Chapter 7.11
Negotiating Online Privacy Rights

Cãlin Gurãu
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 chapter, 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.

Copyright © 2008, IGI Global, distributing in print or electronic forms without written permission of IGI Global is prohibited.

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

5 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage: www.igi-global.com/chapter/negotiating-online-privacy-rights/23286

Related Content

Wearable Computing: Security Challenges, BYOD, Privacy, and Legal Aspects
John Lindströmand Claas Hanken (2014). *Analyzing Security, Trust, and Crime in the Digital World (pp. 96-120).*
www.irma-international.org/chapter/wearable-computing/103813

Effective Malware Analysis Using Stealth Breakpoints
Amit Vasudevan (2012). *Threats, Countermeasures, and Advances in Applied Information Security (pp. 444-461).*
www.irma-international.org/chapter/effective-malware-analysis-using-stealth/65782

A Simple and Fast Medical Image Encryption System Using Chaos-Based Shifting Techniques
Sachikanta Dash, Sasmita Padhy, Bodhisatwa Parija, T. Rojashreeand K. Abhimanyu Kumar Patro (2022). *International Journal of Information Security and Privacy (pp. 1-24).*
www.irma-international.org/article/a-simple-and-fast-medical-image-encryption-system-using-chaos-based-shifting-techniques/303669

Proxy-3S: A New Security Policies-Based Proxy for Efficient Distributed Virtual Machines Management in Mobile
Boubakeur Annaneand Alti Adel (2022). *International Journal of Information Security and Privacy (pp. 1-38).*
www.irma-international.org/article/proxy-3s/285022

Will it be Disclosure or Fabrication of Personal Information? An Examination of Persuasion Strategies on Prospective Employees
Xun Liand Radhika Santhanam (2008). *International Journal of Information Security and Privacy (pp. 91-109).*
www.irma-international.org/article/will-disclosure-fabrication-personal-information/2494