The Web of Privacy: Business in the Information Age

Varun Grover, Liz Hall, and Scott Rosenberg

Over the last five years, with the proliferation of telecommunication networks such as the Internet, tremendous advances have been made in our ability to reduce the effects of geography and time in disseminating information. Businesses, individuals, governments, and other entities are all contributing to this exploding information infrastructure that is being codified and stored in a distributed fashion in databases around the world.

However, even as the technology facilitates free flow of data, the walls that once protected personal information continue to fall and the privacy rights of individuals and businesses are being challenged from many new directions. Although the issues surrounding personal privacy in the Information Age are as complex as they are vast, many of the most important issues can be understood by looking at the three major groups involved in the conduct of electronic commerce: the individual consumers, businesses, and the government.

This essay attempts to articulate the privacy issues in this evolving "information age" by taking a closer look at the various stakeholders in this forum. We examine the privacy of businesses versus that of individuals, then broaden the discussion to include the government and its interests versus those of both businesses and individuals. These two facets highlight some of the most contentious debates on the topic today.

THE PRIVACY RIGHTS OF BUSINESSES VS. INDIVIDUALS

The amazing capabilities of technology often place businesses and individuals at odds with each other in their desire to safeguard privacy. According to a 1995 Louis Harris poll, 80 percent of Americans agree that "consumers have lost all control over how personal information about them is circulated and used by companies" (Knecht 1995). Three areas define the levels of interaction a person has with business. Framing the discussion of this conflict, they are: the individual in the business (at work), the individual and the marketplace (shopping), and the individual on personal business (such as at the doctor's office).

Do we really want—or need—Big Brother and everyone else watching over our shoulders? Well, yes and no....

Privacy at Work

Advances in telecommunications have dramatically lowered coordination costs for businesses. The use of e-mail, company intranets, and the Internet has allowed firms to communicate far more readily and efficiently without a corresponding rise in overall costs. But although this may be beneficial, it is not without its drawbacks.

Allowing employees access to the World Wide Web through the corporate system can be counterproductive for a firm. Employees may browse various, nonbusiness-related sites on company time. Nielsen Media Research recently found that, counted together, IBM, Apple, and AT&T employees visited *Penthouse* Magazine's Web site 12,823 times in one month during 1996. Based on an average stay of 13 minutes, that amounts to 347 eight-hour days. New management monitoring tools, such as WinWhatWhere Corp.'s software that permits monitoring of employees' activities, both in terms of what programs they use and how much time they spend using them, might be a boon to managers.

Electronic mail, while facilitating far-flung communications, can also cost companies in productivity as employees write notes to friends or family during the work day. In addition, e-mail makes it easier than ever to spirit away company information. Now, in the blink of an eye, an employee can transmit proprietary data to someone who should never have access to it. It comes as no surprise, then, that companies usually reserve the right to read their employees' e-mail. This right is almost always held up in court, as a recent court case involving the Pillsbury Co. attests. When an employee sued Pillsbury, charging that his privacy rights had been violated when an inflammatory e-mail written to his supervisor was used as a basis to fire him, the court ruled that the employee had no reasonable expectation of privacy for a voluntarily written message.

However, issues that seem so clear from the company standpoint become very murky when examined from the employee's viewpoint. The biggest issue clearly is the monitoring of employee activities and e-mail. In many employees' opinions, the violation of their privacy simply to find the one, or perhaps two, wrongdoers in an organization is excessive. Instead, managers should monitor the output of their employees and encourage the development of trust in the workplace. Moreover, many employees contend that the *Penthouse* case is extreme—that most use of e-mail and the Web is simply a coffee break activity, a way to relax and get creative juices flowing again. They believe the work product should be the most important criterion in judging their performance, not the time spent on an Internet browser.

Finally, many companies that monitor their employees' computer activities do not inform the employees that they may be monitored. E-mail generated within a company's walls belongs to the company by law, thereby allowing the firm to use it as it sees fit. However, in a survey released by the American Society for Industrial Security, only 37 percent of all companies have written policies about the use of e-mail. Accordingly, many employees are not informed that their e-mail is being monitored. They often learn this after some instance of company monitoring becomes public knowledge. Employees are frustrated that personal letters they mail via the post office are protected by law, but electronic letters are not—a seemingly inconsistent policy from an individual's standpoint.

