies to public data. It does not concern private information. It makes it possible to restrict the use of extensive search functions on technology-based documents containing personal information that has been made public for a specific purpose. The goal is, for example, to prevent search engines from scanning databases to find personal information for purposes other than those for which the information was gathered or published.

One might suppose that this kind of measure is justified by the fact that it often takes a long time to search paper documents because they have to be examined one by one, but technology-based documents are far easier to search in many more ways, which gives rise to fears of misuse. The solution to this hypothetical problem has been to establish technological means of protecting personal data contained in public documents. The form of protection consists in limiting access to only the purposes for which the document was made public, as if the purposes were known and specified. Decision-makers will have to start specifying the purposes of public information. It is difficult to see how this would be feasible without making an *a priori* judgment on the legitimacy of some research, not to mention the difficulty, given the absence of any relevant legislation, in determining the purpose of a piece of public information. Indeed, when information is public, it is available to anyone, unless it can

---

16 *An Act to establish a legal framework for information technology,* R.S.Q., c. C-1.1, < http://www.autoroute.gouv.qc.ca/loi_en_ligne/index.html >.

be shown that the person seeking access will use it for harmful or illegal ends. Unless we deny the public nature of a piece of information, we cannot presume that it should be used only for certain ends but not others. The only legitimate restriction on use of public information is misuse. Postulating *a priori* that misuse will occur leaves little space for the right to information.

With this kind of approach, there is no longer any public information. There is only data that can circulate and be used for predetermined purposes by public or private authorities so long as there are no accusations of possible misuse. It is hard to believe that this is the approach adopted by Québec, which was one of the first to legislate a right to information, specifically in Article 44 of the *Charter of human rights and freedoms*. The values in the name of which some information is given a public nature have been ignored. The only things that seem to count are generally hypothetical dangers to privacy. This bias is troubling and deeply inconsistent with the idea that all rights and freedoms are delimited by the exercise of other rights.

Another weakness in these analyses results from the fact that they show little interest in assessing alternatives to the recommended measures, which invariably remove information from the public domain on the basis of dubious fears. On one hand, specific purposes are lent to freely available information so long as there is no misuse, and on the other hand it is postulated that a piece of information can have only one set purpose. These approaches show growing inflexibility with respect to the notion of purpose.

2. Inflexibility of the Purpose Principle

The purpose principle states that information may be gathered and used only for purposes consistent with those for which the information was originally gathered. The inflexibility that has been given to this principle has helped to immobilize personal information. There has been a tendency to make it into a principle limiting possible uses of personal information. This has often institutionalized redundancy. The same information has to be requested time and again because it is not available if it has been gathered for other purposes.

Yet the purpose principle flows from a concern to maintain accuracy of information. The OECD states the principle as follows:

> Personal data should be relevant to the purposes for which they are used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.[17]

A piece of information might very well be useful for one purpose, but useless or even inappropriate for another. In a world of networks where information circulates and is persistent, it is important to go back to the real foundations of the purpose principle. This means ensuring that the information used is accurate enough for the purpose, and not establishing redundancy as a means of guaranteeing privacy!

Lucas, Devèze and Frayssinet note concerning the *raison d'être* of the purpose principle:

> Rather than in the nature or primary meaning of the information or technology, the danger lies in the purposes for which personal data are used. The purpose has to be legitimate for the information manager and useful or necessary for the individual concerned, who must first be informed and be able to make personal, informed decisions to determine his or her independence with respect to information.[18]

A principle designed to provide legal guidelines for processing personal information from a person has been converted into a principle justifying censure of circulation of information. In the name of possible, hypothetical misuse of information on individuals, a regime has been constructed to control information so as to prevent uses not initially planned and give individuals and bureaucracies a veto over use of the information, as if it were private.

