

Keeping privacy alive: a model for negotiating privacy rights in the networked society

Călin Gurău

School of Management, Heriot-Watt University, Riccarton, Edinburgh, EH14 4AS,
UK; email: c.gurau@hw.ac.uk

Adriana Șerban

School of Modern Languages and Cultures, University of Leeds, Leeds, LS2 9JT,
UK; email: a.serban@leeds.ac.uk

Abstract: *Online privacy is one of the major concerns of the modern society. The privacy issue is complicated by the new social rules and technological applications which characterise the networked society. The paper attempts to present various perspectives on the problem of online privacy, considering the present infrastructure of the society, and proposes a negotiating model for defining, protecting and enforcing privacy rights.*

“Privacy is dead”

Scott McNealy, CEO Sun MicroSystems Inc.

Introduction

With the expansion of new information and communication technologies, networking logic has changed and redefined the structure of social relations. In a networked society the individual becomes only an element, a participant in the connectivity phenomenon. The existence and the value of a person changed its focus from being and doing, to participating.

Since the process of participation has been given that much prominence in the social and economic life, the social expectations have been restructured in line with this new value system. The ‘good’ in the networked society is associated with all the activities that initiate, maintains and increase the effectiveness of participation, the fluidity of information flows. ‘Bad’ are the attitudes that limit and endanger connectivity. In this respect, in specific circumstances, the privacy rights can be included, paradoxically, into this negative value category.

The manifestation and the protection of individual privacy rights represent the field of conflict between various disciplines and social events. The heterogeneous nature of this phenomenon is mirrored in this paper, which aims to present the complex nature of privacy rights in the context of the networked society, as an interplay between technology, philosophy, sociology, law and economics. In order to solve the problem of privacy rights, this study proposes a negotiating model, and analyses the necessary conditions for the implementation of this model on the Internet.

Defining privacy in the networked society

The Privacy Journal, a print newsletter and online web site devoted to privacy matters, defines the present-day use of the word privacy as "the right of individuals to control the collection and use of personal information about themselves" (Privacy Journal, 2003). Similar definitions are provided by law specialists (Gavison, 1980; Laudon, 1986; Warren and Brandies, 1890; Westin, 1967).

The networked society changes the way in which privacy rights are defined (Castells, 2001), used and interpreted, because:

- a. the IT-enabled channels of communication change the rules of personal and commercial interaction;
- b. the participation in the networked society implies a diminishing of individual privacy rights.

The fundamental principle of the networked society is information sharing and processing (Kling and Allen, 1996). Advances in computing technology, that represents the infrastructure of the networked society, make possible to collect, store, analyse and retrieve personal information created in the very process of participation.

The new economy is redefined on the basis of information entrepreneurship (Kling and Allen, 1996; Zwick and Dholakia, 1999). This cultural paradigm has taken roots in business schools and organizations, emphasizing the use of data-intensive analysis techniques for designing and implementing effective marketing and management strategies. This has as a direct consequence the use of an information superpanopticon – a concept derived from Foucault's panopticon (1977), a system of perfect surveillance and control.

Privacilla.org, an online organisation for privacy protection, provides a possible solution for the preservation of personal privacy: absencing from particular commercial and social interactions, the people can decide who receives information about them (Privacilla, 2003). This solution is, however, highly unfeasible, because it implies a strategy on non-participation, which has the effect to marginalise these individuals and to deny them access to most of the benefits provided by the modern day society.

The Internet

The Internet is the perfect example and metaphor of the networked society. Being in itself an international network of networks, the Internet highlights all the benefits and disadvantages of the networking and connectivity.

The Internet allows:

- high-speed connectivity and information exchange;
- ease of participation, association and networking;
- flexibility and efficiency in collecting, storing, processing and analysing data.

On the other hand:

- the transmitted information can be intercepted by third parties, and used for malicious or criminal purposes;
- information can be easily collected, copied and shared covertly, without the knowledge and consent of Internet users;

- in some cases, it is difficult to connect the online identity with the physical address of an organisation or person, which encourages opportunistic and fraudulent behaviour.

Online privacy is a major concern for Internet users (Ackerman et al., 1999). For the individual Internet user, the privacy threats fall into two main categories:

- a. web tracking devices that collect information about the online behaviour of the user (e.g. cookies);
- b. the misuse of the personal information provided by the online user in exchange of specific benefits: increased personalisation, web group membership, etc.