Privacy in the Marketplace

The issue that is perhaps the most widely debated and least understood is the use of personal information obtained through electronic means for marketing purposes. Such information comes in two basic types: (1) that which is obtained through more traditional electronic means, such as point-of-sales scanners, and (2) that which is obtained over the Web through the use of specialized tracking software. Both types are used by companies for their one-to-one marketing efforts.

The concept of one-to-one marketing, or "narrowcasting," is a result of the proliferation of electronic means that makes it easier than ever to find out detailed, personal information on consumers. This in turn allows a company to target specific customers with promotions designed especially for them. Bi-Lo, a popular food chain, offers customers its Bonus Card, which is scanned at the time of purchase and records exactly what was bought. The card allows Bi-Lo to send out promotions and advertisements likely to appeal to that specific customer. Thus, the benefits can be mutual.

However, there is a negative side to this point-of-sales system. Although Bi-Lo offers a proprietary system and does not sell its data, other chains *do* sell data to market research firms. This means that customers lose control of their information from the moment the supermarket decides to sell it. The supermarket, rather than the individual, decides who is a suitable customer for this information.

Further, even though Bi-Lo retains all the information it obtains, the company can still use it in ways customers might find objectionable. For example, a young unmarried woman who buys a pregnancy test is likely to feel that her privacy has been invaded if she begins receiving coupons for baby products. Even the postal service is guilty of selling data to marketers. Rep. Gary A. Condit (D-Calif.) contends that the USPS violated the Privacy Act of 1974 in permitting the sale of change-of-address information to direct marketers, thus allowing people to be targeted by new merchants virtually from the moment they set foot in their new home.

Perhaps most surprising of all is the consumer tracking that takes place on the Internet. Web surfers can be tracked in a variety of ways. One method is with a device called "cookies," a file contained on your hard drive under your browser directory that allows the Web to track what sites you visit and what you do there. The advantages of this are that it allows ads to be targeted according to your taste and, in some cases, lets you peruse several pages and make multiple purchases at the end of an Internet shopping trip rather than totaling up at the end of every page. The downside is that everything you do is being watched. As an example, the cookies file of one of the authors, who has only surfed the Web for pleasure half a dozen times, is shown in **Figure 1**.

In response to cookies, companies like PrivNet offer software such as their Internet Fast Forward (IFF), which erases the users' cyberfootprints. There are also services on the Web that permit one to browse the Web anonymously.

Many Internet advertising brokers specialize in watching over your shoulder as you surf. One of them, DoubleClick, tries to target the ads you see based on your operating system, software, Internet address, and reading habits. It seems difficult to believe that this kind of information is easily available, but it is. One of the authors dialed up an information service called Discreet Data (which assists in locating "hard-to-find" data) on the Web and in less than 10 seconds was given information on his accessed pages. Although the source address was incorrect, everything else was on target. Such information gives agencies like DoubleClick all they need to start tracking a person's activities on the Net.

It is crucial to note that it is currently difficult to obtain a person's actual name and address. Most often, this information is obtained when provided by patrons at Web sites. Some companies that operate sites sell these data. Other sites may be accessed by hackers looking for the consumer profile the site is likely to represent. Consequently, linking a particular person by name to his or her actual surfing habits should not yet be a real concern for Web visitors. However, when you sign up for a free service, such as a newspaper or e-mail provider, be aware that the information you give is almost certainly going to be used by marketers.

Large Internet-based databases also infringe on individual privacy. Internet phone books can allow virtually anyone, except those with unlisted numbers, to be found. One such product is P-TRAK by Lexis-Nexis, an Internet-based service that links a person's name with a current address, two previous addresses, and a phone number. The company recently received a barrage of complaints after Social Security numbers were added to the list, making it easier for individuals to become the targets of criminal activity, such as fraudulent credit card accounts. Some of these services even provide a map of the area in which an individual lives, creating an even greater security concern.

Many proponents of Internet-based, one-to-one marketing argue that marketers have been gathering information on consumers for years through mail-order purchases, magazine subscriptions, and the like. The Internet is simply an expansion of this effort. Moreover, one-to-one marketing allows companies to provide consumers with purchasing incentives they are likely to use—an approach many customers like. And because much of the information obtained is public, it requires no special protection. The difference, then, is that these new electronic methods make it easier to obtain personal information that was previously hidden because of the difficulty and cost of locating and collating it.