---

17 OECD, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, Paris, OECD, 2002, < http://www.oecd.org/document/18/0,2340,en_2649_201185_1815186_1_1_1_1,00.html >

18 André LUCAS, Jean DEVEZE and Jean FRAYSINNET, *Droit de l'informatique et de l'Internet*, Paris PUF coll. Thémis droit privé, 2002, n° 11 [our translation].

The purpose principle results from an approach that sought mainly to punish misuse after the fact. It was supposed to be employed once information had been used and questions had arisen about whether the use was indeed consistent with the purposes for which the information had been gathered. The principle has been turned into a rule that applies *a priori*, even to information that is public.

Yet, the purpose principle makes no sense unless it is used to assess whether information has been misused. Underlying the prohibition on changing purposes, there is a concern to prevent significant, harmful changes in the way information is used. In a centralized electronic environment where users do not have access, there has to be a way to ensure that ambiguous information is not used in decision-making. What is problematic in the use of information for new purposes is the risk that it is not appropriate for those purposes. Because there is no will to promote means to guarantee that the information used to make decisions concerning an individual is accurate, we have ended up prohibiting changes in the purpose.

Given the danger that information used for decision-making could be inaccurate, we have to consider strengthening mechanisms designed to ensure information quality rather than simply preventing its circulation. Controlling the purpose should therefore be seen as controlling quality. Every time a piece of information is used, it should be checked in relation to the decisions for which it is to be used. In many cases, this could be done by showing the information to the person and having him or her confirm or correct it.

However, rather than promoting the development of requirements that would improve data accuracy, regulators often automatically look to consent, which is a procedure that tends to excuse decision-makers from having to try to ensure information is of high quality.

3. Automatic Use of Consent as a Remedy for Inflexibility

Contortions and artifice are required to reconcile the classical conception of personal data protection with real operation of electronic environments. The most obvious contortions include those flowing from "free and informed consent" practices.

In Québec, the Commission makes disclosure of personal information dependent on clear, free, informed consent given by an individual for specific purposes. Yet the legislation on data protection in the public sector requires authorization, which could be implicit or simply follow from the context. The consent requirement and its accompanying red tape have become a basic requirement in the personal data management cycle. The perverse effect of this kind of slide is a focus on obtaining and managing consent rather than on effective privacy protection.

The obligation to obtain consent was originally designed to provide controls over the right to perform medical operations. When it was imported into the field of personal data protection, the procedure introduced discipline that was originally designed to control actions that could have infinitely more drastic consequences. The requirement about free, informed, unambiguous, written consent is quite understandable when an individual's physical integrity is in question. Is it appropriate for information transfers, many of which are in the individual's interest?

The consent requirement has led to a dysfunction that is particularly noticeable with respect to the circulation of information in networks. In order to circumvent the difficulties resulting from the excessively all-encompassing notion of personal data, practices have arisen based on a veritable mythology of "free and informed" consent. We have to wonder whether the resources allocated to managing consent would not be better invested in tighter risk-based management of personal information.

In France, the CNIL has identified the misunderstandings that dependency on consent could introduce into information management by public bodies. In 2001, in its 22nd operational report, the Commission wrote: "Does not promoting consent risk encouraging the belief that every individual is free not to appear on a tax roll, in police records or in government files? This would be to mislead our fellow citizens about their rights and perhaps the essential nature of the social links that require us to reconcile private life and other values of general interest…" The CNIL added that "inversely, could promoting consent not lead to the elimination

of guarantees that are in the public interest based on the fact that the individuals concerned have not given their consent?"[19]

These deviations related to the notion of consent reveal that sight has often been lost of the reason for protection of personal data. From the goal of protecting privacy, we have gone to that of acting on an individual's more or less mythical "veto" over information concerning him or her. Consent began as a means of ensuring that individuals had the control necessary over their private lives, but it has become an end in itself, even though it has to be altered or disguised in order to circumvent the inflexibility resulting from an excessively all-encompassing conception of personal data protection. For example, on the Internet, users are asked to "consent" to all sorts of uses in contracts that no one ever takes the time or has the courage to read. Data protection law has been boiled down to a simple obligation to require the user to click on a button. This shows the ineffectiveness of this formal approach, which is based on so-called free and informed consent.

