

Looking Beyond Privacy

Pierrôt Péladeau (*)

"Nothing was easier to destroy than the intimacy and private morality of people whose only concern was protecting their privacy."

Hannah Arendt, The Origins of Totalitarianism

1. Introduction

This article is an adaptation for Lex Electronica of a scientific popularization text. (1)

It discusses the concept of privacy: is it still as an appropriate one to provide a comprehensive understanding of issues related to the use of personal information systems?

Privacy is a fundamental concept, particularly in our western societies. Our modern concepts of the State, of law, and of society itself, are evolving out of a search for a balance between autonomy (self-determination) and its opposite, heteronomy (external determination). During the last hundred year, the right to privacy has emerged in this discussion as one of the key concepts whenever the debate bears on the extent of individual autonomy in society. In the late 60's, Alan F. Westin provided us with a seminal definition of privacy as the desire of persons to chose freely under what circumstances and to what extent they will expose themselves, their attitudes, and their behavior to others. Among the most recents definitions is the one proposed in the mid 90's by Rohan Samarajiva. More generic, it refers to the hability of individuals to control boundary conditions of social interactions.

The post World War II era was marked by fear of totalitarianism and of the fastly growing capabilities of computer that could be used for surveillance purposes. One of the answer was to call for personal information protection legislation. This call was successfully followed in numerous western countries where such legislation was adopted. In fact, it as been so successful that, today, among many jurists, management consultants, "privacy coordinators" within organizations, government technocrats and even academics, the term *privacy* is now equated only to the application of personal information protection principles and law, if not only to matters related to confidentiality and security. This significant shift of meaning has many causes. This could be the subject of another article altogether. One can point to shear ignorance, the weight of legal institutions in shaping both professional and public discourses, the fact that what was mostly the turf of academics and political activists h as been transformed by the entry of the new players mentionned above, the fact that a restricted definition is useful in keeping at bay discussions of more political issues related to extensive uses of personal information.

The problem is that the branches of confidentiality and personal information protection are now hiding the magnificent tree of privacy, which in turn hides the forest of all the social implications of the use of personal information in this age of the infohighways. A radical shift in perspective would permit to envision the

numerous and complex issues at stake, and thus help privacy to re-emerge as one central concern. This perspective would as well as provide a better understanding of the proper place and role of personal information protection and confidentiality.

2. The perspective of average citizens

When discussing concepts, it is always useful to start with the laypersons' use of them. While citizens are largely concerned about privacy, they do not equate this term with only confidentiality or personal information protection related matters. Significantly, those citizens who are struggling with a poorly designed or intrusive applications of computer technology rarely use the expression "invasion of my privacy". Those who contacted me personally or filed a complaint to a consumers' association, the Ombudsman office or even to one of the privacy commissions, speak instead of a loss of control over their lives, of a bureaucratic nightmare or nonsense or abuse of authority. The following three examples illustrate why they react in this manner.

In March 1997, a woman was fighting with the former supplier of her internet service. Months ago, she had switched suppliers. However, the ex-supplier's computer continued to debit monthly the woman's credit card for the amount of the subscription. By mistake, her file was erased when service to her was discontinued. However, some information in the erased file was necessary in order to deactivate the billing. "It's not our fault, it's the computer" was the explanation repeatedly given the ex-subscriber. It took months of exchanges by telephone, internet and finally by letter before the supplier finally decided to involve a computer analyst, who deactivated the expired account by circumventing the programmed procedure. Did the woman complain about her privacy being invaded? No. She spoke instead of a sudden feeling of extreme dependence and vulnerability vis-à-vis all these machines and these systems that were supposed to be at her service.

In the fall of 1994, a new system for managing subsidies to parents with children in day care was launched. This new system "on the leading edge of technology" replaced another already existing system. However, the transition was botched. The result was an indescribable mix-up of files. The government then had to assign a group of civil servants to reconstitute and process the files manually (their regular duties suffering as a result). Parents and day care centres had to be asked to review each piece of information. A decision that normally took three weeks at most now took a minimum of six months. Many parents were unwilling or unable to wait. They therefore decided not to enrol their child in day care, a decision that in many cases had negative consequences. For some parents, it even meant having to quit work. Many other parents, who took the chance of subscribing to the service anyway, ended up being denied the subsidy several months later. They therefore accumulated a significant debt that they could not easily repay. Before long, Government had to subsidize the struggling day care centres that had lost the clientele consisting of the parents who had not enrolled their children, and had to deal with the unpaid debts of many parents who had. A real computer mini-Tchernobyl in the management of personal information! However, while the complaints were legion, as one can well imagine, no one said anything about his or her privacy being invaded.