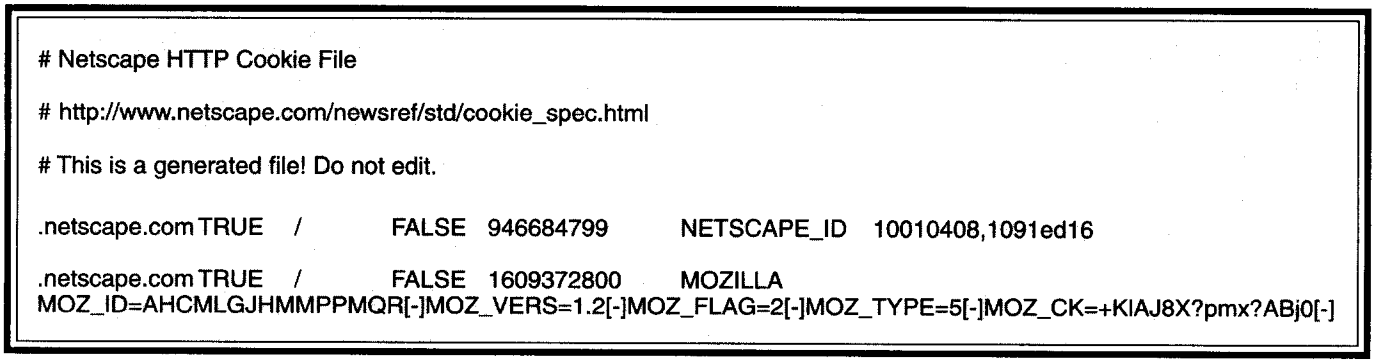
Personal Privacy: The Case of Healthcare

So who truly owns the medical records full of unintelligible scrawl that are generated whenever you go to the doctor? It may be surprising, but currently only 28 states have laws in effect granting people the right to see their medical records. Legally, medical records belong to the doctor or the hospital that treats the patient. This might lead individuals to think that if *they* cannot see them, no one else can either. However, nothing could be further from the truth.

In an effort to keep costs down, provide better service, and control an ever-growing mountain of paperwork, doctors' offices, laboratories, and hospitals are computerizing vast amounts of information about their patients. When an individual changes doctors or files an insurance claim, the information is often transferred electronically. This is where the problems begin.

Surprisingly, medical records are seen by more people than any other personal record.

Figure 1
Author's Cookies File



```
# Netscape HTTP Cookie File

# http://www.netscape.com/newsref/std/cookie_spec.html

# This is a generated file! Do not edit.

.netscape.com TRUE    /        FALSE   946684799       NETSCAPE_ID   10010408,1091ed16

.netscape.com TRUE    /        FALSE   1609372800      MOZILLA
MOZ_ID=AHCMLGJHMMPPMQR[-]MOZ_VERS=1.2[-]MOZ_FLAG=2[-]MOZ_TYPE=5[-]MOZ_CK=+KlAJ8X?pmx?ABj0[-]
```

They are transferred at lightning speed to a variety of institutions. And whereas it is possible for hackers outside the health care institution to gain access to the records contained in these databases, it is far more common for information leaks to occur within the institution. This can result in everything from a new employer learning about your past treatment for alcoholism to the reasonably innocuous flood of junk mail that may follow a child's birth. The crucial issue is that health care consumers have fewer privacy rights and less access to their medical records than many institutions.

"Although patients lose some privacy, they gain informed medical care when they may be most in need of it."

However, this issue is hardly so one-sided. The medical community has found these large databases to be a tremendous asset, permitting quick and easy access to needed information about patients. Doctors can thus treat more patients efficiently and attend to their needs in confidence. This could spell the potential end of malpractice resulting from the lack of vital medical history. Clearly, then, although patients lose some privacy, they gain informed medical care when they may be most in need of it.

The insurance industry has been plagued by fraud for years, and every insurance consumer pays the price for that. Use of these vast medical databases, and many others like them, allow insurance agencies to cut down on fraud and save honest consumers money. Yet even these insurance agencies struggle to protect the privacy rights of their best customers while trying to protect themselves from their worst.

