
PRIVACY! PARADISE LOST?

Introduction

Ethics—The Foundation We Need

The Importance of Privacy

Privacy—Does it Really Matter?

Reassessing Our Demand for Privacy

USA Patriot Act—A Wolf in Sheep's Clothing?

Data Sharing and Privacy—Why Are We Concerned?

Privacy and the Long Arm of the Law

Privacy and Self-Regulation

Privacy Concerns: Citizens and the Internet

Privacy versus Security?

Summary

Those that would sacrifice their freedom for safety will find they inherit neither.

—Ben Franklin

INTRODUCTION

What is privacy? When most of us think about privacy, if we do at all, we think about closed doors and drawn shades or hiding our actions from others. We must change the way we think about privacy. Perhaps we need a better word. If anything, privacy is more about the right to remain anonymous. It's the right to know we are not being watched as we walk down the street or attend a public meeting. It's the right to know that facts about our personal lives are revealed only as we decide to release them and that those facts are correct. Privacy is about massive databases, identity theft, and the access to information.¹ Ultimately, it is the need of individuals to feel safe and secure in their lives and the belief that those activities that they hold to be personal remain so—the ability to determine for one's self which data you disclose and to whom. Privacy—how do *you* define it?

Given society as it has evolved so far today, can we really expect to be in control of our own privacy? Living in an information-rich, information-dependent society and operating at Internet speed with archives of information at our electronic fingertips, can we be happy settling for anything less than full disclosure?

How many of us would take our automobile to a mechanic without first obtaining some information or recommendation, or investigating for ourselves the individual's ability and reputation? Very few marriages are undertaken without both parties having learned a great deal about each other. You won't receive that new bank card without someone taking a long look into your financial history.

Where do we get the information we use to make these major decisions as well as the countless minor ones we make daily? Information abounds, much of it available publicly or through specialty companies who sell it for a fee. Do you really know who knows what about you, how they obtained the data, or if that data is even accurate? Do you care? You should!

Privacy, or our right (it is a right—isn't it?) to keep our lives, activities, and personal information secure, safe and away from undesirable sources, is not a constitutionally provided or protected right. Of all of our inalienable rights put down by our forefathers, privacy, or our right to privacy, was (is) not one of them. The next time you have a moment, take a quick look at the U.S. Constitution (okay, scan it electronically). Do a key word search for the word "privacy." You won't find it. The U.S. Constitution does not guarantee U.S. citizens any right to privacy. What's a person to do?

We are told (more frequently these past many months) that as U.S. citizens we live in a free and open society. One must stop and wonder at times, how open and free? Open and free enough that anyone who wishes, with enough incentive, some discretionary funds, access to the Internet, good social engineering skills, and a little luck, can get almost any piece of information about our personal lives that they desire. Is this what we are willing to sacrifice for living in a free and open society?

Sometimes we cannot truly value something we have (or even perceive to have) until it is lost. Do we value our individual privacy? Do we truly value it? We stand on the brink of losing something we all (I believe we all) hold dear—our privacy. Many actually go on with their daily lives oblivious to this fact or with their heads in the sand.

What exactly is privacy? We've provided the classical definition, yet ask an average citizen, your co-worker, your daughter's soccer coach, to define privacy and see what type of response you get, if you get one at all. Blank stares maybe, shoulders shrugged, mumbled phrases, generic slogans, but no concrete answer. Why? Can we really formulate a universally acceptable, workable, visible definition of privacy? Probably not. Why? For every person in society, for every position, belief, role or responsibility, each will have his, her, their own view or perception of what is and what should be private and what privacy (or the concept of privacy) means to them. Maybe privacy, or attempting to define privacy, could be approached by looking at privacy's "component parts." How do we achieve privacy? It can be said that privacy is made up of equal parts trust and security.

Trust, the idea/concept one has or places in another, to act in a manner acceptable to both parties, with no resultant harm or adverse outcomes to either party. Do we "trust" an individual, a company, to use our information in a manner only related to the nature of our intended relationship, be it personal or business? How does one define trust? Can you touch it? See it? Hold it in your hand? Exactly what is trust? If we have difficulty defining, identifying, even establishing trust, how then can we do the same for privacy?

Security, in its broadest form, simply means being safe, keeping safe, and ensuring safety. How do we keep information, data, our personal data, safe and secure, away from prying eyes, unauthorized users, out of unsavory hands, away from companies who desire to use it for unrelated transactions? Part of ensuring our privacy requires a mechanism to be in place which will, as much as possible, guarantee the safety of our most personal data. Security may be easier to

identify, to see, even to touch; yet many times it remains as elusive as trust. One breach of either and you have lost both!

Ask anyone you know who has been a victim of an unauthorized use of his or her personal information and you can be sure that the word “violated” will come up during the conversation. Loss of privacy, especially one’s personal privacy, leaves the victim feeling violated, vulnerable, and exposed.

We would be remiss in our examination of privacy if we were to limit the building blocks of privacy to trust and security alone, regardless of their contribution and significance. There is an additional component essential to establishing privacy, as elusive as trust and to some degree security, that is the concept of ethics.

ETHICS—THE FOUNDATION WE NEED

Although laws are important to protect privacy, they need to be built upon a foundation. Ethics is the foundation suggested by some. Ethics is defined as a system or set of moral principles. The idea is that an ethical standard must be developed. The ethical standard will give strength to whatever laws are written. If this approach is taken, the first step is to establish ethical decision making. Ethical decision making will put legislators on the path to writing the type of laws that truly protect privacy. This approach of determining what is ethical and then developing a law to support that moral principle may prevent anyone from having to say in the future that a specific action was legal but not ethical.

The first step is to establish guidelines on what is ethical. There are some informal guidelines that many have heard since their childhood, which still hold true. Here are five common guidelines that can help a person test to see if an ethical dilemma exists.

1. *Shushers.* This is a situation where a person says, “Don’t say anything.” The person feels something unethical has happened but it should be kept a secret. Being shushed should trigger an internal moral alarm.
2. *The Mom test.* This is where you ask, “Would I tell my mother what I did?” Or, would you like it if your mother did what you did? Obviously, the Mom test uses a personal reaction as the first indicator that something is not right.
3. *The TV test.* This is where you ask yourself if you’d like to see what you did on national TV or in the *New York Times*. How would the public react to your story?
4. *The market test.* This approach is a little different from the others. The first three looked at the negative effect. The market test has you look at the positive effect. Would you publicize your behavior and use your action as a marketing tool?
5. *The smell test.* This is more or less a test of your gut feeling. Your unease may not be specific but you know in your bones that something is just not right.

There are formal guidelines that can be followed as well. Formal guidelines are generally a series of questions that must be answered and worked through in order to determine if an ethical dilemma exists. The following are some examples:

- Does this violate corporate policy?
- Does the action violate professional codes of conduct?
- Does the act violate the Golden Rule of “Do unto others, as you would have them do unto you”?

The informal and formal guideline approach can be built upon by using ethical principles. Principles go a little further than guidelines. Guidelines help people sense that a problem exists. Principles provide reasons for ethical behavior. There are three basic principles that can be utilized: deontology, teleology, and Kant's categorical imperative.

Deontology is the theory or study of moral obligation. This principle focuses on responsibility, and rights and duties. Rights are universal privileges that people consider inherent because of nature, tradition, or law. Information Technology generally involves discussions about three rights: the right to know, the right to privacy, and the right to property. The right to know must be tempered by questions such as to what extent we have this right. The right to privacy cuts both ways. People have their right to privacy concerning their personal information. Individuals must also realize that other people's personal information that they have access to through databases is subject to privacy, too.

