



Privacy White Paper

Personal Privacy for Computer Users

**M. E. Kabay, PhD, CISSP
Associate Professor of Information Assurance
Dept. of Computer Information Systems
Norwich University, Northfield, VT
April 15, 2002**

TABLE OF CONTENTS

INTRODUCTION	3
CONCEPTS OF PRIVACY	4
TECHNOLOGICAL THREATS	7
<i>OFFICE SOFTWARE</i>	7
<i>MALWARE AND SPYWARE</i>	7
SUMMARY	9
ABOUT PESTPATROL	9
FURTHER READING	10
REFERENCES	11

INTRODUCTION

Computer users all over the world have consistently indicated that privacy is one of the key elements in their willingness or reluctance to using information technology¹. Collecting information about users has become a lucrative business, with some companies funding their activities primarily through the sale of marketing data or lists of potential customers with details that allow targeted contacts. Unsolicited commercial e-mail, or spam, has become a daily annoyance for millions of e-mail users. Telemarketing phone calls generate enormous resistance, especially when unscrupulous businesspeople call your home during the dinner hour or refuse to take victims off their calling lists. Grocery store loyalty cards not only provide discounts, they also track individual purchases; in some stores, customers' information allows specialized, targeted coupons to be printed at the cash register so that a competitor's product can be purchased at a discount on the next shopping trip.

On the interpersonal level, some people use Web-based services to look into the personal background of individuals on the Internet; employers use search engines and archives to read public postings by potential employees; and criminals sift through personal details to construct forged identities in the furtherance of identity theft. All these activities are possible without the use of computers, but they are greatly facilitated by the availability of large-scale databases online and of efficient search engines for collating data from different sources. Research that might have taken months of legwork, perhaps requiring personal visits to government offices to copy data laboriously by hand, can now be completed in minutes. As a result, finding out about people's lives has changed from one-by-one investigation into massive collation of data about millions of people at a time.

Personal computers have provided fertile ground for data collection about individuals. Many Web sites store information about individual users' browsing patterns in files called cookies, which reside on the user's hard disk. Cookies allow personalized views of a Web site; for example, an online bookstore can keep track of all the books that a user has searched for or requested additional information on. This information then allows the bookstore software to suggest additional titles that might interest that specific user. On a less friendly note, some users of particular software programs have been surprised to discover that their programs are placing unauthorized calls to data collection sites on the Internet to upload information about their systems or system usage.

All of these phenomena raise issues of privacy in the age of cyberspace. In this short paper, ordinary, non-technical users can get a sense of the fundamental issues that face all of us as we try to strike a balance between efficient commerce and our concerns about personal privacy.

CONCEPTS OF PRIVACY

Privacy can be thought of as the power to hide parts of the truth about oneself, or sometimes the power to control the use of truths about one that other people know. For example, many people would consider that the books they read or what they say in private to each other ought to remain private. In addition, the concept of *informational privacy* covers truths they may have revealed to others for specific purposes but that ought nonetheless to be controlled. Medical records, for instance, would seem to be *semi-private* under this view; a patient could reasonably approve having her gynecological data shared with doctors and nurses without wanting the details to be published in a newspaper or on the Web. Simson Garfinkel eloquently addresses the fluidity of privacy as follows: "Privacy isn't just about hiding things. It's about self-possession, autonomy, and integrity It's the right of people to control what details about their lives stay inside their own houses and what leaks to the outside."²

In United States legal theory, a statement by Justice Louis Brandeis sums up the American attitude towards privacy³:

"The makers of our Constitution . . . Sought to protect Americans in their beliefs, their thoughts, their emotions and their sensations. They conferred as against the Government, the right to be let alone – the most comprehensive of the rights of man and the right most valued by civilized men."

Under common law, invasion of privacy can consist of

- Intrusion upon a person's seclusion in a substantial manner that would offend a reasonable person, such as pointing telephoto lenses at a bedroom window;
- Appropriation of a person's name or likeness – of concern primarily to celebrities who object to unauthorized use of their name or image in advertising campaigns;
- Publicity given to someone's private life such as details of sexual conduct, medical or psychiatric history; and
- Publicity placing a person in a false light, such as insinuating that individuals support a particular political view when they don't.