ENTER "BIG BROTHER": BUSINESSES AND INDIVIDUALS VS. THE GOVERNMENT

As can be seen, the issues involving individual versus business privacy are complicated and multidimensional. Surprisingly, however, the issues surrounding individual and business privacy versus that of the government are even greater and more complicated. They run the gamut from regulating the Internet to maintaining national security. One of the hottest and most interesting privacy topics today is that of the use and exportation of *encryption,* a security measure designed to protect the privacy of transactions and communications.

From individual and business standpoints, good encryption is vital. Personal and business computers are increasingly at risk as we become interconnected with the world through the use of modems, networks, and the Internet. Hackers from outside the company can gain access to communications on intranets (internal company networks) and other related networks, thereby compromising the information being transmitted. According to security analyst Richard Power of the Computer Security Institute, the threat to companies of outside penetration "is well over 20 percent" (Geyelin 1995). The threat of inside penetration is even higher.

The theft of such information is not protected by the courts unless a company can prove that it took "reasonable precautions" to protect vital information. Just having to enter a password to access the system is no longer enough. Now companies must consider internal security audits—an often expensive and time-consuming process—in addition to encryption to meet the reasonable precautions requirement. Without security to stop them, companies are powerless to prevent the probing and often damaging raids of hackers and spies. These individuals may represent competitors or even a foreign government. Likewise, modern communications technology (electronic mail, cellular and wireless phones, and satellite communication) has made it easier to expose and violate our private conversations and letters.

For the past few years, a continuing battle has been waged between private groups, who fight to protect their privacy through the use of encryption, and the government, which worries that this protection will inhibit its ability to police society. It is interesting to note that their positions vary only in the degree of control ceded to the government. Both sides recognize that there must be a reasonable balance between the right to privacy and police powers of the state. The two camps of this debate are represented by Louis J. Freeh, director of the FBI, on the pro-government side, and various privacy groups, such as EPIC (Electronic Privacy Information Center), arguing for individual and corporate privacy.

The Clipper Chip

To help bridge the gap between itself and the groups advocating the use of strong encryption, the U.S. government has introduced what is known as the "Clipper Chip." As described by EPIC, this Clipper Chip

> is a cryptographic device purportedly intended to protect private communications while at the same time permitting government agents to obtain the "keys" upon presentation of what has been vaguely characterized as "legal authorization." The "keys" are held by two government "escrow agents" and would enable the government to access the encrypted private communication.

Over the past few years, Freeh has stressed that encryption is a "public safety issue." He simply wants to ensure that his agents have the "lawful court-authorized access that [they] have enjoyed for more than a quarter of a century to the conversations, the records, the plans of those who would break our laws." In fact, the government considers strong or "unbreakable" encryption as munitions, just like an F-16 or an AK-47. It is illegal to export any software product that has strong encryption, defined by the National Security Agency (NSA) as any encryption key longer than 40 bits. This is because it is easy for the U.S. government to break smaller keys. In plain English, this means you can't export anything the government can't break.

As one could imagine, companies and privacy rights groups take issue with the fact that the government would hold the "keys" to their encryption, allowing it virtually free and unrestrained access to private communiqués and transactions. Further, companies in the field of data encryption would be severely restricted in the exportation and use of their products, which often require global interoperability.

Business Control Over Encryption

Despite the important arguments raised by Freeh concerning the government's need for control over encryption technology, the rationale is not always easy to understand. Export restrictions on strong encryption are to ensure that very sophisticated code does not get into the hands of criminals and foreign terrorists. However, criminal elements can easily obtain excellent encryption products abroad. In fact, American limitations on encryption might encourage the development of superior products abroad. This would place U.S. encryption firms at a competitive disadvantage. American businesses and private citizens would be threatened by criminal acts planned and/or carried out over nets so secure that the acts might well be virtually impossible to trace. If the technology were developed within the United States, this sophisticated encryption would be available to American businesses and private citizens. They would benefit from the security provided by the technology even though they might still be vulnerable to attacks using it.