The right to property can be related to our Information Technology hardware and software. Rules or controls are established to protect our Information Technology resources from misuse and abuse. So, although we have inherent rights, we must understand that with these rights comes responsibility. Therefore, we cannot use these rights as a bulldozer that buries the rights of others.

Duty is driven by the feeling that people are compelled by a moral obligation to do a specific action. Also, by accepting certain rights people incur corresponding duties. Here are some samples of what moralists consider personal duty. People have the duty to foster trust, to act with integrity, to do justice, to practice beneficence, to act with appropriate gratitude and make appropriate reparations, and to work toward self-improvement. Essentially, the premise behind acknowledging and accepting these duties is that we assume responsibility for our actions; consequently, those actions will be ethical. This concept can be brought down to earth a little by looking at it in a slightly different way.

Each person has professional relationships. These relationships are with employers, customers, employees, co-workers, and so on. In their relationship with their customers people have the responsibility to provide the product or service the customer requested or contracted. The customer has the responsibility to pay the negotiated price at the specified time. This thought process can be extended to privacy. People provide information to companies for their use in marketing their products, developing marketing strategies, and determining where to allocate their resources. People in turn expect that information to be used for its intended purpose and not be sold to others without their consent. In review, it is clear that rights and duties are related. If a person has and accepts a specific right, then that person incurs and must accept its related duty. This is fundamentally the definition of responsibility.²

Teleology is the next principle to discuss. A more common term for teleology is consequentialism. This concept looks at judging whether an action is right or wrong by its outcome. The focus is on the outcome resulting in the least harm to the many. Again, to restate this concept, teleology concentrates on considering the greater good. For the purpose of selecting a principle to guide us along the path of respecting privacy, there is a subset of consequentialism called utilitarianism. The principle of utilitarianism is group-centered, not self-centered. A key point here is that the individual is part of the group, and therefore benefits as well. Using this principle as a guideline for decision making should result in ethical decisions. This principle puts one in the realm of operating in the public interest. Therefore, people can evaluate such issues as personal privacy in terms of everyone involved.

The third principle is Kant's categorical imperative. Immanuel Kant, an eighteenth-century philosopher, formulated the categorical imperative, which contains two principles he named: consistency and respect. The principle of consistency goes beyond the basic concept of treating everyone equally. It demands that people refuse to act if harm will result. The principle of respect requires that people treat each other with dignity. This principle means people do not use other people. This can be extrapolated to mean that people will not use another person's personal information without his or her consent (i.e., they will not invade another person's privacy)³ and thus, forms the basis for the ethical use of data, and the ethical treatment of personal information by companies and individuals with access to these data.

The attainment of privacy in a virtual society is possible only when its basic components (trust, security, and ethics) are brought together and made to function in harmony and unison (see Exhibit 1.1).

THE IMPORTANCE OF PRIVACY

Exactly how important is our privacy, the perception of privacy, and the need for corporations to protect confidential, private consumer (and trading partner) data? Read on.

Privacy concerns remain high when it comes to shopping on-line. A vast majority of survey respondents from a PricewaterhouseCoopers survey (see Exhibit 1.2) think Web sites are responsible for asking individuals about sharing personal information, yet more than 40 percent believe they do not seek permission.

Exhibit 1.3 illustrates how consumers think an Internet company should be punished if it violated its stated privacy policy and used personal information in ways that it said it would not.

The world has changed significantly since September 11, 2001, or at least many individuals' view of a previously safe and secure world has changed. Many private, public, and governmental organizations are debating the pros/cons and the benefits/risks of national ID cards, biometric recognition technology and the granting of access to sensitive personal data in the name of national security. These actions *may* finally awaken individuals to more closely question and investigate the privacy policies (or lack thereof) of companies they do business with. Given this environment and social perception, companies may have to

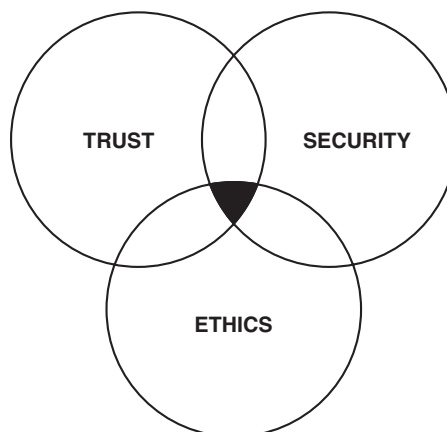


Exhibit 1.1. Privacy's Component Infrastructure

re-think their privacy strategies and redefine the role they see privacy playing in their relationships with their customers.

Analysts say e-commerce companies lose business when consumers don't trust that personal information will be carefully guarded. Forrester Research, Inc., in Cambridge, Massachusetts, estimates that total on-line spending in 2001 of \$46.7 billion would have been \$15 billion higher had it not been for consumer privacy concerns.⁴

Retail Web sites are responsible for asking me before sharing any personal information with other companies.

97%

Retail Web sites are responsible for asking me before using any of my personal information.

95%

It concerns me that retail Web sites store my credit card information online for future use.

65%

I shop from few retail Web sites to minimize overall access to my personal information.

48%

Retail Web sites do not ask my permission before sharing personal information with other firms.

44%

Retail Web sites do not ask my permission before using my personal information.

42%

I always turn cookies off.

29%

I prefer to pay for online purchases via an 800 number rather than entering credit card information online.

28%

Exhibit 1.2. On-line Privacy Survey

Source: *www.internetworld.com*, "Fast Forward," PricewaterhouseCoopers (January 1, 2001) 30.

The site should be placed on a list of fraudulent Web sites.

30%

The site owners should be fined.

27%

The site should be shut down.

26%

Company's owners should be sent to prison!

11%

Exhibit 1.3. How Privacy Policy Violators Should be Punished

Source: The Pew Internet and American Life Project, "Trust and Privacy Online: Why Americans Want to Rewrite the Rules" (August 20, 2000), *www.pewinternet.org/reports/toc.asp?Report=19*, Section Three: A Punishing Mood.

In a report by the Sageza Groups (formerly Zona Research) published prior to the September 11, 2001, terrorist attacks, 100 security professionals stated that their companies were not very concerned about offering Web customers an opportunity to get out of sharing their personal identifying information with third parties.⁵ Top priority concerns by the survey respondents were protecting access to customer data that had already been collected, and ensuring that the data could not be accessed or used by unauthorized third parties (see Exhibit 1.4).

Additional findings of interest from the Sageza survey include:

- Survey respondents indicated that their organizations had only a passing concern for liability issues related to practices involving customer data collection.
- Although more than half of the companies responding have privacy policies and note the same on Web pages, fewer than half disclose to customers what they do with the data they collect.
- Greater than half (58 percent) of those responding agreed that the government should require Web sites that collect identifiable personal information to comply with minimal privacy guidelines.

Sageza Group’s findings confirm those reported by Cutter Consortium. In Cutter Consortium’s E-Business Trends, Strategies and Technologies report released in 2000, e-businesses placed privacy low on their list of priorities, behind hackers (security), cost, overall reliability, user connection speed, and a lack of standards.

Of those responding, slightly over half (53 percent) had any formal privacy policy. Examining the results and numbers differently raises some concern for both users and organizations alike.