The databases, intelligent agents and tracking devices are surrounding the Internet users with a web of surveillance, which is often hidden and unknown to the subjects (Poster, 1990). The surveillance is initiated by the simple act of presence on the Internet (Gandy, 1996). Specialised software applications, such as 'cookies' are tracking the online behaviour of Internet users, feeding the data into databases, which create and permanently update a profile of online consumers. These profiles are then use for segmenting the market and targeting the most profitable consumers (Kotler and Armstrong, 1996).

A company can use cookies for various valid reasons: security, personalisation, marketing, customer service, etc. However, there is an important distinction between cookies, which are active only within a specific web sites, and the ones that can track the user's activity across unrelated web sites. Recently some aggregator networks have deployed hidden 'pixel beacon' technology that allows ad-serving companies to connect unrelated sites and overcome the site-specific nature of traditional 'cookies' (Mabley, 2000). Additionally, come companies are now connecting this aggregated data with offline demographic and credit card data. Eventually, these resulting databases can be used or sold as powerful marketing tools.

Exercising control of information, after it was voluntarily released, presents another critical problem. The misuse of personal information covers many possible aspects, which can be defined as any use which is not explicitly defined in the company's privacy disclaimer, or which is not approved by the informed customer. For example, in 2000, Toysurus.com was subject to intense debate and controversy, when it was discovered that shoppers' personal information were transferred through an unmarked Internet channel to a little known data processing firm, for analysis and aggregation. This operation was not disclosed in the company's privacy disclaimer, and therefore, online customers were not aware of it.

The philosophical foundations of individual rights

In the postmodernist view, it is a mistake to think of personal choice and individual decision-making as motor concepts in social theory (Mohr, 1995). There is no individual prior to social processes. The individual is a product of culture, a social construction emanating from the social mind or what postmoderns call "social discourses." But as the plural "discourses" suggests, society is not of a single mind. So the constructed thing is not a unity, the "individual" being simply the point where a

number of social identities intersect. The constitutive identities themselves, according to deconstructive principles, are disparate and contradictory (Mohr, 1995).

The fragmented self needs to be negotiated and re-defined in every circumstance depending on the power and position of a person within its daily networks. The personality elements cannot be therefore protected in absolute sense – because they are subjected to multiple changes and roles in the process of social interaction. In these conditions, the personal rights are losing their objective nature; their fundament do not rest anymore in the individual person as a living being, but in the particular circumstances of the every-day social interaction.

Another defining trend of the postmodernism is the increased commodification of society (Habermas, 1987). The social commodification engulfs also the digital self of people. Personal information has become an important asset, both for individuals and for companies. People are willing to provide information about their age, gender, habits and preferences, in order to get connected to the networked economy and benefit from customised interactions with business or other individuals. Companies are treated the aggregated information about their customers as corporate property: in 2000, Amazon.com announced that in the event of bankruptcy, customer databases would be treated as an asset to be sold along with other property held by the company (Oakes, 2000).

A more positive vision of the networked society and of the future it promises is provided by Lombardo (2003). He argues that the networked society creates the basis to model human organizations on participatory networks, rather than dominance hierarchies. The computer, information technology, the communication network, and the emerging global intelligence are all demonstrating the features of evolving interactive systems of complexity and creativity. Morality is moving toward an evolutionary dialogue.

Besides the utopian tone of these predictions, they cannot ignore the relativism of the social values, which are open to debate, dialogue and negotiation.

Private versus public

Since the fundamentals of rights shifted from the person to social circumstances, it is increasingly difficult to protect the privacy of individuals sharing a public space, or performing public activities.

Internet is considered as a public space (Ó Baoill, 2000), and many activists militate to keep it like this in order to maintain freedom of speech and interaction (Poster, 1995). The public nature of the Internet has been somehow diluted by the claim of online organisations that their web site is a private place, and that online data is protected by copyright laws. By comparison, the individual Internet user cannot claim any of these rights. The data s/he creates by simply browsing the web is not virtually concentrated in any well-defined web site, and it is not purposefully created or written down.

The problem of power status is also important: many Internet users are not aware of the ways in which organisations or other individuals can abuse the information

provided by them on the Internet. Those who are aware, often lack a clear legal infrastructure capable to empower them and their privacy rights.

The protection of privacy can also be limited through specific interpretation of public or individual 'good'. The monitoring of web behaviour by public authorities in order to track and prosecute criminal activities represents a strong argument in favour of violation personal privacy for the public good. On the other hand, online companies are using web-collected information to target more precisely individual customers with personalised offers, which can be perceived as an added benefit for the customer. However, some companies start from the assumption that these customers want to receive these spontaneous offers, without bothering to ask them for permission.