One fine spring day in 1988, a large financial institution launched a new system to facilitate access by its customers to sums deposited through automated banking machines and inter-branch banking. Until then, these deposits were "frozen" by the institution for a few days (the time required to complete "clearance", to use the terminology of banking). The new system provided instant access to money according to a points system based on a standard customer profile. Unfortunately, the new system had been poorly designed. The base profile was that of a person all of whose assets and loans were held by a single branch of a single institution. It had not occurred to the system's designers that only a very small percentage of customers fit

this ideal profile. Thus, for ten of thousands of customers, the result was the exact opposite of what was intended. For several days, individuals were denied access to funds deposited, even pay cheques and income tax refunds personally deposited at the counter of their own branch. For their part, many businesses suddenly found themselves unable to pay their employees or their suppliers. Flooded with complaints and account closings as customers switched to competitors, the financial institution halted the operation of this system that had taken years to develop. Customers complained of discrimination, loss of control over their own money, abuse of authority, bureaucratic nonsense and management based on false information. But what about invasion of their privacy? Not a word.

The vast majority of Canadians have, some day, experienced incidents like these. This is the finding of an extensive opinion survey conducted in 1995.²

At one time or another, they have also been the object of the unnecessary collection of personal information, the coupling or communication of personal records and a solicitation for business or charitable purposes following the exchange or sale of their name, address and telephone number. But even there, it should be noted that they do not themselves characterize such activity as "invasion of privacy" as spontaneously as do reporters, lawyers and other experts. Their use citizens make of the term privacy is closer to the definition provided by the Westin and the Samarajiva. So, incidents like breaches of confidentiality or of fair information principles as well as other negative impacts of misuses of personal information would not necessarily fall under the concept of privacy.

In short, there is a distance between the perception of laypersons and the one of specialists. It could be argued that the former are more in touch with reality.

3. Some realities of the uses of personal information

3.1 The Weight of Information in Daily Lives

This is a truism: more and more personal information is being collected about individuals. This information is increasingly used in transactions (electronic or not) in which individuals are participants. This information is also being used to make more and more decisions about people, individually or collectively.

Some individual decisions are regarded as important: admission to a program of study; hiring or firing; securing a mortgage or assistance from a social security program. An even larger number of decisions are regarded almost with indifference: authorization of a credit card transaction; identification as the target of a direct advertising campaign.

Collective decisions taken using information on us are less obvious. However, they have just as great an impact on human lives. For example, certain information in one's medical record may be compiled along with that on thousands of others. These statistics will be used to justify the opening or closing of clinics or hospitals, the establishment or dismantling of a particular health or social services program, the hiring or transfer of a particular category of professionals.

The development of the information highways will only accelerate the production of personal information and its use in transactions or decision making. And the average citizens do not seem to think that, in itself, this considerable increase in collection of personal information can be equated to an invasion of privacy.

3.2 The Weight of Machines

It is often stated "Computers know everything about us". Wrong. Computers know nothing. They are totally indifferent to the information they store and process, as well as to the consequences of the operations they perform, correctly or incorrectly (see our three earlier anecdotes). A distinction must be made between information and knowledge. The term "information" can be used to describe very different realities. The definition that we use here describes information as writing, i.e., a material object that can support knowledge. This object, this writing, may have various forms (words, sounds, images) or storage media (paper, tape recording, silicon chip). Machines can also be designed to manipulate these objects. But even today, it is still only in the mind of an animal (particularly the mind of higher primates) that this object can evoke or generate "knowledge". It is this distinction that is illustrated by the following two replies based on incidents that occur from time to time:

A civil servant: "Sir, I know that the fact that you have not received a retirement pension cheque for several months is making life difficult for you [knowledge]. Unfortunately, since this inadvertent coupling of records [information], you have been declared dead [information]. Administratively, I have to prove that you are still alive" [information].

A school principal: "Madam, I can clearly see that your child definitely is old enough to attend school [knowledge]. Unfortunately, since she has never been issued a birth certificate [information], she does not exist in the eyes of the law [information]. I am not therefore able at this time to enrol her in school [information]."