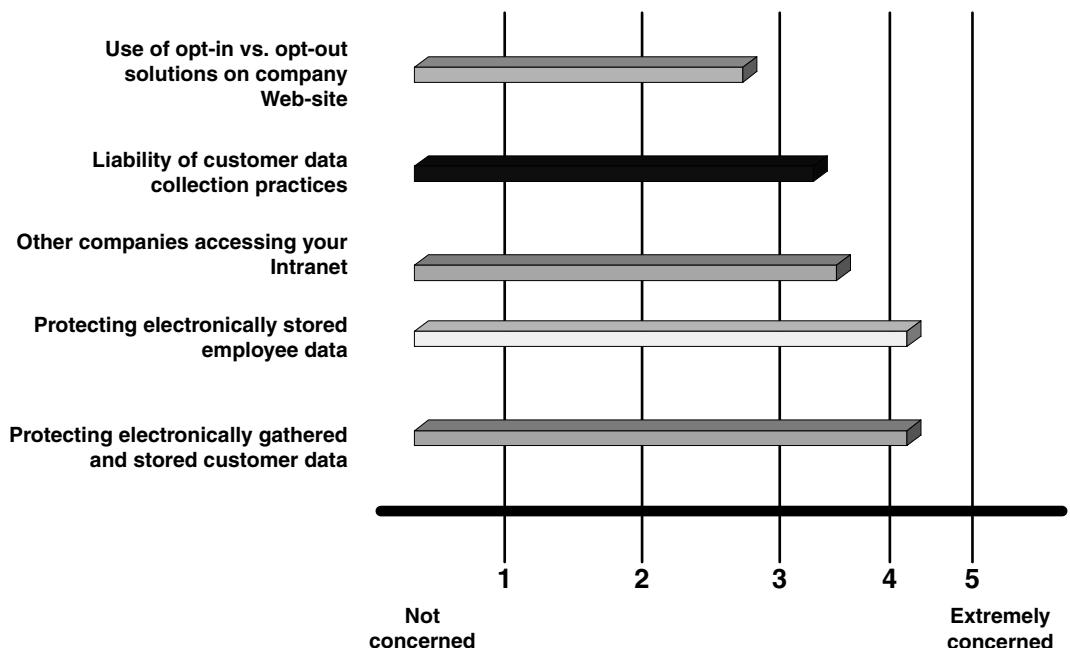


Exhibit 1.4. Privacy Hot Spots: How Concerned Is Your Company About These Privacy Issues?

Source: The Sageza Group, Inc., Mountain View, CA. Internet Study of 100 Security Professionals (multiple responses allowed), March 2002.

Given the results of the survey, 47 percent of e-businesses operating in virtual markets have no privacy policy, formal or not. This raises concern, or at least it should, with consumers as to what is being done with the data collected by these businesses and with whom they are sharing it.⁶

A more recent *Information Week* study of 300 information technology (IT) professionals asked the question: “Is government intervention necessary to ensure adequate privacy protection for users of the Internet?” The response is in Exhibit 1.5.

While it appears that public opinion still favors non-interference by government factions, the events of September 11, 2001, and the subsequent months have begun to change public opinion and spur the U.S. government into further action.

PRIVACY—DOES IT REALLY MATTER?

The privacy issue can be an emotional one and therefore the amount of press given it may be disproportionate to its actual significance. An effort must be made then to quantify the need for privacy. Is privacy the big issue many believe it is or is it a non-issue? There have been several surveys conducted in the last 23 years that address the importance of privacy. The surveys focused on information privacy and assessing individual opinions regarding privacy. One survey was conducted in 1989 among four separate companies.⁷ The companies were assigned generic names at their request; the survey distribution is shown in Exhibit 1.6. The first three questions of this survey help answer how important an issue privacy is for people. Question one was “Compared with other subjects on your mind, how important is personal privacy?” The respondents were given four choices: very important, somewhat important, not too important, and not important at all. Sixty-three percent said it was very important and another 30 percent said it was somewhat important.

The second question was “How concerned are you about the invasion of personal privacy in the United States today?” Again, the respondents were given four choices: very concerned, somewhat concerned, only a little concerned, and not concerned at all. Forty-five percent said they were

Exhibit 1.5. Is Government Intervention Necessary for Adequate Privacy Protection?

	2001	2000
Yes	31%	29%
No	64%	71%
Don't Know	5%	

Source: *InformationWeek* Research's Outlook for 2001 Study of 300 IT executives, www.informationweek.com/bizint/biz819/quality.htm#story5, InformationWeek Research (January 8, 2001).

Exhibit 1.6. 1989 Survey Distribution

Site	Number of surveys distributed	Number of surveys returned	Response rate
Bank A	373	213	57.1%
Life Insurance	100	68	68.0%
Credit Card	180	121	67.2%
Health Insurance	450	302	67.1%

Source: H. J. Smith, *Managing Privacy: Information Technology and Corporate America*, University of North Carolina Press (1994). Reprinted with permission.

very concerned and 44 percent said they were somewhat concerned. The third question is rather lengthy but narrows the focus significantly. Question three was “As computer usage increases in business and the general society, more and more information on individual consumers is being acquired and stored in various computers. How serious a threat to personal privacy is this development?” Again four choices were given: very serious threat, somewhat serious threat, only a slightly serious threat, and not a serious threat at all. Approximately 30 percent said it is a very serious threat. Forty-eight percent said it is a somewhat serious threat. The results of this first survey support the conclusion that privacy is a big issue. Over 90 percent of the respondents felt privacy was at least somewhat important; 89 percent were concerned about invasion of personal privacy; and at least 78 percent saw the accumulation of information on consumers as a threat to personal privacy.

The second survey is an opinion poll (see Exhibit 1.7) and the source of the information is from Equifax, Inc.⁸ The question this survey focused on was “How concerned are you about threats to your personal privacy in America today?” This question was asked in 1978, 1983, 1990, 1991, and 1992 polls.

The percentage of people very concerned or somewhat concerned went from about 65 percent in 1978 to about 78 percent in 1983. In each of the three survey years in the 1990s the results were in the 80 percentile. This second survey covers a longer period and a broader audience than the first. Although its numbers are a little lower than the first survey, the number of people concerned about threats to their personal privacy is significant and increasing.

The third survey was conducted via telephone from September 7 through September 10, 2000, by the *Seattle Times* and Northwest Cable News. The telephone interviews were conducted with 400 adults over the age of 18; all respondents had access to the Internet. The survey was conducted in Washington and Oregon and had an overall margin of sampling error of $\pm 5.0\%$. The results of this survey give mixed signals concerning privacy.

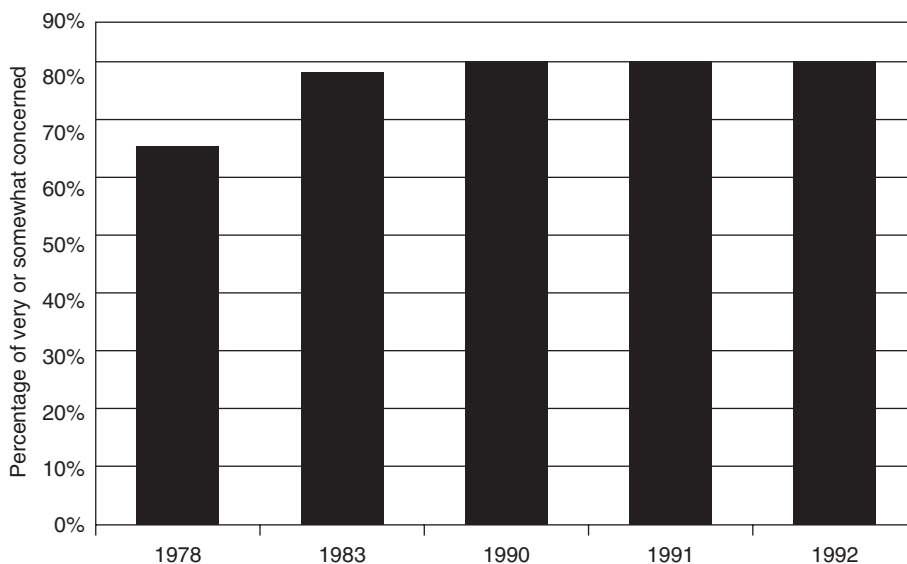


Exhibit 1.7. Level of Concern over Personal Property

Source: The Equifax Report on Consumers in the Information Age, conducted by Louis Harris & Associates and Dr. Alan F. Westin (1990); Equifax-Harris Consumer Privacy Survey, Equifax Inc., Atlanta, Georgia, and Louis Harris & Associates, New York (1992).