Where should be draw the limits of online privacy rights ? If the web is indeed a public space, and the browsing is a public activity, the covert collection of information is permitted, as it is possible to observe the activities of the passers-by on the street. On the other hand, within the private space of a company web site, a customer can decide to provide personal information in exchange for specific benefits such as group membership or personalised offer. In these conditions, part of the digital self of that person is treated as a commodity, and the customer-company interaction can be defined as a contractual relationship, ruled by law or by the legal provisions of privacy disclaimer.

The legal protection of privacy rights

Regulators and legislators have addressed the controversial privacy issue quite differently across the world (Nakra, 2001). The USA, the largest world's financial and Internet market, has not yet adopted a national, standard-setting privacy law (Jarvis, 2001). US privacy statutes have primarily focused so far on protecting consumers' financial data, health information, and their children's personal information (Desai et al., 2003; Frye, 2001; Rombel, 2001). In comparison with the American official opinion that online privacy protection is a matter of voluntary self-regulation by market-driven companies, the Europeans consider that it is more effective to enforce specific legislation regarding this issue.

The current European approach is based on three basic tenets (Lillington, 1998):
(1) individuals have the right to access any data relating to them and have it kept accurate and up-to-date;
(2) data cannot be retained for longer than the purposes for which it was obtained, nor used or disclosed "in a matter incompatible with that purpose", and must be kept only for "lawful purposes";
(3) those who control data have "a special duty of care" in relation to the individuals whose data they keep. Data commissioners oversee these rights in each European country and require most "data controllers" - people who handle data - to register with them to track what information is being collected and where. They are charged also with investigating all complaints from citizens.

These principles have been incorporated in the European Data Directive, which came into effect in 1998, and more recently, in the European Directive on Privacy and Electronic Communications, adopted in 2002, which requires implementation of its provisions in Member States by 31 October 2003 (DTI, 2003).

The new Directive:

- replaces existing definitions for telecommunications services and networks with new definitions for electronic communications and services to ensure technological neutrality and clarify the position of e-mail and use of the Internet;
- enables the provision of value-added services based on location and traffic data, subject to the consent of subscribers (for example, location based advertising to mobile phone users);
- removes the possibility for a subscriber to be charged for exercising the right not to appear in public directories;
- introduces new information and consent requirements on entries in publicly available directories, including a requirement that subscribers are informed of all the usage possibilities of publicly available directories - e.g. reverse searching from a telephone number in order to obtain a name and address;
- extends controls on unsolicited direct marketing to all forms of electronic communications including unsolicited commercial e-mail (UCE or Spam) and SMS to mobile telephones; UCE and SMS will be subject to a prior consent requirement, so the receiver is required to agree to it in advance, except in the context of an existing customer relationship, where companies may continue to email or SMS on an 'opt-out' basis;
- clarifies that the Directive does not prevent Member States from introducing provisions on the retention of traffic and location data for law enforcement purposes;
- introduces controls on the use of cookies on websites. Cookies and similar tracking devices will be subject to a new transparency requirement - anyone that employs these kinds of devices must provide information on them and allow subscribers or users to refuse to accept them if they wish.

Despite these legislative efforts, it is not yet clear how these measures will be implemented, controlled and enforced by the EU States. The direct involvement of governmental institutions can be considered as a form of censorship that can undermine the freedom and the flexibility of the Internet domain.

Negotiating online privacy rights

Considering the social and economic reality of the postmodernist world, we should adopt a model of online privacy protection which is compatible with the rules and values promoted by the networked society.

The relativism of personal rights, and the increased commodification of the digital self, indicate a negotiation model based on contractual rules as the most appropriate for defining and enforcing personal privacy.

A classical negotiation situation comprises a number of essential elements (Zlatev and van Eck, 2003): parties, rules (a negotiation protocol), a system of law enforcement (established and maintained by regulators), and specific benefits to be negotiated by the parties (negotiation objects).

In an on-line situation, the parties negotiating privacy rights are often in a position of inequality. Most privacy statements and disclaimers act as a standardised contractual clause, that has to be entirely accepted by the Internet users. There is no room for

negotiation, and the only alternative is non-participation in that particular transaction. On the other hand, after the Internet user discloses its personal information, as part of the online deal, s/he has no direct possibility to control the way in which the organisation uses its personal information. The storage, retrieving and processing processes are fully covert, and the only hope of the Internet user is that the company will respect its promises.