4. Mushrooming Legal Exceptions

Inflexible enforcement of personal data protection regulations and excessive extension of some notions have destroyed the balance. This is probably why legislators have increasingly been obliged to pass acts in order to re-establish lost equilibrium in personal data protection. Herbert Burkert notes that in a number of countries, many acts establishing exceptions have sprung up to re-establish balance in specific areas. He writes that

> One has only to look at the pieces of legislation passed since the first personal data protection acts in order to see that many of them target specific sectors. Not all of them take the form of special laws. Some are simple amendments or appendices. The legislation, particularly that concerning

---

[19] Commission nationale de l'informatique et des libertés, *22e rapport d'activités 2001*, Paris, La documentation française, 2002, p. 108 and 109, < http://www.ladocumentationfrancaise.fr/BRP/024000377/0000.pdf > [our translation].

> the processing of data held by the public sector, has overall limited the scope of general principles in the area by introducing what has been seen as a compromise between respect for privacy and the requirements of public interest. While it is true that individuals want their privacy protected, they are quick to forgo it when they have to choose between confidentiality and social or public security.[20]

This tendency to pass many pieces of legislation so as to adjust personal data protection to the sector is an indication that the general mechanisms are inappropriate. The general legal framework of the protection is too inflexible, or perceived as such, to accommodate other requirements. As an illustration of the scope of the aberration, note that in Québec, legislation was adopted to allow information to circulate in order to permit prevention of suicide and other violent acts against identifiable individuals.[21] The legislation added section 59.1 to the Act on Access, which provides:

> A public body may also release nominative information, without the consent of the persons concerned, in order to prevent an act of violence, including suicide, where there is reasonable cause to believe that there is an imminent danger of death or serious bodily injury to a person or an identifiable group of persons.

The fact that we have had to resort to such a solution in order to make legally possible what would have been, under a reasonable, sophisticated interpretation of the legislation, a legitimate reason to give access to personal information shows the inflexibility of conceptions of personal data protection. Until the amendment was passed, personal data

---

[20] Herbert BURKERT, « Progrès technologiques, protection de la vie privée et responsabilité politique, 89 *Revue française d'administration publique*, janvier-mars 1999, pp. 119-129, p. 125 [our translation].

[21] *An Act to amend various legislative provisions as regards the disclosure of confidential information to protect individuals*, S.Q., 2001, c. 78. < http:// publicationsduquebec.gouv.qc.ca/fr/cgi/telecharge.cgi/180F0206.PDF?table=gazette _pdf&doc=180F0206.PDF&gazette=4&fichier=180F0206.PDF >

protection was read so as to give protection for information about an individual priority over protection for his or her life!

II. Means of Strengthening Privacy Protection in Networks

Given the deficiencies of personal data protection legislation, we need to identify means of meeting contemporary requirements for better circulation of information while strengthening the level of privacy protection for individuals. Mechanisms for protecting the rights of individuals have to be reinforced in order to provide effective privacy protection. This has to be carried out in a way that provides both real protection for human dignity and free circulation of information belonging to the public forum.

Faster circulation of information and the resulting consequences require appropriate adjustments to normative frameworks. The instantaneous nature of networked activities is increasingly in conflict with the stability and conformity so dear to some bureaucracies. Normative frameworks have to reflect the speed at which information travels; norms that freeze information under the pretext of protecting it will not work.

The spread of information-sharing platforms makes information exchange and publishing available to all. With respect to information held by government, the legal framework should focus on controlling the conditions for access by individual government officials rather than trying to prohibit circulation. In this context, what is important is not to know whether the government has the right to hold a piece of information, but rather whether the government has the right to access and use it to make a decision in a specific situation.

A. An Updated Reading of the Principles of Personal Data Protection

In a networked world, an essential aspect of information is that it circulates. It has to be available when needed to deliver services. The foundations of personal data protection have to be refocused on the increased speed resulting from digital networks and other information environments.