Similar issues arise when applied to potential domestic criminal activities. One of the most emotional arguments against encryption today is that the Internet, combined with encryption, would allow child pornographers, molesters, and any number of other negative influences to flourish. Yet technology is inherently neutral; the Internet and encryption are simply tools, albeit powerful ones. For every potential negative use, there are many more positive ones. For example, encryption will permit secure transactions over the Internet, a boon to both consumers and businesses. It will also ensure that the private communications of both businesses and individuals are more likely to stay that way. Rather than shying away from this new technology, we should work to control its abuse.

An excellent example from history would be the development of x-ray technology. When first developed, x-ray machines became almost like parlor games, with people getting x-rays as a form of entertainment at parties, not yet understanding the damage they were doing to their bodies. Soon health problems erupted from overexposure, necessitating the development of safeguards, such as the lead shields we currently use. X-ray technology now continues to benefit society every day in a completely safe manner.

"Encryption is not just about child pornographers; it is also about facilitating safe and secure commerce on a global scale."

Encryption is not just about child pornographers; it is also about facilitating safe and secure commerce on a global scale. All the potential benefits and risks of advanced encryption must be weighed before a logical decision can be reached regarding its use. Focusing on just one or two inflammatory issues may persuade citizens to forfeit their rights to privacy to ensure the perceived safety of children or other groups. This trade-off may not be necessary. In the process, these individuals could give up some very real benefits.

Recent Regulatory Developments

Legislation has become more and more slanted in favor of individual and business privacy. The recently proposed Clipper II would allow private entities to hold on to their keys until needed by the FBI. This year saw the introduction of two bills, one in the Senate and one in the House of Representatives, that supported the development of strong encryption technology, its export to other countries, and the right to use it.

The Promotion of Commerce Online in the Digital Era (Pro-CODE) Act was introduced to the Senate in 1997. It essentially restricts the Commerce Department's authority to establish technical standards for commercial encryption, prohibits state and federal governments from imposing a mandatory key-escrow system in which the government would have "back door" access to computer files, and relaxes export controls. In the House, a similar act was introduced: the Security and Freedom Through Encryption (SAFE) Act. This new legislation reflects the current shift in Washington's view of encryption.

Global interconnection, which is occurring much faster than electrification did a century ago, will have far-reaching effects on privacy that will be felt by virtually every person and organization that now possesses a modem or phone. Information privacy must be investigated in the context of a workable societal objective: an equitable balance between (1) the efficient functioning of society via a corporation's use of personal information, and (2) the individual's right to privacy in which "reasonable" procedures are in place to protect it. The stakeholders in this debate are the businesses with their profit motives, individuals with varying degrees of value placed on privacy, and the government as a purported representative of society.

In the debate between business and individual consumers, the issues are far from resolved. All parties concerned expect that information about them will be kept private through the ability to control access to that information. Access to information is often gained when an individual voluntarily releases it. However, access may also be the result of theft, corporate espionage, or misappropriation. Clearly, these thorny issues will not be easily legislated. However, we suspect that increasing consumer backlash will result in businesses having to pay a growing premium for access to consumer information. This might be in the form of incentives (such as discounts with special gold card membership) or in the form of new information technologies (such as smart cards) that allow consumers to control their own information or neutralize attempts at obtaining it without their permission.

New types of companies called "infomediaries" could seize on the opportunity to act as custodians of consumer information, marketing it to businesses on the consumer's behalf and protecting customer privacy to boot. This allows consumers to control the amount of information revealed and the price they are willing to accept for that information, possibly in the form of customized products and services.

In the debate between people and business versus the government, current regulations imply that limiting encryption is necessary given society's criminal elements. However, the fact that encryption is used in nefarious activities is a reflection of the activity, not the software involved. Fortunately, the movement to liberalize the regulations on encryption technology will likely continue. This would seem to be a positive development in the use of such tools to protect individual privacy and ensure the lasting growth and development of the Internet and international trade. ❐

References

Edward Baig, "How to Practice Safe Surfing," *Business Week*, September 9, 1996, pp. 120-121.

William M. Bulkeley, "Cryptographer is Told by U.S. that Case is Over," *Wall Street Journal*, January 12, 1996, p. B2.

Peter Cassidy, "New Crypto Controls: Big Step or Big Lie?" *Wired*, March 1997, p. 108.