The power of computers and telecommunications systems lies in their ability to manipulate rapidly, systematically and efficiently material objects called "informations". Some of these informations concern individuals. These informations form files that constitute material doubles of individuals. These informational doubles are used in making various decisions. Some regard as pure and simple "invasion of privacy" the fact that the credit agency computer "knows" a lot about their different places of residence, their jobs, their income, their debts, their late payments, their marital history, their criminal records, etc. This, however, is merely the accumulation of objects in the entrails of a computer that has no intelligence. However, it becomes a real concern as soon as this information is communicated - specifically to banks, employers, merchants or landlords who will use these informational doubles of individuals to make a decision that will affect individuals to a greater or lesser degree.

The issue is therefore much more about control of the individuals over their informational doubles, and hence over the decision-making process that affects their own lives. This problem did not just appear with the invention of the computer. It has existed since the invention of writing some 6000 years ago. More specifically, with the development of the bureaucracy which followed. The difference is that operations that used to require an army of bureaucrats can now be performed by a single computer (which has no understanding of what it is doing), and that today, the good idea or error of a single bureaucrat or technician can affect the lives of ten of thousands, indeed millions, of humans at a single stroke.

This could explain why the issue of control over personal information was so important to the respondents of the 1995 survey. Their responses showed that they do tend to equate privacy to one's ability to control the use of personal information about oneself, rather than to matters of confidentiality or the applications of the principles of protection of personal information.

3.3 The Materialization of Social Transactions

Hardly a week goes by without the media reporting the statements of some expert or guru in economics, law, sociology or the information technologies holding forth on the effects of the "dematerialization of the economy" or of the "culture of the immaterial" which is supposed to be a consequence of the development of the information highways. These preconceived notions are so divorced from reality that we must seriously ask ourselves whether such talk is not rooted squarely in ideology. On the contrary, what we are witnessing is an unprecedented materialization of social transactions.

The new information and communications technologies exist solely because of the possibility of manipulating material objects. Electrons, protons and magnetized molecules are infinitely small and hard to distinguish to be sure, but no less material and capable of being manipulated than the beads on a Chinese abacus or the gears of a pendulum clock. The development of the information highways is therefore contributing to a materialization of social transactions. Identifying self, authenticating our identity, exchanging knowledge, money or goods, concluding agreements, exchanging our consents and voting are all transactions for which technicians will have to design new rituals and the material mechanisms through which these transactions can be performed. We are entering an age of the efficient norm. A statute or a regulation may very well gather dust on a shelf without having any concrete effect. However, no one can ignore the rule incorporated in an information system with which we have to deal.

One example is the development of the electronic medical file. There already exist numerous visions of this file that are being developed and that will soon be a reality. One such vision, the "intelligent virtual file", could be described as follows. John Smith goes to see his doctor, Mary Jones. At one point, Dr. Jones has to prescribe a medication for her patient. She must satisfy herself that there is no contraindication. She therefore makes a request by computer to a "computer agent" who in turn transmits an inquiry by Internet to all the computers of health care professionals around the world. There are perhaps more than 100 pages of information archived on John Smith, which would take too long to read, especially when a doctor is paid on a fee-for-service basis. That is why all the computer agents of all the computers concerned will work among themselves to identify the few lines of information that really pertain to the prescription (other prescriptions, illnesses or conditions that could be contraindicated). As a final step, Dr. Jones' computer agent will convert all this information to an appropriate format so that she can make her decision concerning a prescription quickly and efficiently. Just like that! You can now applaud.

This is how the "intelligent virtual file" now being developed will facilitate the circulation of medical information on the information highways. Paradoxically, however, this application is possible only if there are multiple constraints on communication. In this case, in order to allow access to health professionals around the world, access must also be denied to everyone else. In this application, the computer agents will have to apply a whole series of rules like the following: only a particular type of professional can have access to a particular type of information only on a particular type of person only for a particular type of decision, and so on. Once adopted, each of these rules will be applied all together, automatically, by tens of thousands

of programmed machines. But who will determine what are the rules? John Smith? Dr. Jones? The other professionals whom John Smith consults? The medical corporations? An anonymous standardization committee? The Legislator? An international organization (to the extent there will be transborder data flow)? The company that develops the application? This question is central to most of the personal information highways applications. A question which goes far beyond the issues of confidentiality and protection of personal information. It goes even beyond privacy itself.