One of the best definitions is as follows:

"Privacy:

- 1 The right of an entity (normally a person), acting in its own behalf, to determine the degree to which it will interact with its environment, including the degree to which the entity is willing to share information about itself with others
- 2 The right of individuals to control or influence what information related to them may be collected and stored and by whom and to whom that information may be disclosed⁴

Another key concept is that “There are two kinds of truth that the law might try to protect:

- 1 Truths about you that you have revealed to the public, either by giving some information over to someone else, or by being observed in public; or
- 2 Truths about you that you have kept private.”⁵

Prof. Lawrence Lessig analyzes conceptions of privacy into three major concerns: minimizing intrusion, maintaining human dignity and constraining the power of the state (what he calls the substantive conception).⁶

Cryptographer and security theorist Bruce Schneier makes an interesting point about the fundamental types of privacy violations: “There are two types of privacy violations—targeted attacks and data harvesting—and they are fundamentally different. In a targeted attack, an attacker wants to know everything about Alice. If ‘Alice’ is a person, it’s called stalking. If ‘Alice’ is a company, it’s called industrial espionage. If ‘Alice’ is a government, it’s called national intelligence or spying . . .” In contrast, writes Schneier, *data harvesting* uses inference to sift through different lists of data about large numbers of data subjects and allows the attacker to generate a list of people who fit specific selection criteria.⁷

The US Constitution does not specifically mention privacy, but the Fourth Amendment is usually applied when discussing government intrusion on people’s lives. The Amendment specifically forbids unreasonable search and seizure by government and law enforcement agents.

The distinction between government intrusion and intrusion by private commerce is important, because in the US, there are fewer privacy restrictions on private industry than on government. For example, buying a book, ordering a video, seeing a movie in a theater and eating in a restaurant have traditionally been seen as public activities; US law has said little about limiting observations of these kinds. Certainly financial information about consumers has been widely shared among lending institutions (including such unexpected entities as auto dealerships and appliance stores) and among credit agencies. The most important difference between government and private intrusions is that consumers can (often unknowingly) sign away their privacy rights by agreeing to contracts. End-user license agreements often contain language that specifically reduces a member’s or a user’s privacy rights.

In contrast, the European Union has promulgated much more stringent regulations – primarily the *Data Protection Directive*⁸ – on the sharing of private information – to the point of causing friction with US-based firms doing business in Europe⁹. Until 1998, there were serious limitations to how European countries could transfer personal data to firms doing business in the USA; however, the “Safe Harbor” agreement provided a framework that gave credibility to the non-governmental, self-regulatory strategies favored in the US¹⁰.

The US government has also progressed in national legislation to protect privacy. The two most important measures¹¹ are the Health Insurance Portability and Accountability Act (HIPAA)¹² that governs privacy of medical records and the Gramm-Leach-Bliley (GLB)¹³ Act that protects financial records about individuals.

In daily life, many people also have concerns about their privacy at work¹⁴. In general, in the USA, the *reasonable expectation of privacy* governs to what extent employers may monitor electronic communications *except personal phone calls*. Because organizations own or control their e-mail,

voice-mail and Internet-access systems, managers do have the right to monitor or intercept communications made via those media. However, it is generally accepted that employees be allowed to make personal phone calls from work; indeed, according to the Electronic Communications Privacy Act (ECPA)¹⁵, any manager monitoring a live phone call is supposed to stop listening as soon as it is clear that the call is a personal one. All of this monitoring supposes that employees are aware of the likelihood of monitoring and that monitoring is carried out in a fair, unbiased way that cannot be construed as harassment or persecution of individual employees. Normally, employees must sign waivers (in many places every year) stating that they understand that the communications channels provided by their employer are the property of and under the control of the employer and may be monitored or intercepted at any time. A good rule of thumb is that no one should be doing anything on employer-supplied equipment that they would be embarrassed to discuss with their manager. Certainly writing extensive personal e-mail messages at work or spending hours on the Web in searches that are unrelated to one's job will result in questions about an employee's level of productivity.

In Europe, in contrast to the US situation, all personal communications by employees, including telephone, e-mail and via the Internet, are considered private and therefore subject to the Data Protection Directive restrictions¹⁶.