When asked how confident the person felt about the security and privacy of his or her financial transactions on the Internet, 56 percent answered very confident or somewhat confident. However, when asked if they were concerned about the question of privacy on-line, 71 percent said they were very concerned or somewhat concerned about privacy on-line. This appears contradictory. The answer may be that people feel that financial transactions are protected and that non-financial events are not protected.

USO Software, Inc., conducted a survey in October 2001. This survey was conducted with 500 Internet users to determine the effect of real and perceived privacy violations on consumer retail expenditures. The survey results exposed a broad range of privacy concerns. Eighty-nine percent believe those companies sharing credit card information without permission committed a privacy violation; 83 percent felt companies sharing names and home addresses without permission perpetrated a privacy violation. The analysis completed by USO Software, Inc., indicated that these privacy concerns cost retailers \$6.2 billion in lost business. Overall, it appears safe to state that privacy is a significant issue in the United States.⁹

REASSESSING OUR DEMAND FOR PRIVACY

When the numbers are examined, one feature stands out—public opinion about threats to personal privacy peaked in the 1990s and remains high. There appear to be two major forces driving this increased focus on privacy.

The first driving force is technological. One technological driver is that information is readily available in a computerized format rather than a paper format. This makes information easier to access and easier to transfer, and privacy harder to protect. The reason is the effort effect. Under a manual system, or even using pre-1980s technology, it took considerable effort to manipulate data into a meaningful form. Generally, access to data required multiple people. Consequently, although access was not denied, privacy was guaranteed mainly because misconduct required too much effort.

A second technological driver is the ability to join data items from multiple sources and draw inferences. Relational databases have given companies the power to pull data from both internal and external sources to create powerful information packages on anyone and everyone. This heightens concerns about the threat to privacy because these informational packages paint a more complete picture, and therefore seem more invasive.

A third related technological driver is the advent of the wide area network (WAN). WANs enhance inter-company interaction and information sharing. This high-speed information highway linking both private and public organizations makes information sharing very easy. Clearly there is a sense that control over personal data is much more difficult, and potential problems with data errors are quickly exacerbated. The final technological driver is the downsizing of companies' computing capabilities. Where most data were stored on mainframe computers, much of this information is now on personal computers. When data were centrally controlled, privacy safeguards were easier to establish. Now that control of data is decentralized, there are significant challenges concerning the safeguarding of personal privacy.

The second factor driving the focus on privacy is the increasing value of information. The marketing community is changing from a one-to-many marketing approach to a one-on-one marketing approach. This micro-marketing approach requires much more personal data on each individual. Information equals dollars and this equation has created an industry of its own.

Now that the threat to our privacy has been established as an important issue, the task is to locate the smoking gun. Is the computer the culprit? One way to answer this question is to borrow a concept from the gun control issue. Guns don’t kill people; people kill people. Computers don’t invade our privacy; people invade our privacy.

Arthur Miller said “the computer is capable of immense social good, or monumental harm, depending upon how human beings decide to use it.”¹⁰ The computer, or in a broader sense, Information Technology, is merely a tool. Information Technology is a tool with no mind of its own. Information Technology has no conscience. Information Technology has no independent capability to invade our privacy. What must be the concern and what must be dealt with is how people use and misuse the tool.¹¹

The impact of the brutal terrorist attack on the World Trade Center has heightened data-privacy concerns not only in the United States, but globally. In the wake of the attacks, in the United Kingdom for example, the National Hi-Tech Crime Unit (NHTCU) had asked telecommunication carriers and Internet service providers (ISPs) to preserve their data logs from September 11. Such requests tend to put pressure on existing privacy legislation and sometimes force it to be re-evaluated in ways which might contravene the privacy-protection legislation itself.

The actions of NHTCU in the United Kingdom tests the tenets of the United Kingdom’s Data Protection Act, while falling under the oversight of the Regulation of Investigatory Powers (RIP) Act. Legal and governmental powers around the globe are acting to address the need to access data, while at the same time, attempting to ensure the privacy of a free and open citizen population.

Just how far can legislation go? Do governments have a right (possibly a responsibility) to suspend privacy laws in an effort to secure and ensure national security? If these rights are suspended or investigative powers increased, how will they be reversed and returned to pre-terrorist levels when the necessary data has been obtained? Can they ever be? Will the guise of national security and a hunt for terrorists return our nation (or any nation) to an era of McCarthyism, this time fueled by the full power of technology? Will security and a perceived sense of safety trump privacy?

According to Gaylyn Cummins, a San Diego-based constitutional law attorney with Gray Cary Ware and Freidenrich, “Security concerns overwhelm privacy protection. Everything has changed.”¹² This has become the mantra among legislators and industry PACs (political action committees), all seeking to gain a foothold into the cracking fortress of privacy concerns once defended so viciously by consumers. Privacy obsessions have gone into a hasty hibernation. Some issues, like the fervor over cookies that allow Web surfing habits to be monitored, seem small when viewed through the lens of September 11, 2001.¹³

USA PATRIOT ACT—A WOLF IN SHEEP’S CLOTHING?

On October 25, 2001, President Bush signed into law the USA Patriot Act. This single piece of legislation may be destined to forever change the world of privacy and our ability to move about in that world.

The Act allows U.S. police (and associated colleagues) the right to browse educational, library, and medical data, as well as travel, credit, and immigration records, all in the name of tracking down possible terrorists in the hopes of preventing future attacks.

The Act expands the use of wiretapping and Internet monitoring, giving the government access to personal data records and allowing for secret searches. Some laws expire after four years

unless renewed; others remain in force unless amended.¹⁴ Does the Act go too far? Some privacy groups and civil liberty critics say, yes! The individuals who represent these groups say that the Act violates the civil liberties of U.S. citizens by giving the federal government too much access to personal, individualized data which may exist on-line, or in massive company databases.

The Act, along with associated legislation, may indeed foreshadow a decline in individual privacy rights and greater government intrusion into our personal lives than many individuals have witnessed before. Is this so bad? If you have nothing to hide, why worry? Would you be willing to give up or trade off some of your rights to personal privacy for a more secure society, for the “feeling” of being safer?

This is the argument often used by those who support more federal government access to personal, private data. But, how does one go about measuring the “feeling” of increased security? Can we ever feel completely secure? Does giving up my right to privacy ensure my improved safety and security? How can I prove this? Can I see improved safety? How do I know I am secure? I can quantify and tangibly identify when I am asked to provide personal data, or when my privacy may be challenged either directly or indirectly. Scarier, however, is my total lack of knowledge of the times my personal, confidential, and private data is accessed, reviewed, analyzed, cross-referenced and mixed, without my knowledge and/or consent.

Some critics of the Act state that such legislation strips authority from judicial authorities at a time of crisis and throws the nation back to a darker time. A time of the Alien and Sedition Acts of 1798, criminal restrictions on free speech during World War I, and the ever-present domestic spying rampant during the Cold War. Upon closer examination, the details of the Act shift the legal balance in favor of police powers, with hopes of early identification of potential terrorist activities aimed at U.S. infrastructure and citizens. In doing so, however, this same legislation, if not held to its strictest interpretation, could also weaken existing rights which currently exist to protect racial minorities, immigrants, prisoners, and students.