The basic principles of personal data protection legislation underlie the structure of international personal data protection instruments, such as the *OECD Guidelines*,[22] the *European Convention* and the *European Commission Directive*, as well as the legislation in many countries.[23]

In a networked environment, the need to gather information has to be seen in relation to all of the families of services concerned by the information. Once the information has been gathered, the need to retain it has to be assessed with respect to a set of decision processes. The retention principle and the purpose principle are linked. The principle according to which purposes have to be specified is thus strengthened. By specifying purposes as strictly as possible, the information gathered will be limited to what is really indispensable for the purposes of the set of services to be delivered using the network.

The rule preventing circulation and re-use of information, which is based on the argument that the information could be used for purposes other than those for which it was gathered, has to be reconsidered given the increased dialogue made possible by networks. More than ever, government is in a position to tell every individual what information it holds on him or her and what information it intends to use to make a decision. Individuals are now able to interact and demand the withdrawal or addition of information.

The spread of networks requires that we assess the need for information with respect to all of the situations concerned by the information environment in question. Naturally, the need will always have to be evaluated with respect to the legitimacy of information collection and holding, as under current principles. However, we have to ensure that specific decision processes employ only relevant and authorized information. This means that we have to separate assessment of the need to hold information from assessment of the need to access it for a specific decision or service.

---

22 OECD, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, Paris, OECD, 2002, <http://www.oecd.org/document/18/0,2340,en_2649_201185_1815186_1_1_1_1,00.html >.

23 R.S.Q., c. P-39.1.

Limits on collection suppose the establishment of decision processes that use as little personal information as possible in order to deliver services or make decisions. There has to be clear justification for the collection of every personal datum.

The purpose principle says that personal information may be gathered and used only for purposes consistent with those of the initial collection. The purpose principle is related to maintenance of information accuracy. The OECD Guidelines express this requirement as follows:

> Personal data should be relevant to the purposes for which they are used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.[24]

In a networked environment, the question of purposes requires taking into account the fact that the information may already be gathered and available. Compliance with purpose no longer concerns holding but access to and use of information. In a network, the principle of control at the level of access authorization ensures compliance with purposes. Access to information is permitted only for authorized purposes and when one is performing an activity in order to achieve such a purpose.

Compliance with the purpose principle supposes that the user is indeed informed about the families of purposes for which the information will be used. Information on the purposes for which data are held must be available at all times and brought to the attention of users every time data is gathered. In order to comply with limits on use, information environments should be employed for well-defined families of services. This ensures that personal information will be used for purposes related to and compatible with the purposes of the initial collection.

Transparency is an essential condition for credibility and trust in networked environments. Users have to be able to know with whom they are dealing and how the information process is designed. In this respect, it is of greater importance to have public audits of information environments

---

[24] OECD, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, Paris, OECD, 2002, <http:// www.oecd.org/document/18/0,2340,en_2649_201185_1815186_1_1_1_1,00.html >.

and information sharing for electronic service delivery. The stakes and risks associated with networked electronic services have to be publicly disclosed, debated and assessed.

Quality of information has to be evaluated in terms of the services to be delivered using the information. There has to be a guarantee that the information used to deliver a given service is correct, accurate, unambiguous and legally authorized. The legitimacy of circulation of personal information is strengthened when the individual concerned is able to review and correct personal information online or otherwise. The right to correction, which has until now been used very little, would then become truly meaningful.

Since personal data are available on networks, the legal framework has to require service deliverers to ensure that the information they use to perform a service concerning an individual is of suitable quality for the service requirements and context. The direct dialogue potential of network technologies needs to be exploited to ensure quality.

In this respect, the principle of individual participation of the person concerned in decisions relating to the processing of personal information in networks has greater scope. In networks, it is possible to present the information held and validate it in real time with the person concerned. The guarantee that the data is accurate can also be strengthened when an organization validates information as it delivers a specific service.

