Privacy–Dangers and Protections

William H. Friedman
University of Central Arkansas, USA

INDIVIDUAL AND SOCIAL CONCERNS

It is no wonder that the average citizen is concerned about the difficulty of guarding one's privacy. Now, your own cell phone can reveal your ever-changing whereabouts by means of "location technology" (Lagesse, 2003). Chips that receive coordinates from global positioning satellites now make it possible to locate persons, cars, merchandise, in short, whatever we value. Like most new technology, it is easy to see advantages as well as drawbacks. Some positives of location technology are that ambulances, police and fire services can reach victims more quickly; driving suggestions can be delivered in real time to motorists (thus helping to avoid traffic tie-ups and prevent getting lost); advertisers can inform potential customers of the existence of a nearby hotel, store or restaurant; stores utilizing RFID (see the **KEY TERMS** section for explanations of possibly unfamiliar terms) can trace merchandise movement to reduce waste, replenish inventory, and stem shoplifting. Some negatives are that nefarious agents can also use location technology to track their prey; location-tracking history can be subpoenaed by one's legal adversaries; and it is inevitable that corporations and government will have an interest in conducting such monitoring (Griffin & Whitehead, 2001, 2002).

Privacy is an area that involves governmental, legal, social, managerial, and technical matters. Claims to privacy rights usually involve one or more senses of the notion of privacy. Table 1 gives some idea of the main connotations of "privacy" that are relevant to and will be applied to information technology; hence, they form the basis for the following discussion.

The first definition embodies respect for a computer user's wish to be in an insulated, protected space; no individual or program should interfere with the user's computer activity in a way that unexpectedly and undesirably disturbs that user. This presupposes freedom from concern that someone might hack in to the system and disrupt it, or barge into a chat room. Intrusive pop-up advertisements and junk e-mail can also contravene the first notion of privacy.

The second definition would suggest that any form of even unconcealed monitoring is a breach of privacy. An important exception in many people's minds is that government agencies might need to monitor computer activity when there is reason to suspect criminal or terrorist activity. A very similar exception arises when employers (Haag, Cummings & McCubbrey, 2004) feel that certain employees are abusing computer privileges, not working appropriately, or are otherwise jeopardizing the company's welfare. This can happen when the employee's computer activity leaves the company open to litigation or when the employee discloses company secrets (Brandt, 2001). Each of these exceptional cases, in order to be tolerated in an otherwise free society, presupposes some warranted authority for the monitoring. Less malicious, but perhaps equally bothersome is commercial monitoring to learn our buying habits by observing our Web searches and purchasing proclivities. Cookies to achieve this end are deposited and visible in a "Cookies" folder on our hard drives. Even when only aggregate, not identifiable individual data are harvested, most people would reject such a practice as beginning to slide down a slippery slope of more serious privacy invasion (Hamilton, 2001).

The third sense of privacy appeals to a desire to be free from being the object of concealed surveillance. Governmental and other spies have tried to plant programs or devices in suspect computers to log activities without the users knowing about it and report what they do to a distant receiving station.

The fourth sense expresses our desire not to suffer anyone's forcing his/her way into our space in plain sight in order to seize our computer or copy our files, in complete disregard of our wishes to keep these to ourselves. To have any property or information taken by stealth is offensive, but even more so for information that might presumably be detrimental to our best interests, such as credit card numbers.

The fifth connotation (as used particularly in database contexts) pertains to the natural expectation that our computer files be reserved exclusively for our own dissemination and access. To lose exclusive control over access and dissemination of our data files leaves us open to blackmail, financial fraud (as with discovery of our credit card numbers), malicious mischief, and even identity theft. While crimes may seem to be the modus operandi of ordinary crooks, we must contend with hackers and "script kiddies" who engage in this sort of pursuit for sport and, of course, sometimes also for profit.

The sixth meaning expresses our concern that when we purchase something or register at a Web site, unless we opt in, we do not ordinarily wish to have the information entrusted to the site shared with any other party. An opt-in permission granted to the site should imply that one is later able to cancel the service, or "opt-out". A great deal of junk e-mail is delivered under the pretext that, at one point, one did opt-in for the program with a related third party, a statement that may or may not be correct.

Very few downloaders of software have the patience to inspect the license agreement that must receive assent before installation can proceed. Nearly everyone accepts it by checking "I agree" without actually scrolling and reading the extended window full of legalese. Unfortunately, the end-user license agreement may not indicate the full extent of what the software does. An honest EULA may state that the program performs anonymous profiling, an assurance that your computer activities are being documented for future use, but not with identifying characteristics of the user per se. This type of software is used to generate a marketing précis of one's interests and attributes. Thus, if you visit Web sites that feature a certain service or product, you may be directed to other Web sites that feature the same thing. Vendors advertise with spyware companies, because of the selective targeting offered. By catering to consumers' preferences as exhibited in Web browsing, they presumably also benefit because they are presented only with items that really interest them and are spared much spam. Despite this alleged advantage and with promises of not recording personal data, many consumers disapprove of this practice on general principles and try to delete the uninvited spyware, often a difficult if not impossible task.

There are many techniques to invade our privacy—in both hardware and software. Even the FBI is reputed to use the infamous but mysterious program, "Magic Lantern," to spy on criminals attempting to hide their activities when using encryption for their e-mail. "When the user types the password, Magic Lantern software would capture it, giving the agency the ability to decrypt users' communications" (Paulson, 2002).

A wide variety of such snares awaits law-abiding citizens as well, and can be conveniently lumped under the rubric of "spyware". Table 2 summarizes some of the spyware that can be used to violate privacy.

A person's first thought upon discovery of a parasite on his/her computer is how to remove it. Although parasites are not easily removed, anti-parasite programs can detect and remove them. In addition, several Web sites have parasite detection scripts that analyze your computer and provide you with removal instructions (for example, visit www.doxdesk.com/parasite). Parasites are often fellow travelers of demos and freeware that are offered on the Web. A surfer must take the trouble to read the small print that appears in the EULA and privacy policy at the bottom of most Web sites. Sometimes one can opt out of selecting any extra utility that asks be installed along with what you originally ordered.

Due care must be given to permission windows asking if you wish to run a certain program, the function of which is not totally clear. ActiveX controls on the Web cannot only install parasites that compromise our privacy but also install viruses. XSS involves everything: all sorts of nefarious activity such as account hijacking, changing of user settings, cookie theft, and fake advertising.

PRE-INTERNET LEGAL PROTECTION

While the U.S. Constitution does not explicitly mention a legal right to privacy, this right is traditionally considered to have been implied by the first, fourth, and fifth amendments to this constitution (Blumenfeld, 1998). The First Amendment does not really grant privacy in any of the senses mentioned earlier; instead, it guarantees free speech (which could pertain to the Internet, but not really to privacy). The fourth amendment prohibits unreasonable searches and seizures (applicable to data and computer equipment, of course). The Fifth Amendment states: "nor shall private property be taken for public use, without just

Table 1. The relevant senses of the concept of privacy

1. Freedom from being subjected to unwanted contact
2. Freedom from overt monitoring
3. Freedom from secret surveillance
4. Freedom from unauthorized intrusion
5. Confidentiality
6. Freedom from disclosure by others of personal data to unauthorized persons