Current laws restrict the gathering of data for one purpose and using the same data for a second unrelated, yet potentially connected, purpose. The Patriot Act could markedly change that. Sharing data and making logical links, which may correlate seemingly unrelated data, is critical. This point could not be proven more correct given the events and aftermath of September 11. At what point, however, does sharing data go beyond the need for maintaining national security and invade privacy, which so many citizens have grown to believe is an inalienable right?

Lest we feel that the encroachment of government into our private lives is solely an American issue, the aftermath of September 11 has prompted governments globally to re-access and rewrite a broad range of legislation aimed at accessing data (of all types) in the face of (or in the name of) national security. The European Union already permits its member governments to bypass existing privacy laws when national security is threatened. Following the terrorist attacks in America, the European Union moved ahead with a bevy of legislative measures designed to combat terrorism and terrorist acts, tougher laws addressing money laundering, and an EU-wide search and arrest warrant.

DATA SHARING AND PRIVACY—WHY ARE WE CONCERNED?

Another question to address is: When did the invasion of personal privacy start? Is this concern an issue born in the 1990s or has it been around longer? Concern for personal privacy and an uneasiness with general privacy issues have appeared in surveys conducted throughout the

1970s, 1980s, and 1990s. Threats to personal privacy go back to the first time someone decided to borrow money. Myron Brenton, author of *The Privacy Invaders*, suggests that a creditor will lend the money only after “as much of your personal and financial history has been unearthed as he deems necessary.”¹⁵ The gathering of information to determine one’s ability to repay a loan seems a reasonable activity. Most people willingly disclose substantial amounts of personal information in order to secure loans. The personal information provided is generally supplemented by data on personal payment habits, and so forth. However, one might feel the credit bureau is stretching its information gathering “right” when it begins to ask neighbors, employers, and landlords about you the person. The major concern is that this hearsay is recorded along with your income and other factual information. Once information is recorded it is difficult to distinguish fiction or hearsay from fact.

Credit checks are one common source of invasion of privacy but clearly not the only one. The national census asks a series of personal questions every 10 years. While many may agree that determining where people live is essential to helping determine the number of congressional seats for a district, many of the questions asked have no relationship to this fundamental requirement. For example, the 2000 census form asks, “How well does this person speak English?” Another question is, “What time did this person usually leave home for work last week?” Many people questioned the need to provide answers to these types of questions. A third question on the census form asked what one’s wages, salary, and commissions were for 1999. The government already has this information on file with the Internal Revenue Service, so why ask for it again? A fourth example is the question about whether the person ever served in the military. Again, this information is on file with the Department of Defense; why have it in the census form?

Another tool used to invade our privacy is the Freedom of Information Act (FOIA). This Act permits the release of personal information gathered by the government to almost anyone who requests it. Title III of the Crime Control Act of 1968 gives law enforcement the statutory authority to wiretap and intercept certain communications. These authorities are augmented further through the passing of the Patriot Act. Whether one sees this as a necessary evil in order to combat crime is neither here nor there. The point is that this Act (FOIA) permits invasion of privacy under specified conditions. The First Amendment is another tool that can be used to invade our privacy. The press has often printed personal information about celebrities and others. Their “right” to do this has been upheld by the courts under the First Amendment—freedom of speech. This brief analysis illustrates that information technology isn’t the culprit. People are asking the probing questions, not information technology. Laws currently exist that sustain the violation of one’s privacy. People, not information technology, write these laws.

Big business is also invading employees’ privacy. The American Management Association (AMA) conducts an annual survey called Workplace Monitoring and Surveillance. The AMA started this survey in 1997 and now has five years of data; the results are shown in Exhibit 1.8.¹⁶ The alarming fact is that each year the amount of monitoring by employers has increased. Review of e-mail messages has increased from 14.9 percent (1997) to 46.5 percent (2001). Review of computer files has increased from 13.7 percent (1997) to 36.1 percent (2001). Clearly, Big Brother along with Big Business is watching!

The sharing of information between and among federal government agencies (as well as with corporations) can help, as supporters argue, to increase efficiency and reduce overhead expenses. However, these actions also directly threaten the anonymity of sensitive data and

Exhibit 1.8. Workplace Monitoring and Surveillance

	1997	1998	1999	2000	2001
Recording and reviewing of telephone conversations	10.4%	11.2%	10.6%	11.5%	11.9%
Storage and review of voice-mail messages	5.3%	5.3%	5.8%	6.8%	7.8%
Storage and review of computer files	13.7%	19.6%	21.4%	30.8%	36.1%
Storage and review of e-mail messages	14.9%	20.2%	27.0%	38.1%	46.5%

Source: 2001 AMA Survey Workplace Monitoring and Surveillance, www.amanet.org/research/pdfs/ems_short2001.pdf, American Management Association, adapted with permission.

expose (or disclose) the identity of individuals linked to that data. Such action thus presents new privacy concerns for U.S. citizens, and individuals in general, who may not be citizens but either living or working in the United States.

In a 172-page report entitled, “Record Linkage and Privacy: Issues in Creating New Federal Research and Statistical Information,” the General Accounting Office (GAO) explains that the increasingly common practice of linking data sets from several different agencies often creates new information about citizens (see Exhibit 1.9).¹⁷ That new data can in turn be used to unwittingly or maliciously identify citizens whose identity was previously masked by the separation of that data.

The sharing of information between agencies can benefit citizens. However, if this information is misused, it can be a nightmare with the potential of disclosing previously confidential and private information (see Exhibit 1.10). The increasing sophistication of computer technology has enabled “interlopers,” hackers, and data thieves to identify individuals by combining fragments of data (e.g., age, gender, ethnic background, zip codes, etc.). Given the ease with which data can be obtained for one reason and used for a second, unrelated purpose, controls should be established within organizations to prevent or seriously restrict the ability to combine and share data without the consent of the data owner.

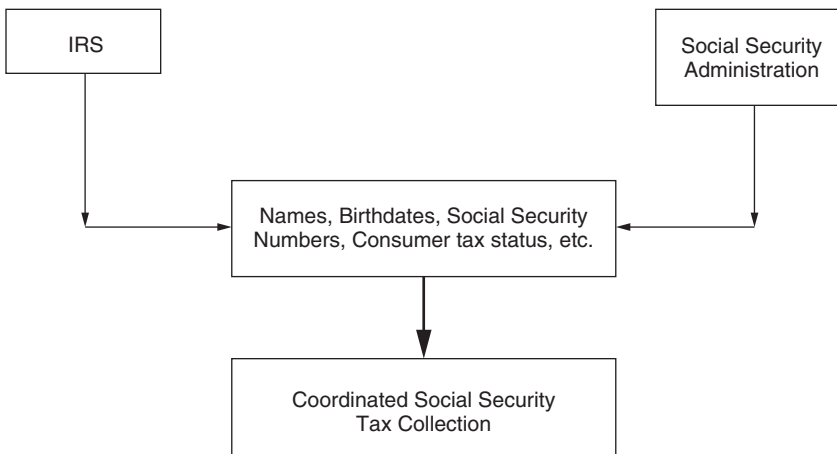


Exhibit 1.9. Linking Personal Data from Separate Government Agencies

Source: Newsbytes, Staff, “Linking of Federal Documents Raises Privacy Fears,” www.infowar.com/class_1/01/class1_040201e_j.shtml (April 20, 2001).

Organizations seeking to establish a better “customer image” in emerging virtual markets would benefit from establishing proactive data sharing and data disclosure policies. First examine existing practices. Does your organization share customer data with subsidiaries, third parties, mail houses, and so on? Do your clients/customers know you do this? If they found out, would they approve? Do system controls exist that prevent disclosure of private, confidential data to unauthorized third parties? Has your organization identified and secured private, personal, and confidential data residing on its computer systems? If you are unable to answer each of these questions in the positive, your organization may be faced with financial liability and exposure (and potential federal investigation) for the disclosure of such data, some of which may even be protected by existing (or newly enacted) federal legislation.