> ☞ With respect to responsibility, every entity able to access personal data on a network can be considered the legal holder. This makes every such entity responsible for confidentiality. In this respect, it is important to delimit management duties and responsibilities with respect to confidentiality and security. Indeed, the norms that will be used to assess the behaviour and responsibility of both individuals and managers must be specified.

Both physical and technological security measures are obviously essential requirements for every networked environment. The legal framework has to require those in charge to take measures to ensure the security of information on individuals. In addition to a culture of security, there has to be a set of procedures able to prevent attacks and especially to provide remedies when information processing is in danger.

B. The Need for Trust

User/citizens have to trust every step in the information processing cycle. Processing has to be completely transparent. Trust is built by informing users about what happens to the information they entrust to the government. The more sensitive the information, the greater the precautions required to guarantee the appropriate level of trust. When guarantees are given, appropriate measures absolutely have to be established to ensure compliance.

> Establishment of a network environment should flow from public assessment of the stakes and risks. In order to obtain the legitimacy and trust essential to render circulation of personal data acceptable, all stakes and fears have to be taken into consideration. Questions from individuals have to be answered.

Christine Noiville says that decision-making with respect to phenomena that entail risk to the community has to have explanatory and deliberative components. She writes:

> Let's not forget: no risk is acceptable in itself. It becomes so through the prism of debate, which makes it legitimate. Acceptability is not an essence that imposes itself on an individual faced with risk. [...] Thus, since "acceptable risk" is not a given but the result of assessment that is always renewed, the meaning that it should be given must be negotiated as much as possible.[25]

The establishment of information environments in which personal information is processed involves stakes similar to those that arise when the environmental impact of a project is assessed. Concern is expressed about precautions taken, unforeseen consequences and specific problems that some people might experience. There is a desire to be reassured with

---

[25] Christine NOIVILLE, *Du bon gouvernement des risques*, Paris, PUF, "Les voies du droit," 2003, p. 120.

respect to the precautions, impact analysis and controls designed to prevent problems.

Yet, public bodies promoting projects anticipate such concerns and try to design services that ensure a high level of protection. The public process makes it possible to inform the public about the precautions. It permits informed debate on future choices and critical assessment of past choices.

C. The Right to Technology Compatible with Privacy Protection

Effective privacy protection requires the development of a right to technological environments that increase rather than diminish privacy protection. Public decision-makers and private enterprises could be required to demonstrate that the technology they use meets minimum privacy protection requirements. This would require taking legal aspects into account when planning the introduction of technologies. This is not always done. Very often, information environments are developed with no concern for legal aspects and then presented as a kind of inevitable situation to which we have to adapt. If there is an area where law should play a bigger role, it is with respect to requirements on the development of information environments.

Security does not automatically equal privacy protection. It is easy to agree that privacy protection supposes that information and systems have features ensuring the physical and technological security of information. However, privacy protection requires mechanisms that go far beyond what is required to make an information system or network secure.

Use of information technologies changes the scale of the risks associated with circulation of information. This requires assessing risks, but not basing the required level of protection on the worst-case scenario. Those who set up technology-based environments should be required to demonstrate that such environments comply with respect for private life understood as a means of protecting human dignity. In particular, there is no reason for individuals to have to shoulder the burden and protect their own privacy. The duty to protect individuals' privacy is easier to bear at the level of implementation and deployment of environments. This is particularly true in environments designed to serve the public.

However, this requires establishing a consistent process for assessing systems ahead of time. Such assessment should not be based on catastrophic scenarios but should instead be designed to check whether choices have been made so as to comply with rules stated in recognized principles. Later, if situations arise that violate privacy, there should be an inquiry to document problems and prescribe corrections to prevent them from happening again.

