

## The Impact of Information Systems on the Quality of Life, in Terms of Privacy<sup>†</sup>

Pierre Tabatoni<sup>\*</sup>

*Privacy* and, more narrowly, *intimacy* are the expression of the *self*: of human dignity (body, home, family, personal life, and health), citizenship (nationality, political and civil liberties), and economic and social life (property, contracts, trade, work, social rights, and housing (Cabrillac et al., 2001)). Individuals and society judge security and a person's autonomy and privacy, as major components of the quality of life.

With their operational and communication potential, new information systems such as the Internet, broad-band channels, numerical treatment of information, electronic messaging, mobile phones, and a great variety of software, have extended people's potential to search for and access new information autonomously, to develop new interpersonal relations, transact a wider variety of commercial activities, take better care of their health, education and leisure, and to participate in multimedia events.

The origin of the word 'private' lies in the Latin *privare*, meaning to separate, differentiate from others, *public* and *private* affairs. The ancient Greeks considered any subject that was not important enough to be discussed in the People's Assembly as private. The Romans clearly distinguished between *publice* and *privatim*. Modern cultures attach their own meanings to public and private, and although the usage of each shifts with time, the distinction between public and private is fundamental.

In western civilisation, which forms the historical and cultural framework of this discussion on privacy, individualism fostered the idea of freedom of speech and privacy. The ideas reached a higher

---

<sup>\*</sup> Pierre Tabatoni is Member of the Académie des Sciences Morales et Politiques, Paris, and Chairman of the former ALLEA working group *Privacy in the Information Society*.

<sup>†</sup> The autor wishes to express his deep gratitude to Prof. Jeanne Brett, from the Kellogg Graduate School of Management, Northwestern University, for her careful reading, suggestions, and English editing.

status with Humanism, Enlightenment, and, especially, John Locke and Jean Jacques Rousseau's discussions on liberty. By the end of the 18th century the US Constitution and the French *Déclaration des Droits de l'Homme et du Citoyen*, had formalised citizens' rights. The legacy of the 19th century was the extension of education, freedom of the press, political liberties, and social rights for a greater number of people.

Despite the conceptual and institutional distinction between 'public and private', the two concepts are not totally independent of each other, as every person lives in a public environment and frequently acts in the presence of others, and under their observation. Furthermore, public authorities must define the limits of everyone's rights to privacy. A societal question is how much public entities should be allowed to monitor the private acts of individuals. Limitations of the right of public authorities to intrude on private affairs are as ancient as the acknowledgement of those affairs. But, by the late 19th century, the concern for privacy focused on the relations between private agents when interacting: employees and employers, customers and businesses, readers, users of media and their suppliers of information, patients and doctors, renters and landowners, visitors on the Internet and servers etc. In addition, almost any individual act today generates data that can be *treated* by information systems, and whose *confidentiality* becomes an issue - the exception to this rule may be thoughts and emotions.

We can distinguish between different methods of protection in terms of how they combine social norms, laws, professional self-regulation, security software, public opinion and social monitoring of confidentiality. They interact with one another within what we can call *systems of privacy protection*, within their specific performance, and in terms of quality of privacy protection. Despite their differences, these methods have in common a confirmation of the legitimacy of privacy, a definition of the criteria of fair-practice, commitment to the right of *non-interference*, and limits to investigation of individual behaviour.

### ***Privacy, security, and quality of life***

Privacy and security respect human dignity and human development. Psychologists (see *Revue Internationale de Psychosociologie*, 2000) emphasise that the distinction between private and public, like the distinction between 'sacred' and 'profane', is a corner stone of societal de-

velopment. In Germany, Holland, Switzerland, and Spain, privacy is a *right to the development of one's personality* ("die Freie Entfaltung seiner Persönlichkeit", in the German Fundamental Law; art 10-13 of the Dutch Constitution (Gutwirth, 2001). The German law further protects *informational self-determination*, or people's right to use their personal information as, when, and how they wish, without manipulation, opacity, abuse, or insecurity (Simitis, 2000).