Measures have to be taken in order to provide a level plain field for the online negotiators. The use of intermediaries (information brokers) is a possible solution.

Laudon (1996) proposes the implementation of National Information Accounts, a market-based negotiation system, in which information about individuals is bought and sold at a market-clearing price, to the level where supply equals demand. Within this system, individuals would create information accounts at specialised institution, where they would deposit their personal information. Depositors would then grant to potential information users the right to use their information after paying the market price for it. The use of information would be limited to a specific period of time, and maybe, for specific purposes. The specialised information banks would have the role to aggregate the personal information deposited by their clients, retaining a part of the payment for covering the costs of their current operations.

This system implies a strict control of the information transfer in the society, possible enforced and maintained by the government. This model, although interesting and ingenious, neglects the multiple possibilities to collect, store and process information in a networked society, centred around the Internet, as a global, unregulated communication channel.

A possible online alternative would be the use of specialised cybermediaries, that can negotiate on behalf of their clients with online commercial organisations, in order to get a better deal and protect the use of personal information. However, the main problem remains: the negotiation would take place in the present online environment, which does not offer an appropriate protocol for a conflictual dialogue between users (or cybermediaries) and organisations. The negotiating aspects of personal privacy should be embedded into the technological tools of online interaction.

This is already happening: in May 1998, the Web Standards Organisation has released the first public draft of the Platform for privacy preferences, or P3P – a protocol meant to provide an automatic. Common web language for the acceptable use of personal information (Cranor, 1998). A P3P-compatible browser automatically detects a Web site's privacy policy, and depending on the level of promised protection, releases or not the customer's personal information. If the business practices do not satisfy the privacy standards, the P3p protocol tries to negotiate alternative terms or, as a last resort, notifies the user, who then decides how to proceed (Oakes, 1998).

The P3P protocol still has many critics, but its possible limitations should be considered as problems to be solved and not as valid grounds for eliminating the entire concept. For example, it not clear how the protocol would be able to improve the control over the use of personal information accounts and to track down any possible infringement of the negotiated clauses. This will imply an increase in the

governmental and inter-governmental control over the use of online information, which is considered unacceptable by the militants against Internet censorship. Another way will be the introduction of a voluntary auditing system, in which the online organisations will be monitored by independent assessors (possible specialised cybermediaries). The organisations infringing the protocol will be denied the ‘seal of approval’, that can become a differentiating sign between ethically correct and ‘rogue’ companies.

Concluding remarks

Privacy rights and policies represent a subject of intense concern, debate and research world-wide (Cranor, 1998). The explosive development of the Internet has only highlighted this problem of the modern-day society.

Various research approaches can be used to further study this phenomenon:

- surveys and analysis of the level of privacy described in companies’ disclaimers, as well as the real versus the perceived protection provided by these statements;
- surveys of the public opinion regarding online privacy, and analyses of the relation between privacy standards and consumer trust;
- studies regarding the use by individuals of specific tools of privacy protection, such as encryption programmes or anonymizer applications, and their effectiveness.

Online privacy will continue to provoke debate until a dynamic, adaptable solution will be found and implemented. This solution should balance the interests of individual customers with those of commercial organisation, and with the values of the present-day society. The definition and enforcement of privacy rights should represent a compromise between responsible individuals and ethical organisations, depending on the particular circumstances of every interaction. More than anything else, this ongoing interest and debate demonstrate that privacy is far to be dead. On the contrary it is very much alive and kicking...

References:

- Ackerman, M.S., Cranor, L.F. and Reagle, J. (1999) “Privacy in E-Commerce: Examining User Scenarios and Privacy Preferences”, Proceedings of the 1st ACM conference on Electronic commerce, Denver, Colorado, United States, pp.1-8.
- Castells, M. (2001) *The Internet Galaxy. Reflections on the Internet, Business, and Society*, Oxford University Press, Oxford.
- Cranor, L.F. (1998) “Internet Privacy: A Public Concern”, *netWorker: The Craft of Network Computing*, 2(3), pp. 13-18.
- DTI (2003) “The Directive on Privacy and Electronic Communications”, http://www.dti.gov.uk/ind...electronic_communications_200258ec.html, [accessed May 2003].
- Desai, M.S., Richards, T.C. and Desai, K.J. (2003) “E-commerce policies and customer privacy”, *Information Management & Computer Security*, 11(1), pp. 19-27.
- Foucault, M. (1977) *Discipline and Punish: The Birth of the Prison*, Vintage Books, New York.