There is little room for error. Because once certain rules are built into the infrastructures, the chips and the machines, any change can quickly become costly. Take, for example, the recent case of Pharmanet in British Columbia. This is a small application designed to allow any pharmacist to access files held by other pharmacists in the province. Here too the objective is to avoid problems resulting from overmedication or interaction of medications. However, consideration was not given in time to addressing the concerns of many customers that certain information on the prescriptions not be allowed to circulate freely between pharmacies. Two of the obvious cases that come to mind are AIDS patients and those with some mental illness. The introduction of a customer card with a personal identification number could have been a way of exercising this control. However, since it was considered too costly to change the infrastructure in place, it was decided instead to fix the problem with a optional blocking mechanism that limits access to information to a single pharmacist chosen by the customer. However, installation of this mechanism is so laborious that the province's pharmacists have been handed an argument for dissuading customers from taking advantage of this service. . .

The focus on personal information protection and confidentiality is leaving the citizens clueless about the changes in the making. And the fatalist discourse about dematerialization is leaving them powerless. They do are feeling more and more so, as surveys show.

4. An alternative vision

4.1 Political Choices by Design

"The purpose of computer technology is social organization", to quote André Vitalis.³

Informational infrastructures materialize communications between organizations and individuals. They regulates relations between them. They permit certain controls and excludes others. The technical choices are in fact political choices.

As development of the information highways technologies proceeds, the political nature of the technical choice becomes more apparent. We are no longer in the sixties where the only model available was the large, centralized computer. Today, information processing capacity is widely available in many forms: microcomputers, computerized equipment, and even wallet-sized smart cards. Networks allow all these machines to communicate and work among themselves. Software engineering and cryptography can today create very diverse applications.

Thus, a single user card can be designed either to give the State or a corporation complete control over the individual or, conversely, to enable the individual to control the work of public and private bureaucracies alike. For example, it could become practically impossible to transfer information from the credit agency and

from bank A to bank B for a credit analysis of an individual without this individual first authorizing this transaction by inserting his or her card in an automated machine and entering his or her personal identification number. The obligation to obtain prior consent to the communication would then be given material form through a computer procedure that would be relatively difficult to circumvent. The same applies to electronic payments. Today it is possible to design payment systems yielding a lot of information that would provide a bank with a large number of details on each of an individual's transactions. It is equally possible to design an anonymous and secure payment system that would yield as little information as payment in cash.

The range of possibilities is constantly expanding with each new technical or software development. But, again, if there are choices to be made, who is to make them, and on the basis of what criteria?

4.2 Human rights as Criteria

In a number of societies, human rights and fundamental freedoms continue to be fundamental, immutable values that define choices of a social nature. This is true even though, of course, we must also take into account a set of other values more economic, social, legal and ethical in nature.

However, once the possibilities that the information highways offer are clearly understood, it seems clear that the relevant human rights values cannot be limited solely to respect for privacy and freedom of expression, even if they are the two most often referred concepts in such discussions.

In fact, if we consider only the possible use of personal information in various decision-making processes that could affect our personal lives, there are more than 150 concepts of human rights and freedoms that may come into play: the right to equality, to health, to education, to work, to the peaceful enjoyment of one's property, freedom of movement, etc.

Moreover, if we consider all the new information infrastructures being developed and its multiple applications other than for individual decision-making, then almost all the concepts of fundamental rights and freedoms come into play. For a clearer understanding, let us abandon for a minute the metaphor of the information highway in favour of another metaphor that relies on the notion of social space. Rohan Samarajiva of Ohio State University proposes in particular exploring the metaphor of the classical agora. We can explore this metaphor to explore the human rights dimensions.

The classical agora was first the marketplace, the site where goods and services were exchanged. It is very clear today that commerce will become a dominant feature of the information highways. The proper operation of a market involves not only the freedom of vendors to sell their goods and the freedom of choice of buyers, but also the preservation of the independence of individuals and the right to information without which the market cannot function properly.

The classical agora was also the centre of communication and exchange of news, information and ideas. The telephone, radio, television and now the Internet fulfil this function of facilitating communication between individuals and groups. It is not surprising that concepts such as freedom of expression assumed such importance in this context.

The classical agora, however, also could serve as a democratic forum and a judicial forum. The Internet is already complementing these roles and itself permits gatherings of individuals for collective debate and decision making. The metaphor of the agora thus evokes a completely different set of fundamental rights of the individual as citizen (the right to equality, the right of access to information, freedom of opinion) but also civil and political rights (e.g. the right to vote, the right to run for public office) and judicial rights (the presumption of innocence, the right to an impartial hearing by an independent court). This introduces the discussion of rights and freedoms of a more collective significance.