Our information-based societies have facilitated easier, faster, cheaper, and networked interactions, exchanges and transactions. The costs of communications have been dramatically reduced. In the current information society, the right to privacy would benefit from more rigorous laws, private privacy policies, widely available security software, and the public opinion support. One major on-going threat to the protection of the right to privacy is caused by the efforts required to stay informed of the newest developments in regulations, techniques, equipment, software, and social norms that both protect and endanger privacy. Another danger is that the computer literacy could become an inequitable source of degradation of the quality of life of the less informed. Happily our youth seem undaunted by the challenge of monitoring and mastering these on-going changes. Eventually, *over-information* can become a nuisance for everyone, just as too much noise can; it requires more attention, and the utilisation of more sophisticated and difficult to use search processes.

Yet, despite safeguards and sophisticated monitoring, everyone has heard about and many have experienced computerised intrusion into private life. Every new telecommunication device that increases the complexity, speed, or real time connectivity, increases the risk of intrusion by monitors, hackers, viruses, 'ET' spying programs, worms etc.

Without anyone knowing, and often automatically, new data-mining software, associated with on line commercial transactions (Agre & Rotemberg, 1999; Garfinkel, 2000), can collect all types of personal information with the purpose of exploiting it in marketing strategies. Access to electronic addresses permits advertisers to target publicity on a huge scale. This practice, called *spamming*, is detrimental to the quality of life if experienced as invasive.

People are insecure about the protection offered them when using credit and smartcards, social security and bank account numbers, or about their health records, or on-line transactions. They may wish to provide personal data for specific purposes, but they are usually very

concerned that such data could be resold, on 'information markets' (Tabatoni, 2002), and be made available to competitors, landowners, employers, insurance and banks, leisure or political organisations, and, of course, public authorities who could use data for other purposes. Nevertheless, in the USA, for example, about 56% of consumers of business products are willing to supply personal data, as long as safeguards are provided that they can trust.

Safeguards should include a clear and fair description of the privacy policy and of data treatment - which are legally regulated in Europe - and a detailed explanation of the rewards and possible loss of privacy associated with providing personal data. The rewards include better commercial information, commercial advantages like rebates on prices, premia, labels specifying the quality of the privacy, or even 'free' access to the Internet or Internet services, all classical ways to attract clients and create a strong market position. The reward can also be an opportunity to promote oneself through the media, a public image, or to participate in shows, such as reality shows that offer indiscreet or indecent information, but are expected to provide both actors and spectators with enjoyment.

Increased feelings of insecurity after September 11, 2001 may be shifting people's definition of the role of privacy in their life. The 'anti-terrorist' legislation adopted by many countries since September 2001, allows extensive control of personal communications, such as the collection and prolonged storage of data, interconnection among different databases, and many forms of surveillance, such as video surveillance and electronic monitoring. Today, a double paradox seems at work. One is that people are willing to accept more public security intervention, while, at the same time they have become more conscious and knowledgeable of risks to privacy. A second one is that they are asking for a greater transparency of public authorities and other empowered private actors' activities, which often generates greater risks of intrusion into their own privacy. For Hannah Arendt 'transparent' societies are totalitarian.

### **Privacy, liberty, right(s) to privacy and democracy**

Privacy, with its characteristics of confidentiality and secrecy, is a liberty. It is one of the liberties granted by democratic societies, like ex-

pression, belief, travel, opinions, relations, commerce, action and non-action, and possibly harbours contradictions. The conflict between private liberty and liberty of the press was at the centre of the debate on liberty in the 19th and 20th centuries. Today, certainly in the USA and in Europe, the liberty of the press seems to have won the battle with privacy. Serge Gutwirth argues that privacy is equivalent to freedom in its general sense: "Privacy can have a truly emancipatory impact (...) violations of privacy are not attacks on an 'autistic' subjective right but on the freedom of individuals" (Gutwirth, 2001). Social scientists, and especially jurists, are debating the interrelationships between *privacy liberty* and a formal *right to privacy*, whose protection is instituted, regulated, and implemented through legal or contractual processes.