- Frye, C.D. (2001) *Privacy-enhanced Business: Adapting to the Online Environment*, Quorum Books, Westport.
- Gavison, R. (1980) "Privacy and the limits of law", *Yale Law Journal*, 89(3), pp. 421-471.
- Habermas, J. (1987) *The Theory of Communicative Action*, Beacon Press, Boston.
- Hassan, R. (1999) "Globalization: Information Technology and Culture within the Space Economy of Late Capitalism", *Information, Communication & Society*, 2(3), pp. 300-317.
- Jarvis, S. (2001) "Maybe this year stricter internet privacy laws may emerge", *Marketing News*, 35(9), pp. 14-15.
- Kling, R. and Allen, J. P. (1996) "How the Marriage of Management and Computing Intensifies the Struggle for Personal Privacy", in D. Lyon & E. Zureik (eds.), *Computers, Surveillance, and Privacy*, University of Minnesota Press, Minneapolis, pp. 104-131.
- Kotler, P. and Armstrong, P. (1996). *Principles in Marketing*. Prentice Hall, Englewood Cliffs.
- Laudon, K.C. (1986) *Dossier Society*, Columbia University Press, New York.
- Laudon, K.C. (1996) "Markets and Privacy", *Communications of the AMC*, 39(9), pp. 92-104.
- Lillington, Karlin (1998) "Hands off that data - I'm European!", *Salon*, July 7, <http://archive.salon.com/21st/feature/1998/07/07feature2.html>, [accessed May 2003].
- Lombardo, T. (2003) "A Draft on a Philosophy for the Future", <http://futures.rio.maricopa.edu/philosophythemes.html>, [accessed October, 2003].
- Mabley, K. (2000) "Privacy vs. Personalisation", *Cyberdialogue*, <http://www.cyberdialogue.com/library/pdfs/wp-cd-2000-privacy.pdf>, [accessed September 2003].
- Mohr, R.D. (1995) "The Perils of Postmodernism", <http://hem.passagen.se/nicb/mohr.htm>, [accessed September 2003].
- Nakra, P. (2001) "Consumer privacy rights: CPR and the age of the Internet", *Management Decision*, 39(4), pp. 272-279.
- Oakes, C. (1998) "Privacy as Computer Language", *Wired News*, 21 May, www.wired.com/news/technology/0,1282,12425,00.html, [accessed September 2003].
- Oakes, C. (2000) "Expedia Rewrites Privacy Rules", *Wired news*, 19 September, <http://wired.com/news/print/0,1294,38852,00.html>, [accessed September 2003].
- Ó Baoill, A. (2000) "Slashdot and the Public Sphere", *First Monday*, 5(9), http://firstmonday.org/issues/issue5_9/baoill/index.html, [accessed September 2003].
- Poster, M (1995) "CyberDemocracy: Internet and the Public Sphere", <http://www.hnet.uci.edu/mposter/writings/democ.html>, [accessed September 2003].
- Privacilla (2003) "Privacilla's Two-Part Definition of Privacy", <http://www.privacilla.org/fundamentals/privacydefinition.html>, [accessed October 2003].
- Privacy Journal (2003) "Activism: Privacy", <http://www.activism.net/privacy/>, [accessed October 2003].
- Robinson, G.P. (2002) "A Mythic Perspective of Commodification on the World Wide Web", *First Monday*, 7(3), http://www.firstmonday.dk/issues/issue7_3/robinson/index.html, [accessed September 2003].
- Rombel, A. (2001) "The privacy law debate: navigating the privacy law divide", *Global Finance*, 15(1), New York, p. 28.

- Singer, B. (2002) "Against data Determinism in a Networked World", <http://www.bsing.net/toc.html>, [accessed September 2003].
- Warren, S.D. and Brandeis, L.D. (1890) "The right to privacy", *Harvard Law Review*, 193, pp. 193-220.
- Westin, A.F. (1967) *Privacy and Freedom*, Atheneum, New York.
- Zwick, D. and Dholakia, N. (1999) "Models of Privacy in the Digital Age: Implications for Marketing and E-Commerce", ritim.cba.uri.edu/Working%20Papers/Privacy-Models-Paper%5B1%5D.pdf, [accessed November 2003].
- Zlatev, Z. and Eck, P. van (2003) "An Investigation of the Negotiation Domain for Electronic Commerce Information Systems", in: Camp, O., Filipe, J., Hammoudi, S. and Piattini, M. (eds.), *Proceedings of the Fifth International Conference on Enterprise Information Systems, ICEIS 2003, Angers, France, April 23-26. Volume 4*, pp. 386-391.