Finally, the agora was the place to simply "hang out", relax and enjoy oneself, to meet for not so serious purposes. The play dimension and the interpersonal dimension of the information highways have both developed strongly. They thus call to mind other human rights concepts: freedom of movement, freedom of association and indeed, privacy.

We could continue in this vein with this spatial metaphor because the agora, a public space, served as a transition between numerous private spaces: production spaces, family spaces, interpersonal spaces, etc. Consequently, if we really want to rely on human rights concepts in making choices regarding development of the information highways, consideration must be given to all those concepts that are genuinely evoked by a particular application, and not just to one or two key concepts like privacy or freedom of speech that serve so many purposes that they unfortunately tend to lose their significance. This more comprehensive use of human rights concepts provides a much clearer picture of the challenges we have to meet, and of the social implications of the decisions we have to make while discussing personal information intensive applications of information highways technologies.

5. Conclusion

Privacy as a field of study and practice emerged in good part from the "computer and society" studies. This field became more or less autonomous with its own publications, conferences, legal and administrative institutions, professional associations and networks. In the process, the use of very concept of privacy slowly parted from the original meaning related to the delimitation of an individual's sphere of autonomy, more or less free from external intervention. In the jargon of specialists, privacy is more and more equated with the institutions designed to provide confidentiality and protection of personal information. We have not mentioned the fact that even within these circles, there are emerging discourses which advocate the need to discuss a redefinition of even these reduced definitions, in order to facilitate secondary uses of personal information for scientific research, management or marketing purposes. Thus, even the definition of what constitutes privacy could become in itself a debatable and conflictual issue.

But the problems arising from the interactions between information technologies and society still remain, especially as it related to individuals. We are talking about implication between information technologies and society in its philosophical meaning, which is the impossibility of understanding one term without referring to the other: these technologies are the products of society, their origin and development are determined by it; conversely, these technologies influence, even impact, on the evolution of society and its institutions.⁴

This domain includes numerous and complex sets of inter-related technical, social, legal, economical, cultural, political and ethical issues. It related to formidable challenges about defining prospective visions of what should be the socially acceptable directions for the development of information societies. Discussions

about the social, legal and ethical issues arising from the use of personal information should not be completely divorced from this larger debate. Within this larger framework, confidentiality and protection of personal information appear as essential but rather secondary issues. Within this framework, privacy re-emerged as a central concept that, nevertheless, does not and cannot cover all the field. Within this framework, discussions about the impact of an personal information intensive application can stand outside the technicalities of security and the legalities of confidentiality or protection of personal information. The discussion of the real life impacts on real people lives and on existing organizations or social institutions becomes possible. A discussion with which the average citizens can relate to. Within this framework, rigorous and sensible use of non-synonymous terms such as security, confidentiality, protection of personal information and privacy becomes almost mandatory.

In fact, it seems that it is only within a framework that looks well beyond privacy that privacy can remain an appropriate concept to understand a large set of the issues related to the use of personal information systems. This framework also undelines the need for more comprehensive social assessment of projects of information highways' infrastructures or specific applications as well as for prospective technology watch to provide advance warning about the profound social changes in the making. Looking beyond privacy is nothing but a necessity.

Lex Electronica Volume 3, numéro 2 (hiver 1997)

Notes

(*) Researcher, Center for Bioethics, Clinical Research Institute of Montreal
Scientific Coordinator, Telehealth Ethics Programme
E-mail: peladep@IRCM.Umontreal.ca

1. Cybernews asked me to adapt for this issue a scientific popularization piece I wrote in French for the Cybersciences website, http://www.cybersciences.com/Cyber/textes/vie_priv.rtf

2. Public Interest Advocacy Center & Fédération nationale des associations de consommateurs du Québec, Surveying Boundaries: Canadians and their personal information, Ottawa, PIAC & FNACQ, 1996.

3. Vitalis, A. Informatique, pouvoir et libertés. 2nd edition. Paris: Éditions Économica, 1988.

4. From the definition of the field "Informatique et Société" proposed in CREIS (Centre de coordination pour la Recherche et l'Enseignement en Informatique et Société), Thésaurus Informatique et Société, Paris, CREIS, (Bulletin de liaison N° 10), mai 1992.