Category: Applications of E-Technologies

Negotiating Online Privacy Rights

Călin Gurău
Groupe Sup. de Co. Montpellier, France

INTRODUCTION

The *Privacy Journal* (2003), a print newsletter and 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." Similar definitions are provided by law specialists (Gavison, 1980; Warren & Brandies, 1890).

The *networked society* changes the way in which *privacy rights* are defined, 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 & Allen, 1996). Advances in computing technology—that represents the infrastructure of the networked society—make possible to collect, store, analyze, and retrieve personal information created in the process of participation.

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. The study proposes a negotiating model of online privacy rights, and analyses the necessary conditions for the implementation of this model on the *Internet*.

The new economy is redefined on the basis of information entrepreneurism (Kling & Allen, 1996; Zwick & Dholakia, 1999). This cultural paradigm emphasizes 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, a system of perfect surveillance and control.

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

a. Web tracking devices that collect information about the online behavior of the user (e.g., *cookies*);
b. The misuse of the personal information provided by the online user in exchange of specific benefits: increased personalization, 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 users. The surveillance is initiated by the simple act of presence on the Internet. Specialized software applications, such as cookies are tracking the online behavior of Internet users, feeding the data into databases, which create and permanently update a profile of online consumers. These profiles are then used for segmenting the market and targeting the most profitable consumers.

A company can use cookies for various valid reasons: security, personalization, marketing, customer service, etc., however, there is an important distinction between cookies, which are active only within a specific Web site, 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, some 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 was transferred through an unmarked Internet channel to a 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.

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). U.S. privacy statutes have primarily focused so far on protecting consumers' financial data, health information, and children's personal information (Desai, Richards, & Desai, 2003; Frye, 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:

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 purpose 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. Despite these legislative efforts, it is not yet clear how effective are the measures implemented by 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.

THE DESCRIPTION OF A NEGOTIATION MODEL FOR ONLINE PRIVACY RIGHTS

The relativism of personal rights in the networked society 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 & van Eck, 2003): parties, rules (a negotiation protocol), a system of law enforcement (established and maintain by regulators), and specific benefits to be negotiated by the parties (negotiation objects).

In an online situation, the parties negotiating privacy rights are often in a position of inequality. Most privacy statements and disclaimers act as a standardized 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 his or her personal information, as part of the online deal, he or she has no direct possibility to control the way in which the organization uses this information. The storage, retrieving and processing of information are fully covert, and the only hope of the Internet user is that the company will respect its promises.

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 institutions, where they would deposit their personal information. Depositors would then grant to potential information users the right to use the 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, possibly 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, centered 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 organizations, 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 organizations. The negotiating aspects of personal privacy should be embedded into the technological tools of online interaction.