Taking a page from the GAO study mentioned earlier, organizations (as well as agencies) may wish to consider implementing one or more of the GAO’s recommendations:

- Obtain signed consent forms from clients, customers, and citizens prior to, and in order to, join their public data with more sensitive, confidential data.
- Obtain data from secure data centers, and known, reputable sites, where data can be used and analyzed under controlled conditions.
- To potentially “disguise” sensitive data, consider adding “random” distracting data in order to mask the identity of the data owners.
- Consider allowing an independent contractor to combine the data, stripping out all identifying data elements prior to turning the data over to or selling the data to a third party.

Large differences and serious concerns exist between consumers and business groups over the question of the sharing of consumer data between businesses, and this serious concern has kept many consumers from using the Internet as a means of commerce.

Jason Catlett, President of Junkbusters.com, said consumers should be given the opportunity to learn how information is being collected and shared about them, and that they should be able to choose whether they wish to allow the process to continue.¹⁸

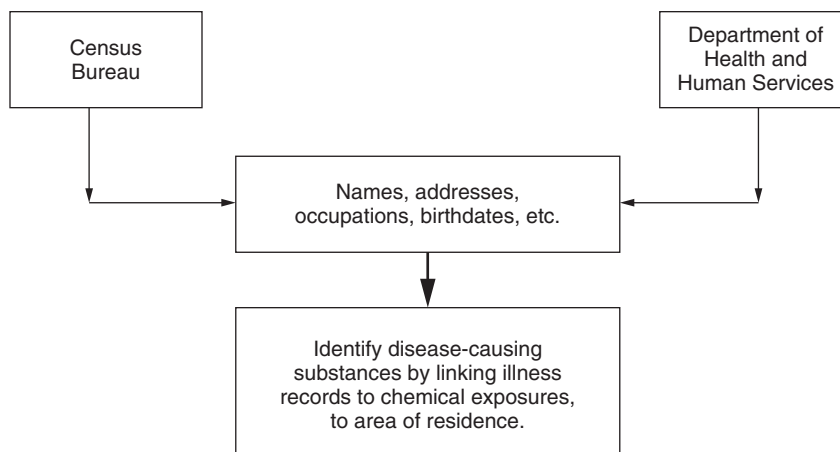


Exhibit 1.10. Example of Possible Benefit of Information Sharing Among Government Agencies

At a forum hosted by the Federal Trade Commission (FTC), Commissioner Orson Swindle said that a “trust gap” exists between businesses and consumers. Catlett countered that if a trust gap truly exists, the best way to bridge this gap is to create greater transparency in the right for (of) consumers to see what is going on with their data.

To further cloud and confuse the issue, government agencies are no better protected or poised to protect or prevent the disclosure of sensitive data. In a report released by Privacilla.org (www.privacilla.com), the company found 47 specific instances where federal agencies announced their intent to exchange personal data and combine this data into their own databases. As the U.S. Congress continues to introduce new legislation and debate existing bills designed to protect consumer privacy, the issue of consumer data-sharing promises to complicate organizational efforts to establish viable, working privacy policies and to effectively monitor those policies.

PRIVACY AND THE LONG ARM OF THE LAW

We can see that some laws seem to encourage invasion of privacy. Are there laws that protect the American people from this threat? The answer is a resounding maybe. There are laws on the books that address certain issues. However, these measures have been industry or product/service specific. The laws concerning privacy in the information technology environment have been reactive versus proactive. Legislators have targeted specific problems. However, this approach has done little to develop a national policy supported by law. “For example, in 1988 Congress was outraged to find that a Supreme Court nominee’s video rental records were legally released to a newspaper reporter.”¹⁹ Addressing this situation, they quickly passed the Video Privacy Protection Act. While this was well and good it was too specific, leaving large gaps in general privacy protection. What is extremely interesting about existing legislation is that it often exempts direct marketers’ collection and transfer of consumer information. The Video Privacy Protection Act is one example where this clause is present. It specifically states that “materials may be disclosed if the disclosure is for the exclusive use of marketing goods and services to the consumer.”²⁰

In 1994 a similar loophole was written into the Driver’s Privacy Protection Act. This Act limited the release of Department of Motor Vehicle (DMV) registration information but provided exceptions for journalists conducting research. One’s video records and our DMV records are now partially safe, but what about the records of one’s other purchases such as computer software, clothes, food, beverages, and so on?

The good news is that there is some method to the madness in establishing legislative protection. There are two primary goals or concepts associated with the legislative effort to protect consumer privacy. The challenge faced by legislators who are attempting to achieve these goals is protecting consumer privacy while avoiding hurting the marketing industry’s efficiency. The first concept is the mechanism of effective notice. This approach requires that the consumer be given an informed opt-in or opt-out choice. Essentially you are warned prior to providing any personal data and given the opportunity to exit the process. The second goal is to put limitations in place and control the use of consumers’ personal data. From a practical standpoint, these two concepts are generally blended together to help ensure privacy protection. Opt-in schemes guarantee that personal data will not be used for purposes other than what it was originally collected for without consent. The problem with this approach is that once the information has been col-

lected it is difficult, if not impossible, for consumers to change their mind, thus stopping the transfer of this data. The opt-out method allows consumers to remove their name from marketing lists. The problem with the opt-out list approach is that it is an all-or-nothing proposition. The consumer could be removed from all marketing lists, essentially taking the consumer out of the marketing loop completely. One alternative that may bridge the gap between the opt-in and opt-out schemes is a mandatory flagging scheme. This method allows the consumers' information to be flagged, thus indicating that they do not wish to participate in a specific product or service marketing campaign.

The tragedy of September 11, 2001 has sparked a renewed interest in Internet surveillance and laws to expand the government's powers. The Patriot Act has broadened the government's "investigative" powers. Many Americans feel that cyber-crime and cyber-terrorism are on the rise. Eighty-seven percent are worried about on-line credit card theft; 82 percent are apprehensive about terrorists using the Internet to inflict chaos; 80 percent are worried that the Internet can be used for widespread fraud; and 76 percent to 78 percent are concerned about hackers getting into business or government networks.²¹ However, despite this growing concern, not all Americans are ready to abandon their right to privacy. Sixty percent are extremely or very concerned about law enforcement obtaining increased access to their e-mail. Over 60 percent are extremely or very concerned about law enforcement gaining expanded authority to track their Web habits. Finally, 70 percent are extremely or very concerned about law enforcement acquiring more access to their financial records.

Thus the answer to an earlier question, "Are there laws that protect us from this threat?", is still a resounding maybe!²²

Organizations and government agencies are not alone under the privacy microscope. Legislation enacted by the U.S. Senate (Senate bill S290) requires academic institutions to obtain parental consent before collecting personal information from students for commercial use. The Student Privacy Protection Act requires academic institutions to give parents advanced notification of potential data collection within schools by corporations or other groups. The Act also stipulates that parents are to be advised as to how the collected data will be used, whom it will be shared with or given to, and how much class time any information gathering would take. Academic institutions would also be required to notify parents of any changes to their policies.

Enactment and passing of the Student Privacy Protection Act was prompted by a GAO report which disclosed that academic institutions across the country were engaging in a variety of activities with third-party marketers and companies, in exchange for subsidies for funding of new technology, school initiatives, and extracurricular activities. Adding further measures to protect the children and youth of our emerging virtual communities, federal legislation exists which requires child-oriented Web sites to tailor their parental consent practices to the nature of their information-gathering practices. Under the existing federal law, youth-oriented Web sites must obtain parental consent before collecting any personal data from children younger than 13. Verification of parental consent is allowed via e-mail between parent and Web site, if the information being collected is only to be used internally by the Web site.