Privacy is a right. Since the notion of privacy is complex and paradoxical (Rigaux, 1990, 2002; Gutwirth, 2001), jurists have found it difficult to define it precisely. Laws more often regulate 'particular' rights to privacy, e.g. in 'sensitive data' which express intimacy, telecommunications and electronic exchange, treatment and transfer of personal data, people's relations with the media, confidentiality of health and judicial information, and protection of children vis à vis the media.

In their famous 1890 article, two American lawyers, Samuel D. Warren and Louis D. Brandeis, defined the right to privacy as the "right to be let alone", the general issue being the liberty of the press, and, possibly, press indiscretions about Mrs Warren's social life. Justice Louis Brandeis, in a Supreme Court decision in 1928, added that "privacy is the most comprehensive of all rights (...) and the right most valued by civilized men". François Rigaux defines the "right to privacy (as) simply privacy freedom, which is strongly related to human dignity" (Rigaux, 2002). Jurists and politicians have referred to rights to privacy as basic human rights and liberties of the person (Gutwirth, 2001). In many countries, the right to privacy is considered a 'personal right', and a 'subjective right' (Rigaux, 1999; Terré, 2001, 2002), but François Terré observes that personal rights "cannot easily be distinguished from the notion of 'public liberty'".

Since 1945, several founding texts and constitutions have formally recognised and structured the *right to privacy* (Gutwirth, 2001). An earlier example is Art. 8 of the 1951 Convention on Human Rights and Fundamental Liberties. This recognition was extended with the 1981 *Convention 108 of the Council of Europe*, and focused, by the 1995 European Community's Directives on *the treatment of personal data*

*and free circulation of data*, and, in 1997, by the directives on telecommunications. In 2000, the *Charter of Fundamental Rights in the European Union* specifically included the right to privacy. National legislation in separate European countries has followed those founding texts. Nevertheless, today the rate at which the use of the Internet, electronic commerce and wireless communications is expanding, challenges the existing legislative apparatus.

### ***Law, self-regulation, and technique***

As Gutwirth and Simitis point out, the basic foundations of privacy laws are relevant whatever the technical environment, but technical invention, enhanced by economic innovation, may have a significant impact on the performance of the legal guarantees granted to privacy. For Simitis, "technology puts a limit to the application of a regulation which it had initiated (...) integration and instrumentalisation of information technology will become the most significant symbol of the next generation (of privacy laws)". Rewriting general laws takes time, but special laws and self-regulation are more flexible. Although self-regulation is the general practice in the USA (Tabatoni, 2002), there are several important state privacy laws, and specific federal laws strictly regulating certain aspects of privacy related to children, health data, telecommunications, finance and credit, but there is no overarching law as in Europe. Some privacy analysts are forecasting general federal legislation within the following five years (Erbschloe & Vacca, 2001). However, the risk of public regulation is a powerful incentive for businesses to self-regulate in a satisfactory way.

In our ALLEA working group, we believe that protection by 'general' laws, such as those that protect computerised personal data in Europe, is the best solution. The USA experience of self-regulation has shown that the quality of protection supplied to customers is highly variable, although the risk of public regulation stimulates satisfactory self-regulation.

Nevertheless, there are obstacles to an efficient and equitable protection by law. Simitis (2000) denounces "vague and general clauses in the legislation (...) open doors to different interpretations", and also 'clustering' effects due to the proliferation of specific legislations and particular privacy rights. For Rigaux (1999) "the certainty brought

about by our juridical systems is more illusory than it could appear to non-jurists (...) the wall of private life is not a tight division but a porous one (...) the concept of privacy is undetermined". Furthermore, since different liberties may compete with one another, in each case the judge has to 'balance' opposing interests to reach a decision (Rigaux, 1999).