D. Control of Personal Data

Protection of privacy and personal information supposes that individuals have an acknowledged right to exercise some control over information concerning them. However, the right to control has never been and cannot be absolute. Lucas, Devèze and Frayssinet note that "there is no social life without exchanges of personal data." They add that "an individual is not only a physical and psychological being but also an informational being…" We therefore have to come to a consensus on the principle's limits when we state it. The Truche report points out that "the principle of control over personal data cannot be stated in absolute terms."[26] The CNIL also has reservations about a right to control over personal data, and calls attention to the fact that what is essential is that data be accurate. The CNIL's 22nd activity report contains the following:

> However, we can argue that the reason that the right to access is rarely exercised is because in the end what is essential for our fellow citizens is not so much to check the content of data that in most cases they themselves have provided to the government department in question, but to have the guarantee that the data will not be used for something other than the initial purpose, needlessly

---

[26] Pierre TRUCHE, Jean-Paul FAUGERE and Patrice FLICHY, *Administration électronique et protection des données personnelles livre blanc,* Rapport au ministre de la fonction publique et de la réforme de l'État, Paris, La documentation française, 2002, p. 77 < http://www.ladocumentationfrancaise.fr/brp/notices/024000100.shtml > [our translation].

> disclosed to third parties, or used against them many years later.[27]

The right to control data can be seen as an *a priori* right, but it can also be exercised *a posteriori* if information has been used inappropriately and this has to be corrected. Thus, an *a priori* right to control can be exercised by an individual over all personal information held about him or her. It should be possible to have rapid access to information so as to request corrections. One should also always be able to ensure the quality of information used to make decisions concerning oneself. By being guaranteed a right to access and validate information concerning a transaction or decision, individuals are given constant, targeted control over their personal data. This requirement also increases the incentive to keep only the information that is necessary and establish means of quality control.

E. Quality Requirements

In a world where information will circulate more, the challenge is to ensure that it will be of appropriate quality for every use. Circulation of information has to be conditioned with guarantees concerning information quality. Quality is a component of the trust that necessarily has to exist between users and government. If users are not certain that everything is being done to ensure that decisions are being made based on information that is as accurate as possible, they will not trust the government. Thus, we should focus on establishing effective regulation of personal data rather than trying to expand the scope of application of legislation, even with respect to public data.

Legislation intervenes to identify the quality of information to be used. Individuals concerned are thus given a right to access and correct information about themselves. In one of the rare attempts to assess effectiveness of application of the French legislation on information technology and freedoms, Valérie Sédallian says that she went from surprise to surprise as she discovered the carelessness of a number of

---

[27] COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS, *22e rapport d'activités 2001*, Paris, La documentation française, 2002, p. 108, < http://www.ladocumentationfrancaise.fr/BRP/024000377/0000.pdf > [our translation]

holders of public data with respect to data security and especially effective exercise of the right to access and correction.[28]

In a number of situations, information quality can be assessed in accordance with the context. A piece of information might be appropriate for one purpose but clearly inadequate, or even inappropriate, for another. With respect to network interactions, it is possible to assess, in cooperation with the person concerned, whether the information meets the quality requirements of the decision in question. By strengthening provisions prohibiting the use of certain kinds of information for making certain kinds of decisions, we can reduce the tendency to employ irrelevant or inaccurate data to make decisions concerning users of public or private services.

Access and correction, two rights that are rarely exercised, need to be updated. If real, effective recourse were made available to individuals, invading privacy would become more risky and less profitable. Instead, we remain complacent in respectable good cheer, seeking to settle complaints amicably. For example, in Québec, the Commission responsible for enforcing the legislation on personal data in the private sector has never found it appropriate to take criminal action against companies that sell credit information. Yet, dozens of complaints are filed against such companies every year, and consumers with the stomach for it have to seek civil remedies in order to be compensated for harm caused by the circulation of inaccurate credit information.

In sum, by taking data quality requirements seriously instead of exhausting ourselves trying to prevent circulation, we would greatly improve privacy protection. This supposes appropriate enforcement mechanisms.