TECHNOLOGICAL THREATS

Office software

Modern computer technology offers many avenues for violating users' privacy. For example, few users realize that if they allow Microsoft Office products to use "fast saves," they silently keep a full record of all the changes that they have made in a document. The same principle applies to changes made with "track changes" enabled. When such documents are sent to others, much more information may be revealed than expected; examples include comments from editors, reconsidered phrases, and even factual information that was supposed to be suppressed. Even the seemingly inoffensive Properties sheet may carry more freight than a user wants; many documents show the names of previous employers, details of managers' names and positions, and even comments that should not be made public. Before sending any MS-Office products to anyone else, all users should check to see that

- The properties sheet has no more information that they wish to reveal;
- They have unchecked "fast save" in the TOOLS | OPTIONS | SAVE menu;
- They have turned off TRACK CHANGES by using the TOOLS | TRACK CHANGES | ACCEPT OR REJECT CHANGES menu and converting all changes into decisions on the final copy to be released.

Malware and spyware

Malicious software such as viruses (programs that reproduce by inserting themselves into other programs) and worms (self-reproducing programs that propagate through networks) sometimes carry victims' documents with them. Recent examples of such privacy-busting malware include the Sircam worm¹⁷ and the Nimda virus-worm¹⁸.

*Spyware*¹⁹ is software that covertly transfers information about an unsuspecting user to a corporate site where the information can be collated and used for marketing or as material to be sold for a profit. Spyware often enters a system through freeware or shareware, especially those that are ad-supported²⁰. Some browser plug-ins that offer new functions may contain spyware. Even HTML-enabled e-mail sometimes contains tiny one-pixel graphics images (*Web bugs*) that reside on undocumented Web sites; reading such e-mail causes a hit on the data collection site, thus confirming that the message has been opened and allowing an advertiser to be charged for the potential exposure to another victim of covert monitoring²¹.

Many spyware products allow uncontrolled downloading of arbitrary code, thus threatening the integrity of the operating system; for example, the *update-dll.exe* file has already been found in three different versions in the wild, some of which may be transformed to download unauthorized code. This file is installed by the Aureate / Radiate toolkit, which is used in programs that currently reside on over 30 million computers today.

Spyware programs have also been demonstrated to cause browser and operating system crashes. For example, one of the files associated with the Aureate/Radiate toolkit is *advert.dll*, which is routinely removed by technical support personnel to stop repeated system crashes.²²

One way of discovering that a computer is infested with spyware is to set a personal firewall to alert the user whenever a new request for an outbound connection is made. Tools such as BlackIce²³, Norton Personal Firewall²⁴, and ZoneAlarm²⁵ provide such functions. In addition, a spyware-blocking tool called Silencer²⁶ can block all messages from being returned to spyware “mother ships.” Steve Gibson, a highly-respected programmer, makes a free utility called LeakTest²⁷ that checks your firewall or spyware-blocker to be sure that unauthorized messages are in fact being blocked.

Many spyware programs resist uninstallation; even after going through the uninstall routines, functional programs may persist and continue to communicate with their host systems (this is known as “phoning home” in a reference to the movie “E.T.”). It can be frustrating and time-consuming to remove all vestiges of unwanted spyware, and most users lack the technical ability to ferret through the system registry and file system looking for unauthorized entries.

Another category of threats to privacy is the remote-administration trojan, sometimes called *RAT*. These tools masquerade as legitimate programs for administrators to use when providing technical support; however, products such as BackOrifice²⁸, NetBus²⁹, and SubSeven³⁰ are *trojan horses*³¹ which include undocumented functions that allow unauthorized individuals to gain complete control over the compromised systems. Infested systems can show bizarre behavior, such as repeated opening and closing of the CD-ROM tray, disabled keyboards, and pop-up messages. Worse still, the remote attackers can extract all kinds of information, including screen snapshots, lists of files, copies of private files, and even keyboard logs showing the keys pressed while entering passwords. Any online activity, including instant messaging, is vulnerable to invasion by these stealthy invaders.

A number of products are available to address the removal of some or all of these types of malware. Aureate/Radiate DLL Remover³² and AdAware³³ from Lavasoft specifically address certain types of spyware; PestPatrol³⁴, from the company that commissioned this paper, addresses the removal of trojans, hacker tools and denial-of-service attack agents in addition to spyware and adware.