### **Privacy and power**

Rigaux (2002), as well as Gutwith (2001a) and De Woot (2002) pose the question whether the practice of privacy confronts individuals with more powerful organisations. Rigaux asks whether "the individual is a subject or an object of the information society". Modern information and communication systems, their use in business, in the media, and in scientific work provide impressive means with which to influence people's behaviour (Agre & Rotemberg, 1999) as well as their attitudes towards the quality of their life and their privacy. Yet, simultaneously, the potential of technology risks, such as computer software and 'malware', biotechnology disasters, genetic engineering, destruction of natural resources, unhealthy food etc., has lead organisations capable of intruding into formally private realms to adopt a 'principle of precaution'. Recent examples concern human genetic engineering, the risks of 'mad cow disease', or of genetically modified cereals. Strong public and professional regulations have tried to respond to people's fears, and also to their leaders' desire to safeguard themselves against potentially being held personally responsible. The principle of precaution, of course, is not without uncertainty as far as the impact of the policies it introduces is concerned.

### ***Privacy and public authorities***

Relations between individuals and public authorities have always been a challenge to privacy. The rapid development of applications of modern information systems in public administration and political life can improve citizens' quality of life. Yet, public data are no less vulnerable to breaches of security than private data. And the mere comprehensiveness and interconnectedness of public databases make them particularly

vulnerable to *cyber-crimes*. Citizens are thus demanding that their governments provide *cyber-security*. In November 2001, the Council of Europe voted for a new *cyber-crime Convention*, which tries to balance security and privacy needs.

Security enhancement measures nevertheless encroach upon privacy of communications, e.g., wiretapping in all forms, restrictions on encryption, video-surveillance, data banks cross-examination, and genetic inquiries and tests etc. On the Internet, the USA *Carnivore* system, and the British *Echelon*, and other countries' electronic surveillance systems have gone very far in penetrating privacy. But, even in the context of anti-terrorist legislation, such inquisitive surveillance should be better controlled by judges, and subject to the basic principles of being necessary, appropriate, proportionate and limited in time.

### ***Privacy and economic power***

The extended use of electronic communication in information and commercial processes provides business professionals with powerful computerised opportunities to influence financial, transactional and important ethical choices (see De Woot, in ALLEA Report Series 2, 2002). An example is the desire of employers to control their employees' private use of electronic communications during their work time, and to allow information to be used for personnel management. The USA culture and practice tend to accept employer monitoring as long as it is not abusive. Britain accepts monitoring in cases of fraud risk, sex and racial abuse, and other situations defined by legal codes of conduct, or by the Information Commissioner (Bell, 2002). A 2001 French Higher Court decision confirmed the secrecy of personal communications, and has forbidden any clandestine monitoring at work. In many countries there is a trend for the employer to honestly inform his employees about any projected mode of control.

The 'new economy' increased the interdependency between privacy concerns and legislation, and economic objectives (Gentot, 2001; Gutwirth, 2001; Simitis, 2000). Information about customers' personal tastes, needs, and behaviours has always had strategic values for marketers, but new information technology permits more 'personalised' marketing methods, targeting people's very specific needs (Erbschloe & Vacca, 2001). The capacity of firms to analyse personal data

(Garfinkel, 2000, Rigaux, 2002) and draw commercial 'profiles' of customers, allows them to rapidly extend their networks of clients and users, and gain competitive market places (Varian, 1998). Modern marketing software can give an almost 'instant' profile of customers' behaviour. This allows targeted advertising that draws and retains the 'attention' of viewers of commercial messages and 'induces', or 'seduces' them into buying.