Marilyn Chase, "Health Journal: How to Gain Access to Your Medical Files Amid Varied Laws," *Wall Street Journal*, December 2, 1996, p. B1.

Marilyn Chase, "Health Journal: You Can Take Steps to Close the Leaks in your Medical Files," *Wall Street Journal*, December 9, 1996, p. B1.

"E-mail Guidelines," *Association Management*, October 1996, p. 26.

EPIC, "The Clipper Chip," http//www.epic.org/crypto/clipper/

Louis J. Freeh, speech before the International Cryptography Institute, September 21, 1996, http:/www.fbi.gov/dirspch/crypto.htm

Louis J. Freeh, speech before the Senate Appropriations Committee on child pornography, April 8, 1997, http:/www.fbi.giv/congress/porn/pornsph.htm

Milo Geyelin, "Legal Beat: Why Many Businesses Can't Keep their Secrets," *Wall Street Journal*, November 20, 1995, p. B1.

J. Hagel and J.F. Rayport, "The Coming Battle for Customer Information," *Harvard Business Review*, January-February 1997, pp. 53-65.

Malcolm Howard, "No Freedom of Information," *Wired*, April 1997, pp. 90-96.

Albert R. Karr, "Administration Moves Toward Encryption," *Wall Street Journal*, July 15, 1996, p. B4.

G. Bruce Knecht, "Reporter's Notebook: Is Big Brother Watching your Dinner and Other Worries of Privacy Watchers," *Wall Street Journal*, November 9, 1995, p. B1.

Peter Kruger, "Identify Yourself," *Communications International*, October 1996, pp. 53-56.

Larry Lange, "Net Monitoring Tool Fuels Debate Over Privacy," *Electronic Engineering Times*, December 9, 1997, p. 24.

Todd Lappin, "Winning the Crypto Wars," *Wired*, May 1997, p. 94.

John Markoff, "Compromise Bills Due on Data Encryption," *New York Times*, March 4, 1996, p. D4.

John Markoff, "U.S. Fails in Global Proposal for Internet Eavesdropping," *New York Times,* March 27, 1997, p. A1.

Marianne Kolbasuk McGee, "E-mail Study Shows Few Constraints," *InformationWeek,* December 9, 1996, pp. 103-105.

Paul Miller, "NCOA Under Fire for Lax Oversight," *Catalog Age,* October 1, 1996, p. 5.

Zina Moukheiber, "DoubleClick Is Watching You," *Forbes,* November 4, 1996, pp. 342-344.

Zina Moukheiber, "OECD Adopts Guidelines for Cryptography Policy," March 27, 1997, http//www.oecd.org/news_and_events/release/nw97-24a.htm

Dan Pacheco and Michael Whitney, "Encryption Analysis," WashingtonPost.com

Richard Poynder, "Infringement of Privacy or a Big Fuss About Nothing?" *Information World Review,* November 1996, p. 16.

Steven Richards, "Privacy Rights Can Survive War on Insurance Fraud," *National Underwriter,* September 9, 1996, pp. 52, 59.

Joan Indiana Rigdon, "Management: Curbing Digital Dillydallying on the Job," *Wall Street Journal,* November 25, 1996, p. B1.

Ben Rothke, "Of Munitions and Encryption Software," *Storage Management Solutions,* July 1997; http://www.smsmag.com/articles/current/Munitions.html

David Sobel, "The Next Big FBI Lie," *Wired,* January 1996, p. 76.

Thomas E. Weber, "IBM Compromises on Encryption Keys," *Wall Street Journal,* January 18, 1996, p. B7.

Thomas E. Weber, "Net Interest: Browsers Beware—The Web Is Watching; But Your Privacy May Be Jeopardized Less Than You Think," *Wall Street Journal,* June 27, 1996, p. B8.

Stephen H. Wildstrom, "They're Watching You Online," *Business Week,* November 11, 1996, p. 19.

Bart Ziegler, "Group Blasts U.S. for Modifying Encryption Pact," *Wall Street Journal,* December 6, 1996, p. B2.

Varun Grover is a professor of information systems and Business Partnership Foundation Fellow at the University of South Carolina in Columbia, where **Liz Hall** and **Scott Rosenberg** recently graduated from the Master of International Business Studies program. This study was partially funded by USC's Center for International Business Education and Research (CIBER).