By April of 2002, this sliding-scale model was set to terminate, requiring all children-oriented Web sites to obtain a more verifiable form of consent (i.e., digital parental signature, or a printed and mailed form from a parent approving the gathering of information), regardless of their information-gathering methods. However, the FTC pushed to keep the sliding-scale model in place through 2004, stating that digital signature technology hasn't advanced as rapidly as expected.

In a survey conducted by the nonprofit organization Pew Internet and American Life Project, the results disclosed that 68 percent of Internet users who were surveyed worried that malicious hackers might steal their credit card information. However, a substantial margin (86 percent) believed that on-line companies should ask permission of individuals first, before using their personal information.²³

Member companies of the high-tech community are pressing a different tack—wanting lawmakers to leave industry alone to solve its own problems, both through self-regulation and technology. One such means is through the adoption and incorporation of a technology referred to as “Platform for Privacy Preferences” (P3P). P3P relies on HTML-like code embedded in Web sites, which allow browsers to evaluate whether a site uses cookies or tracks usage once visitors have left a site. In theory, P3P would alert users when they visit a Web site if it does not meet their personal privacy standards.²⁴

Although privacy legislation will be addressed in much more detail in later chapters, it is worth noting here two pieces of legislation which tend to be recognizable bellwether legislative actions related to privacy. The first, Senate bill S.2606, introduced by Ernest Hollings (D—South Carolina) of the Senate Commerce Committee, would require Web sites to obtain consumers expressed consent before they are able to collect personal and identifiable data. Hollings’s proposed legislation also would create a private right of action against Web sites which violate their posted privacy policies. This would ultimately require companies to track consumer preferences on allowable data collection authorization, to verify a Web site’s compliance to the legislation and as a defense in the event of a lawsuit.²⁵ A second piece of legislation, this one introduced by John McCain (R—Arizona), the Senate Commerce Committee Chairman, would allow consumers to get out of the data collected or proposed to be collected by Web sites but would also force Web sites to clearly state how the personal data is collected and how this data will be used once collected.²⁶

In a study funded by the Association for Competitive Technology (ACT), a group founded by Microsoft Corporation, two specific objectives were set:²⁷

1. Determine a cost for making commercial Web sites compliant with the provision which allows individuals to access the information collected about them, and
2. Determine a cost to develop the tracking databases necessary to establish compliance if a firm was threatened by a lawsuit or government enforcement actions.

The results of this study may speak volumes and be a predictor of the eventual fate of privacy legislation coming from the federal sector. The study placed a price tag of approximately \$100,000 per Web site as the cost of compliance. If we were to extrapolate this figure, using the FTC’s estimate that some 3.6 million Web sites currently collect personally identifiable information, the study concluded that if only a minimum percentage of Web sites attempted to bring their practices into compliance of the proposed legislation, the eventual price tag could be in the billions of dollars.

Given the expense, which is expected to be shouldered by the Web site owners individually, the likelihood that such legislation will meet stiff lobbying efforts from Web companies is highly probable. Consumers may ultimately have to rely on a Web company’s moral compass pointing it in the right direction, and their own self-preservation “street-smarts,” when visiting and shopping at on-line Web sites, and not on federal legislation to protect their privacy.

PRIVACY AND SELF-REGULATION

As numerous pieces of legislation wind their way through the various branches of the U.S. government, lawmakers are debating whether to require companies to make available to consumers an opt-in or at least an opt-out choice prior to collecting, selling, or using consumers' personal data and records. Many organizations, including such industry heavyweights as the Direct Marketing Association, oppose the new laws, instead favoring industry self-regulation. This movement toward embracing a self-regulation position is gaining momentum as evidenced by the following examples:

- More e-commerce companies are requesting consumer permission for some or all e-mail promotions, including CDnow, Homestore.com, Women.com, OfficeMax, and Gateway.
- Some 84 percent of top Web sites post privacy policies and now at least give consumers the chance to opt out of having their information used or shared by others. Still, few have more stringent opt-in standards.²⁸
- More than 100 on-line companies have hired chief privacy officers (CPOs) to oversee customer privacy issues.²⁹

These examples are coming from organizations that realize that just because they build it, consumers will not necessarily come. Forrester Research recently unveiled survey findings that disclose that two-thirds of consumers responding to their survey worry about misuse of personal data given on-line. As a result of this worry, American consumers spent an estimated \$12 billion less on-line last year than they might have otherwise.

PRIVACY CONCERNS: CITIZENS AND THE INTERNET

According to a survey conducted by Forrester Research in March 2001, consumer fears about loss of personal privacy are mounting directly in response to increases in technological innovation and a lack of industry initiative in addressing this privacy issue.³⁰

As technology increases, the methods and means of poking and peeking into an individual's privacy continue to multiply. Consider that companies can (and do) employ

- Cookies
- Chat-room tracking
- Net mikes
- E-mail and workplace monitoring
- Webcams
- Keystroke monitoring
- Customer management software
- Smartcards with ID chips
- Biometric software that can track finger- or palmprints and perform signature, voice return, or facial recognition
- Fee-paid search engines with access to public record databases, and access to not-so-public databases

How secure and safe do you feel about your privacy now? Threats to personal privacy, once the basis for science fiction, have been forced onto the front pages of today's daily newspapers. Burying one's head in the sand and pretending that the problem, the risk, and exposure will go away, never did, and no longer will, solve the problem or reduce the risk/exposure. Individuals are on notice: a proactive response requiring immediate and decisive action is mandatory. Only by taking appropriate measures, implementing appropriate safeguards, and remaining alert to the changes taking place technologically, can citizens begin to protect their privacy. The personal privacy we all hold so dear and sacred, a right we have for so long taken for granted, a right which has all but disappeared, may never again be fully reclaimed.

A conflict, or maybe more appropriately, a dilemma arises when a society is forced to choose between increasing its quality of life and maintaining the privacy of that life. As technology has enabled individuals to enjoy an easier life than their ancestors, it has also opened their lives to examination and scrutiny by others. Information about your daily habits, likes, dislikes, movements about town, purchases, marriages, and donations have been available since written records of such data have been kept. Such data, even in written form, were dispersed in multiple locations, filed and retrieved manually, and typically required physically traveling to the location of the data/document to see it, or copy it (which early on required actually making a second, physical, duplicate copy of an original document—actually resulting in a second original). The necessity to physically request and travel to retrieve data added a layer of security to the process. The document holder could always request and verify the identity of the data requester and determine if the requester had either authorization or a legitimate right to have access to the data/documents. The document holder could easily deny the requester access to the data. The same information is available today, however, access to it can be accomplished while sitting in one's living room. Located, identified, retrieved, paid for, and shipped—all via electronic interaction between the record holder and the requester, with neither party ever meeting.

The ability of technology (and those who own the technology) to gather incredible amounts of information and misuse it is one of the fastest growing fears among individuals living in today's virtual societies. Protecting one's personal, private data has become a paramount concern of all global citizens.

Informed consent is the buzzword among regulators debating new privacy policies. How informed remains the center of dispute. U.S. data marketing policies offer legalese and fine print that leaves most consumers baffled. Consumers may be given the option of opting out of providing personal details, but few take up such offers.³¹

It would be a misstatement of fact if the reader is left with the impression that concern over one's privacy is a domestic, U.S.-based concern. In reality, fear over the loss of one's privacy is a global concern. Citizens of industrially and technologically advanced and emerging nations are awakening to the realization that there are no more assurances of personal privacy and only they themselves can take actions necessary to protect what little information remains private from the prying eyes of commercial third parties and government agencies.