Over the past ten years the Internet has been the preferred advertising channel of such so-called *one to one selling*. Currently, new forms of electronic publicity and marketing methods, utilising customers' e-mails, like 'spamming', have generated a customer backlash that sees them buying special 'firewall' software to limit such an invasion of privacy. But from businesses' perspective, any aggressive marketing that allows personalised selling is in customers' interest, and should be considered as a positive contribution to their quality of life. A balance has to be struck. After much debate the European Union telecommunications directive forbade spamming in 2001, unless expressly authorised by customers. Recently, DigitPortal Systems of New Jersey, USA offered customers a tool to regulate spamming by means of prior authorisation (The Wall Street Journal, Europe, Personnel section, July 12th, 2002).

Becoming more aware of people's sensitivity to privacy, some businesses are trying to establish longer term 'trust' with their clients in a variety of ways. Some are adopting 'permissive' marketing methods that require customers' prior authorisation of e-mail contact (see above). Rule and Hunter (2001) proposed the application of the idea of 'property rights' to personal data. New market intermediaries, called 'infomediaries' (Hagel & Singer, 1999), acting as customers' agents, offer businesses different forms of adequate privacy protection as private services. Such services could also help business develop 'trusted relations' within their customer relationship management policies.

At the heart of the debate is the role of 'customer consent', i.e. their right to accept any form of privacy policy offered to them, even without a clear understanding of the guarantees offered (Simitis, 2000; Gentot, 2002), or being assured that such policies respect public regulations. Some commentators would reject any right of customers to consent to a reduction of their legal privacy protection. For the majority of authors, however, consent is part of privacy liberty, and the problem for them is reinforcing public authorities' capacity to enforce compliance with their

rules. There is a corresponding controversy about 'opt-in' and 'opt-out' choices. Within opt-in clauses, there can be no collection or analysis of personal data without the client's prior authorisation.

This policy conforms to the principle of 'self determination of information' as a personal right. This is legally imperative with regard to the treatment of 'sensitive personal data' in many countries in Europe (Rigaux, 1999), but less extensively so in the USA. Self-regulating businesses are generally proposing opt-out clauses where clients can ask to have their data withheld from a database. They argue that opt-in clauses are difficult to manage in electronic commerce, and are a serious obstacle to economic growth and competition. As Rigaux (1999, 2002) explains, in our economic system a right to privacy, combined with the right to exchange, makes the balance between these rights a 'patrimonial' right that can be negotiated, as is currently done (see also the observations on 'merchandisation' of personal data in Gentot, 2002; Simitis, 2000).

The diversity and complexity of different, and often contradictory, national privacy laws are a serious challenge for international transactions. In 2000, the United States and the European Union agreed to a compromise between their respective protection systems - the self-regulatory and legal one, respectively - in order to permit the transfer of European personal data to the USA. The practice and performance of this voluntary *safe harbour system* (Tabatoni, 2002) will have to be closely watched on both sides.

## Conclusions

1.- The respect of privacy, as a fundamental liberty of people and a condition of democracy, is at the core of the quality of life. But the right to privacy, which can be implemented through different 'protection systems' in different cultural contexts, is a relative and differentiated one. A legal definition of privacy rights necessitating strict procedural implementation criteria seems to be the most satisfactory protection scheme. But, it is not without problems. Several legal 'deficits' have to be rectified, including improvements in the legal text, increased public resources for stricter control of its implementation, improved education of the public and better integration into a rapidly changing technical, economic, and cultural environment.

2.- In several countries, like Great Britain, Holland, and Sweden, and, more systematically, in Canada, privacy protection systems combine extensive privacy legislation and self-regulation (Bell 2002; Franken, 2002). These systems include professional standards, codes of conduct, formal ratings of the quality of the protection, commercial services for better protection of privacy, greater commitment and monitoring by consumer associations and other private organisations, as well as extensively educating people on privacy, its risks, and how to reduce these. Besides, an increasing number of managers are considering the strategic and competitive value of respectful treatment of their customers' privacy (Erbschloe & Vacca, 2001). The obvious advantage of the flexibility of such a diversified approach could be more widely practised in Europe, as no law forbids it.

