Online Privacy Issues

Hy Sockel
DIKW Management Group, USA

Kuanchin Chen
Western Michigan University, USA

Louis K. Falk
University of Texas at Brownsville, USA

WHAT IS ONLINE PRIVACY?

Businesses need to understand privacy conditions and implications to ensure that they are in compliance with legal constraints and do not step on consumers' rights for privacy. Personal identifiable information (PII) and data can have innate importance to an organization. Some organizations view certain privacy features as essential components of their product or services; for example, profile data is often used to tailor products specifically for their customers' likes and needs. PII can also be used for less-honorable endeavors such as identity theft, phishing, political sabotage, character annihilation, spamming, and stalking.

One of the core issues of privacy is: Who actually owns the data, the holder of the data, or the subject (persons) of the data? The answer depends on many criteria: the users' perspective, the environment that privacy is addressed, and how the data are collected and used. Privacy issues arise because nearly every activity on the Internet leaves traces somewhere. This audit trail has caused many people to be concerned that this data may be inappropriately used. The paradox is that many businesses are also concerned for a different reason. In this age of legislation and litigation, a "minor" misstep or software glitch could easily put businesses in a position of extreme jeopardy. A data breach at T.J. Maxx that allowed hackers to download over 45 million credit/debit card numbers could literally bankrupt the organization. The damage and fines could easily total more than $4.5 billion; some have the figure as high as $8 billion (Ou, 2007). It is important to state that the governments' approach to the protection of personal privacy is neither equal nor universal. Some localities extend protection much further than others. In 1972, California amended its constitution to specifically include the construct of "a resident's inalienable right to privacy." Within the United States, court decisions dealing with privacy have fairly closely upheld two principles (Freedman, 1987):

1. The right to privacy is NOT an absolute. An individual's privacy has to be tempered with the needs of society; and
2. The public's right to know is superior to the individual's right of privacy.

However, some large communities were very slow in becoming involved; Japan did not pass its major protection law ("the Act on the Protection of Personal Information") to protect consumers and to regulate business until 2005 (Yamazaki, 2005).

VIOLATION OF PRIVACY AS AN UNACCEPTABLE BEHAVIOR

The Internet Activities Board (IAB) issued a Request for Comment (RFC-1087) in 1989 dealing with what they characterized as the proper use of Internet resources. Prominent on the IAB's list of what it considers as unethical and unacceptable Internet behavior is the act that "compromises the privacy of users." The reliable operation of the Internet and the responsible use of its resources are of common interest and concern for its users, operators, and sponsors (Stevens, 2002).

Using the Internet to violate people's privacy by targeting them for abusive, corrosive comments, or threats is not only unacceptable, but it is illegal. Privacy violations can do a lot more than just embarrass individuals. Information can be used in blackmail or otherwise coercive behavior. Institutions could use information to deny loans, insurance, or jobs because of medical, sexual orientation, or religion. People could

lose their jobs if their bosses were to discover private details of their personal life.

Not long ago, the people that perpetrate these crimes—crackers—were basically ego-driven; they wanted to see their exploits on the news. However, now it is about money! Attacks today are more sophisticated, designed to capture personal and financial information. In 2006, the terms Crimeware and Ransomware were coined to describe these threats. Crimeware encompasses threats that lie, cheat, or steal to profit from unsuspecting users. Ransomware is an insidious form of blackmail where crackers encrypt the users' data and then try to extort money from them by holding their files "hostage" (Lozada, Lagrimas, Corpin, Avena, Perez, Cruz, & Oliveria, 2007).

ONLINE PRIVACY AND DATA COLLECTION

Online privacy concerns arise when PII is collected online without the consumers' knowledge or consent, and is then disseminated without the individual's "blessing." Dhillon and Moores (2001) found that the top-five list of Internet privacy concerns include: (a) personal information is sold to others; (b) theft of personal data by a third party; (c) loss of personal files; (d) hacker's damage to personal data; and (e) spam. Cockcroft (2002) suggested the following top privacy concerns: (a) unauthorized secondary use, (b) civil liberties, (c) identity theft, (d) data profiling, and (e) unauthorized plug-ins. Online privacy is generally considered as the right to be left alone and the right to be free from unreasonable intrusions. By extrapolation, one can label telemarketers, mass advertisements, "spam", online "banner ads", and even commercials to be relating directly to privacy issues because of the solitude and the intimacy dimension. Westin (1970) frames privacy into four dimensions:

a. **Solitude:** The state of being alone away from outside interference;
b. **Intimacy:** The state of privacy that one wants to enjoy from the outside world;
c. **Anonymity:** The state of being free of external surveillance; and
d. **Reserve:** The ability to control information about oneself.

While organizations can go the "extra mile" to safeguard the data through the data collection, transmission, and storage processes, this may not be sufficient to keep the client content private. Some businesses use the collected user information for credit-worthiness checks, mass customization, profiling, convenience, user tracking, logistics, location marketing, and individualized services. The issue sometimes breaks down as to who has more rights to control the data:

a. The organization that committed resources to collect and aggregate the data; or
b. The people about whom the data is concerned.

When information is collected, there is the matter of trust: Consumers have to decide if they trust the organization to use the data appropriately. The organization has to trust that the information they asked for represents the facts.

Violating privacy hurts everyone. If people no longer believe their data is safe and will be handled appropriately, there is less incentive for them to be honest. "Almost 95% of Web users have declined to provide personal information to Web sites at one time or another when asked" (Hoffman, Novak, & Peralta, 1999, p. 82). Of those individuals that do provide information, more than half of them have admitted to lying on collection forms and in interviews. Chen and Rea (2004) indicated that concern of unauthorized information use is highly related to passive reaction. Passive reaction is one type of privacy control where one simply ignores data collection requests. Users tend to exercise another privacy control - identity modification - when they are highly concerned about giving out personal information for any reason.

ACTIVITIES THAT CAN VIOLATE PERSONAL PRIVACY

Cookies and Web-Bugs

A cookie is a small amount of information that the Web server requests the user's browser to save on the user's machine. Cookies provide a method of creating persistent memory for an organization in the stateless environment of the native Internet. Organizations use cookies to collect information about the users and their online activities to "better serve" their clients,