F. Effective Enforcement Mechanisms

Some information about individuals is important for other people. For example, some public information needs to be consulted in order to

---

[28] Valérie SÉDALLIAN, "La loi Informatique et Libertés vue par la 'France d'en bas' ou le récit de Candide au pays des merveilles," < http://www.juriscom.net/pro/visu.php?ID=79 >.

make informed decisions. The simple fact that such information could be misused should not lead us to censure it as a preventive measure. Instead, we should have effective penalties to punish misuse if it occurs. This would avoid preventive censure of data and provide dissuasive sanctions for misuse. If we do not adopt this approach, we could find ourselves in a world where there are no more archives or information available on individuals.

The effectiveness of privacy protection depends on the possibility of real recourse if the legislation is violated. Yves Poullet describes the principle as follows:

> …just as the Internet makes it easier for electronic communications service providers to gather and process data, such providers should allow users to take advantage of the medium to exercise their rights more easily.[29]

This means using electronic environments to ensure effective exercise of individual rights. Yves Poullet explains how this concept could help to ensure more effective application of the right to privacy:

> …an individual's right could be exercised more easily by simply clicking on an icon providing direct access to a privacy statement. […] The person concerned could exercise his or her right to give or refuse consent directly online. With respect to the right to access properly speaking, in other words, the right to know what data is held, where it comes from, how it is processed, etc. […] one could even imagine that there could be an online request that could be signed electronically. Finally, concerning the right to challenge the relevance or quality of data […] why not allow it to be exercised, and resolve disputes using electronic court referral and dispute resolution mechanisms?[30]

---

[29] Yves POULLET "Internet et vie privée : entre risques et espoirs," (2001) 120 *Journal des tribunaux* 155 [our translation].

[30] Yves POULLET "Internet et vie privée : entre risques et espoirs," (2001) 120 *Journal des tribunaux* 155 [our translation].

The spread of network activities has to be accompanied by the establishment of appropriate tools, preferably situated within such environments themselves in order to ensure effective exercise of human rights. It is difficult to see how it would be possible to maintain a judicial or quasi-judicial process operating at a snail's pace when transactions are performed at light speed.

Conclusion

We have been discussing the challenge of amending the normative framework of privacy protection to make it more effective in network environments. Lucas, Devèze and Frayssinet note that:

> It is between paranoid discourse that sees Big Brother everywhere and soothing or self-interested discourse that refuses to see the reality and potential of today's technology that we have to situate reasoned analysis of the threats to human rights and freedoms created by new information and communications technologies.[31]

We have to acknowledge the changes that the spread of network environments create in production and circulation of information. The changes require the establishment of an effective framework to protect individuals' rights. We cannot protect privacy effectively by leaving in place a legal framework that blocks circulation. On the contrary, we have to refocus the legal framework for information on individuals so as to protect privacy effectively in the wide range of network contexts.

It is dangerous to develop legislation concerning network environments based on approaches that posit the supremacy of privacy rights without regard for the exercise of other rights. Such approaches can result in legislation that is not consistent with democratic principles. They exclude reflection on means to ensure effective privacy protection. We need to calmly assess means of ensuring balanced protection both for the

---

[31] André LUCAS, Jean DEVEZE and Jean FRAYSINNET, *Droit de l'informatique et de l'Internet*, Paris PUF coll. Thémis n° 7 [our translation].

privacy of individuals living in society and for other values that also protect human dignity.

Effective modernization of personal data protection law requires a critical rereading of how it has been implemented and a lucid evaluation of the contexts in which information circulates. Seeking fearful refuge in approaches inherited from earlier times will only weaken personal data protection because it increases the risk of ending up with purely formal protection that would be ineffective in dealing with the real dangers.

The spread of network environments leaves us with little choice. It is becoming increasingly urgent to adopt privacy protection that reflects the whole complexity of cyberspace. This requires acknowledging that information on individuals has never been and cannot be separated from the general environment in which people live. This is how we have to envisage modernization of privacy protection in a networked world.