3.- The innovative development of 'protection software', such as cryptographic keys, anonymisers, smart-cards for access and data treatment, virtual private networks, electronic filters, 'platforms for privacy preferences', electronic passports and safes, provides users with new hopes for more efficient protection. Of course, the performance cost/quality of these innovations is variable, and often badly estimated (Anderson, 2000). Obviously, perfect security does not exist, and breaking down computerised defence has its costs and its rewards.

4.- We need more systematic and easily available means of evaluating different methods of privacy protection from the point of view of their complexity, user-friendliness, general accessibility, and protective performance. Because these methods of protection can be combined and are interactive, we need evaluations of 'systems of protection'. Finally, because privacy needs and norms, and privacy protection, are changing under the influence of cultural and technical change trends, we need mechanisms to ensure continuous attention to change. This is why our working group has proposed the creation of a *European Privacy Observatory* within ALLEA (ALLEA Report Series 2, 2002), composed of networks of experts from the different disciplines working with European networks of privacy experts and professionals.

## Selected references

- Agre, Ph. & Rotenberg, M. (Eds.) (1999). *Technology and privacy: The new landscape*. MIT Press.
- ALLEA (2002). *Privacy protection in the information society. (Background papers of the working group chaired by P. Tabatoni, editor)*. Amsterdam: ALLEA Report Series 2.
- Anderson, R. (2001). *Security engineering*. University of Cambridge, computer laboratory.
- Bell, J. (2002). *La vie privée et l'Internet*, In: *Cahier des sciences morales et politiques*, 3-4-5.
- Beigner, B. (2001). La protection de la vie privée. In : R. Cabrillac, M.A. Frison-Roche, T. Revet, *Libertés et droits fondamentaux*. Dalloz.
- Cabrillac, R., Frison-Roche, M.A. & Revet, T. (2001). *Libertés et droits fondamentaux*. Dalloz.
- Erbschloe, M. & Vacca, J. (2001). *Net privacy*. A guide to developing and implementing an ironclad business privacy plan. McGraw Hill.
- Garfinkel, S. (2000). *Database nation: The death of privacy in the 21st century*. Amazon.
- Gentot, M. (2002). La protection des données personnelles à la croisée des chemins. In: *Cahier des sciences morales et politiques*, 3-4-5, p. 25-44.
- Gutwirth, S. (2001). *Privacy and the information age* (Translated by Raf Casert). New York, Oxford: Rowman and Littlefield Publishers
- Hagel, L. & Singer, M. (1999). *Net worth. Shaping markets when consumers make the rules*. Harvard Business School Press.
- Revue Internationale de Psychosociologie (2000). *Privé et public*. In: *Revue Internationale de Psychosociologie*.
- Rigaux, F. (1990). *La protection de la vie privée et des autres biens de la personnalité*. Brussels: Bruylant/L.G.D.J.
- Rigaux, F. (2002). L'individu, sujet ou objet de la société d'information. In: *Cahier des sciences morales et politiques*, 3-4-5.
- Rule, J. & Hunter, L. (1999). *Towards property rights in personal data; visions of privacy policy choices for the digital age*.
- Simitis, S. (2000) Auf dem Weg zu einem neuen Datenschutzkonzept. In: *Datenschutz und Datensicherheit*, 24.
- Tabatoni, P. (2002). Stratégies de la privacy aux Etats Unis. In: *Cahiers des sciences morales et politiques*, 3-4-5.

- Terré, F. (2001). Sur la notion de libertés et droits fondamentaux. In: R. Cabrillac, M.A Frison-Roche, T. Revet, *Libertés et droits fondamentaux*. Dalloz.
- Terré, F. (2002). La vie privée. In: *Cahier des sciences morales et politiques*, 3-4-5.
- Varian, H.R. (1998). *Economic aspects of personal privacy*. University of California, CRIE.