SUMMARY

There are many threats to privacy in this age of increasing connectivity. You can prevent compromise by criminals and by privacy-invading pest infestations by following these simple rules:

- Read the fine print before installing any software, and especially *adware* that is supported by channeling ads to your computer;
- Install and configure a personal firewall on your computer to identify and block unauthorized *outbound* connections as well as unauthorized inbound connections;
- Always run an antivirus program that updates itself automatically to counter new threats;
- Scan your system regularly with a tool like PestPatrol, which identifies and removes not only spyware but also many thousands of other pests³⁵ that can hurt your computer and your privacy.

ABOUT PESTPATROL

PestPatrol, Inc. is a Carlisle, PA based developer of anti-hacker tools founded in May 2000 by a team of security software professionals to counter the growing threat of malicious non-viral software. The company's founders, Robert C Bales and Dr David Stang, were the original founders of the National Computer Security Association (NCSA), later the ICSA and now known as TruSecure Corporation. The company's flagship product, PestPatrol™, detects and removes hacker, remote administration and distributed denial-of-service attack creation tools, trojans, spyware and adware. Further details about the company and a free evaluation version of the software may be downloaded at www.pestpatrol.com.

FURTHER READING

Alderman, E. & C. Kennedy (1997). *The Right to Privacy*. Vintage Books. ISBN 0-6797-4434-7. 411 pp.

Bosworth, S. & M. E. Kabay (2002), eds. *Computer Security Handbook, 4th Edition*. Wiley (New York). ISBN 0-471-41258-9. 1200 pp. Index.

Cate, F. H. & M. H. Armacost (1997). *Privacy in the Information Age*. The Brookings Institution. ISBN: 0-8157-1315-0. 248 pp.

CERT® Advisory CA-2001-20. *Continuing Threats to Home Users*.
<http://www.cert.org/advisories/CA-2001-20.html>

EPIC, the Electronic Privacy Information Center <http://www.epic.org>

Garfinkel, S. (2000). *Database Nation: The Death of Privacy in the 21st Century*. O'Reilly (Sebastopol, CA). ISBN 1-565-92653-6. vii + 312. Index.

Lessig, L., D. Post & E. Volokh (1997). *Cyberspace Law for Non-Lawyers*. Published via e-mail.
http://www.ssrn.com/update/lsn/cyberspace/csl_lessons.html

Hayes, B., H. Judy & J. Ritter (2002). "Privacy in Cyberspace." Chapter 52 of Bosworth & Kabay (see above).

Kabay, M. E. (2002). "Anonymity and Identity in Cyberspace." Chapter 53 of Bosworth & Kabay (see above).

PestPatrol Web Site:

- Overview <http://www.pestpatrol.com/Pestpatrol/index.asp>
- Frequently Asked Questions (FAQ) <http://www.pestpatrol.com/Support/FAQ/FAQ.asp>
- White Papers <http://www.pestpatrol.com/Whitepapers/Index.asp>

Privacy Rights Clearinghouse <http://www.privacyrights.org/>

Smith, R. E. (2000). *Ben Franklin's Web Site: Privacy and Curiosity from Plymouth Rock to the Internet*. Privacy Journal. ISBN: 0-9300-7214-6. 407 pp.

Whitaker, R. (2000). *The End of Privacy: How Total Surveillance Is Becoming a Reality*. New Press. ISBN 1-5658-4569-2. 208 pp.

REFERENCES

¹ For examples of privacy surveys, see <http://www.cdt.org/privacy/guide/introduction/surveyinfo.html>

² Garfinkel, S. (2000). *Database Nation: The Death of Privacy in the 21st Century*. O'Reilly (Sebastopol, CA). ISBN 1-56592-653-6. Ch.1, p.4.

³ Warren, S. & L. Brandeis (1890). The right to privacy. *Harvard Law Review* 4(193). Cited in Rosenoer, J. (1997). Ch. 4, p. 129. Louis Brandeis later served as an Associate Justice of the U.S. Supreme Court from 1916-1939 and is considered one of the greatest jurists of the United States.

⁴ Shirey, R. (1999). *Security Glossary*. <draft-shirey-security-glossary-00.txt> GTE Internetworking. Expiration date 3 February 2000.