In a March 2001 survey of Canadian Internet users, conducted by the Columbus Group/Ipsos Reid, 82 percent of the respondents stated that they have shared some personally identifiable information through a Web site. Eighteen percent felt that the information they submitted was used in ways they would consider to be a breach of their personal privacy. Of this 18 percent, 86 percent were automatically (and without their permission) subscribed to unwanted e-mail marketing and 43 percent stated that their data had been "sold or transferred" to an unauthorized third party.³²

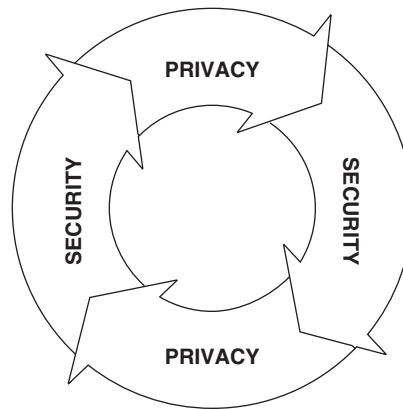


Exhibit 1.11. Twenty-First-Century Paradox

PRIVACY VERSUS SECURITY?

In a world now and forevermore defined as being “post-9/11,” can individuals truly believe we can live in a world where we can have both personal privacy and security? Will we ever again be able to say these two words in the same sentence without a chuckle, or a laugh of despair, without an internal knowing that the innocence has truly been lost?

As society moves forward, the challenge will be to develop policies, procedures, systems, and ideals which will provide for and establish both privacy and security, without limiting or weakening either. Only time will tell, however, whether the age-old question of the chicken and the egg may be replaced with a twenty-first-century paradox of privacy and security (see Exhibit 1.11). Do the concepts of privacy and security have to exist in conflict or will society find a way for both to coexist? Can we truly have both, in the deepest meaning of each?

Months after the worst terrorist attack on American soil, many are reassessing their views of the trade-off between privacy and security. And rightly so! Will all of the intrusive probing into our personal lives (surveillance cameras, metal detectors, scanners, searches, etc.), which we once found to be a violation of our “person,” now be readily accepted? How willing are we to give up some personal freedoms, privacy being one of them, for a sense of security? And that’s all it can be, a *sense* of security. For no individual, no government, and no technology can, with any degree of ethics or certainty, guarantee absolute security of anything to anyone.

Will individual rights be trampled upon in the frenzy to establish, in an almost “half-crazed” knee-jerk reaction, a secure “trusting” environment? Identifying such an environment, which has yet to be fully defined or identified, could be the most difficult task. Even then, such an environment may logically be impossible to secure, at levels most citizens would find acceptable—for the amount of privacy they would be willing to relinquish.

SUMMARY

Could our pursuit of maintaining our personal privacy be the downfall of our own personal security? Or will the (not necessarily our own personal) pursuit of security be done at the expense of an individual’s (or group of individuals’) privacy?

What roles will technology and government legislation play in this eventual and possibly ultimate power struggle? What will (or should be) the individual's role and responsibility in working toward and establishing an environment where both privacy and security can be achieved, and live in harmony? What is the role and responsibility of organizations for identifying, developing, implementing, and maintaining privacy rights for their clients and trading partners?

The following chapters in this text, and the sharply focused "pulse pieces" written by recognized leaders in the privacy field, take a long, hard look at these and many other issues regarding privacy. Issues our global society will face in the coming years as governments, corporations, and individuals come to grips with the new hot zone for the twenty-first century—privacy. In 1971 Arthur Raphael Miller wrote in *Assault on Privacy*:

As recently as a decade ago we could smugly treat [Aldous] Huxley's *Brave New World* and [George] Orwell's *1984* as exaggerated science fiction having no relevance to us or to life in this country. But widespread public disclosures during the past few years about the new breed of information practices have stripped away this comforting but self-delusive mantle. . . apprehension over the computer's threat to personal privacy seems particularly warranted when one begins to consider the possibility of using the new technology to further various private and governmental surveillance activities. One obvious use of the computer's storage and retrieval capacity along these lines is the development of a 'record prison' by the continuous accumulation of dossier-type material on people over a long period of time...constructing a sophisticated data center capable of generating a comprehensive womb-to-tomb dossier on every individual and transmitting it to a wide range of data users over a[n inter-]national network is one of the most disturbing threats of the cybernetic revolution.³³

ENDNOTES

1. Wright, E. S., "Privacy: the ugly truth" (August 7, 2001), www.infowar.com/class_1/01/class1_080901a_j.shtml, special to ZDNet.
2. Grillo, J. P. and E. A. Kallman, *Ethical Decision Making and Information Technology* (New York: Irwin McGraw-Hill, 1996).
3. Bonsall, William R., "Privacy, Does It Really Matter?" (Thesis, Webster University, 2001).
4. Thibodeau, P., "Profitable Privacy," *Computerworld* (February 18, 2002), 46.
5. The Sageza Group, Inc., Mountain View, CA, March 2002.
6. Id.
7. Smith, H. F., *Managing Privacy: Information Technology and Corporate America* (Chapel Hill: The University of North Carolina Press, 1994).
8. Equifax Inc. and Louis Harris and Associates, *The Equifax Report on Consumers in the Information Age*, Equifax-Harris Consumer Privacy Survey, 1992.
9. See note 3.
10. Miller, A. R., *The Assault on Privacy: Computers, Databanks, and Dossiers* (Ann Arbor: The University of Michigan Press, 1971).
11. See note 3.
12. Auchard, E., "Security trumps privacy, online and off," (November 12, 2001), www.infowar.com/class_1/01/class1_111201a_j.shtml.
13. Id.
14. Id.

15. See note 10.
16. 2001 AMA Survey, Workplace Monitoring and Surveillance (2001, April 18) <http://www.privacyexchange.org>.
17. Newsbytes, "Linking of federal documents raises privacy fears," (April 20, 2001) www.infowar.com/class_1/01/class1_042001e_j.shtml.
18. Krebs, B., "Privacy groups clash over consumer data trading," Newsbytes, (March 14, 2001) www.infowar.com/class_1/01/class1_031401a_j.shtml.
19. See note 7.
20. Video Privacy Protection Act, 18 U.S.C. § 2710 et seq., Section 2710 Wrongful disclosure of video tape rental or sale records. www.accessreports.com/statutes/VIDEO1.htm.
21. Harris Interactive on behalf of Privacy & American Business, "Privacy On and Off the Internet: What Consumers Want," Sponsored by Ernst & Young LLP and the American Institute of Certified Public Accountants (AICPA), (February 20, 2002) www.harrisinteractive.com/news/allnewsbydate.asp?NewsID=429.
22. See note 3.
23. See note 18.
24. Id.
25. Id.
26. Id.
27. Id.
28. Davidson, P., "Marketing gurus clash on Internet Privacy rules Opt in or Opt out? Experts differ on best way to sell," *USA TODAY* (April 27, 2001), B01, www.infowar.com/class_1/01/class1_042701a_j.shtml.
29. Id.
30. McGuire, D., "Firms Must Tackle Consumers' Privacy Anxieties-Forrester," Newsbytes (March 5, 2001) www.infowar.com/survey/01/survey03051a_j.shtml.
31. Auchard, E. "Consumer privacy, dark side of Internet age" (April 17, 2001a) www.infowar.com/class_1/01/class1_041701b_j.shtml.
32. "Privacy Policies Critical to Online Consumer Trust" (February 2001) www.ipsosreid.com/media/dsp_displaypr_cdn.cfm?id_to_view=1171 "Canadian Interactive Reid Report", Ipsos-Reid.com and Columbus Group, www.columbusgroup.com.
33. Miller, Arthur Raphael, *The Assault on Privacy: Computers, DataBanks, and Dossiers* (University of Michigan Press, 1971).