⁵ Lessig, L., D. Post & E. Volokh (1997). *Cyberspace Law for Non-Lawyers*. Published via e-mail and archived at < http://www.ssrn.com/update/lsn/cyberspace/csl_lessons.html >. Privacy 1: Privacy law in cyberspace.

⁶ Lessig, L. (1999). *Code and Other Laws of Cyberspace*. Basic Books (New York). ISBN 0-465-03912-X. Ch. 11, p. 146 ff.

⁷ Schneier, B. (2000). *Secrets & Lies: Digital Security in a Networked World*. Wiley (New York). ISBN 0-471-25311-1. Ch. 2, p. 29 ff.

⁸ http://www.privacy.org/pi/intl_orgs/ec/eudp.html

⁹ The Council of Europe (COE) passed the landmark Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Information in 1981, the same year that the Organization for Economic Cooperation and Development (OECD) passed the Guidelines Governing the Protection of Privacy and Transborder Data Flows of Personal Information. These important documents eventually resulted in the European Union's Data Protection Directive, which took effect in 1998. The Directive specifically addresses responsibilities of data collectors towards data subjects, including informing the latter of

- The identity of the collector of the information;
- The uses or purposes for which it is collected;
- How they may exercise any available choices regarding its use;
- Where and to whom it may be transferred; and
- How data subjects may access information relating to themselves by an organization.

In addition, the Directive requires the consent of the data subjects to limit collection and distribution of personal information. Any use of data must be consistent with the original terms of the data collection. Data subjects are to have access to all information that is collected about them and must be given the right to correct errors. Databases of personal information are subject to strict security requirements, and all third-party recipients of such data must respect the original restrictions that the subjects agreed to. Most of the countries in the European Union and a number of others around the world have appointed official privacy commissioners to oversee the implementation of such legal protections.

¹⁰ <http://www.ita.doc.gov/td/ecom/menu.html>

¹¹ For an overview of the other legal provisions affecting privacy in the USA, see

<http://www.cdt.org/privacy/guide/introduction/>

¹² http://www4.law.cornell.edu/cgi-bin/htm_hl?DB=uscode&STEMMER=en&WORDS=hipaa+&COLOUR=Red&STYLE=s&URL=/uscode/42/1397ii.html; see also useful introduction at <http://www.hcfa.gov/medicaid/hipaa/default.asp>

¹³ <http://www.senate.gov/~banking/conf/grmleach.htm> and see overview at

http://www.gibsondunn.com/publications/Uploads/gdi_glb.asp

¹⁴ <http://www.privacyrights.org/fs/fs7-work.htm>

¹⁵ <http://www.cpsr.org/cpsr/privacy/wiretap/ecpa86.html>

¹⁶ For a collection of articles about the Directive, see

<http://www.business2.com/webguide/0,1660,4317,FF.html>

¹⁷ <http://www.symantec.com/avcenter/venc/data/w32.sircam.worm@mm.html>

¹⁸ <http://www.symantec.com/avcenter/venc/data/w32.nimda.a@mm.html>

¹⁹ <http://whatis.techtarget.com/definitionsSearchResults/1,289878,sid9,00.html?query=spyware>

²⁰ <http://www.spychecker.com/spyware.html>

²¹ <http://www.privacyfoundation.org/resources/webbug.asp>

²² <http://grc.com/oo/aureate.htm>

²³ <http://www.blackice.com>

²⁴ <http://www.symantec.com/sabu/nis/npf/>

²⁵ <http://www.zonelabs.com>

²⁶ <http://www.spychecker.com/silencer.html>

²⁷ <http://grc.com/files/leaktest.exe>

²⁸ http://www.cert.org/vul_notes/VN-98.07.backorifice.html

²⁹ <http://netsecurity.miningco.com/library/weekly/aa122898.htm>

³⁰ <http://www.safersite.com/PestInfo/S/SubSeven.asp>

³¹ <http://www.cert.org/advisories/CA-1999-02.html>

³² <http://www.spychecker.com/radiatorremover.html>

³³ <http://www.lavasoftusa.com/>

³⁴ <http://www.pestpatrol.com/>

³⁵ See <http://www.pestpatrol.com/PestInfo/default.asp> for the latest summary of known pests. At the time of writing (mid-April 2002), there were 38,874 pests recognized by PestPatrol.