LIBRARY IN A BOOK

PRIVACY IN THE INFORMATION AGE

Revised Edition

Harry Henderson

Facts On File
An imprint of Infobase Publishing

PRIVACY IN THE INFORMATION AGE, Revised Edition

Facts On File, Inc.
An imprint of Infobase Publishing
132 West 31st Street
New York NY 10001

Library of Congress Cataloging-in-Publication Data

Henderson, Harry, 1951–
Privacy in the information age / Harry Henderson.—Rev. ed.
p. cm.—(Library in a book)
Includes bibliographical references and index.
ISBN: 0-8160-5697-8 (hardcover)
1. Privacy, Right of—United States. 2. Data protection—Law and legislation—United States. I. Title. II. Series.
KF1263.C65H46 2006
323.44′80973—dc22 2005037387

Facts On File books are available at special discounts when purchased in bulk quantities for businesses, associations, institutions, or sales promotions. Please call our Special Sales Department in New York at (212) 967-8800 or (800) 322-8755.

You can find Facts On File on the World Wide Web at http://www.factsonfile.com

Text design by Ron Monteleone

Printed in the United States of America

MP Hermitage 10 9 8 7 6 5 4 3 2 1

This book is printed on acid-free paper.

CONTENTS

PART III
APPENDICES

CHAPTER 1

INTRODUCTION TO PRIVACY IN THE INFORMATION AGE

Privacy, like most abstractions, can mean different things to different people. It can mean seclusion—a place where one need not fear prying eyes. But it can also mean the ability to control access to our personal information. Robert Ellis Smith, editor of *Privacy Journal*, combines the two definitions, speaking of "the desire by each of us for physical space where we can be free of interruption, intrusion, embarrassment, or accountability and the attempt to control the time and manner of disclosures of personal information about ourselves."[1]

In 1928 Supreme Court Justice Louis Brandeis saw privacy as woven into the very fabric of our national life:

> *The makers of our Constitution . . . sought to protect Americans in their beliefs, their thoughts, their emotions and their sensations. They conferred as against the Government, the right to be left alone—the most comprehensive of the rights of man and the right most valued by civilized men.*[2]

However, it must be noted that Justice Brandeis was expressing the minority opinion of a Supreme Court whose literalistic interpretation of the Fourth Amendment had found nothing unconstitutional about the police tapping a phone line without a warrant.

When the Court revisited the issue in *Katz v. United States*, almost 40 years had passed—years that had seen the anticommunist crusade of Senator Joseph McCarthy, the gathering of dossiers on thousands of Americans by FBI chief J. Edgar Hoover, and the establishment of an elaborate national security apparatus. In a world of hidden microphones and radio transmitters, the Court now declared that people have a reasonable expectation of privacy at home and with regard to certain activities. Most Americans agree with this principle, at least in broad terms. For example, we expect that a letter will get to its destination without being opened and read. Likewise, no one should be able to listen in secretly on our phone calls without a court order. And if the police suspect someone has committed a crime, they must go to a judge and obtain a warrant before searching her home.

Besides protecting specific places and activities, privacy can also mean protection for intimacy and family life, and indeed, the right to make decisions about whether to have a family, without interference from government.

Legal scholars make a distinction between the "decisional privacy" that was affirmed in the Supreme Court's *Griswold* and *Roe v. Wade* cases, and "informational privacy." The latter, as described by Columbia University law professor Alan Westin, is "the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about themselves is communicated to others."[3]

However, as Americans go online in search of shopping, entertainment, and social contact, that sense of control over information seems to be missing, and thus privacy seems to be not a firm guarantee but at best an uncertain promise. Thus, according to writer Jeffrey Rosen,

> *. . . as thinking and writing increasingly take place in cyberspace, the part of our life that can be monitored and searched has vastly expanded. E-mail, even after it is ostensibly deleted, becomes a permanent record that can be resurrected by employers or prosecutors at any point in the future. On the Internet, every Web site we visit, every store we browse in, every magazine we skim, and the amount of time we spend skimming it, creates electronic footprints that increasingly can be traced back to us, revealing detailed patterns about our tastes, preferences, and intimate thoughts.*[4]

During the past decade or so Internet users have gradually come to realize that the computer screen is not a sign or a mirror but rather, a window. As the user searches for information and makes selections, data about that person is flowing outward, where it is accumulated in databases. These "electronic footprints" make the consumer himself or herself into a product that can be bought and sold.

While informational rather than decisional privacy is the focus of this book, there is no absolute distinction between the two types of privacy. In a society where communications and information technology are central to economic and even social life, many privacy advocates feel that the right of persons to control how information about them is obtained and used is deeply intertwined with the experience of autonomy and liberty. Without control over their personal information, how can people feel confident about making important decisions? And in a world where cyberspace so often intersects physical space, how can one secure life's private spaces?

PRIVACY ISSUES

As important as the right of privacy is to so many people, it is clearly not the only consideration in making decisions about how society will be organized. What makes privacy issues so often contentious and hard to resolve is the in-

evitable conflict between privacy and other important goals, such as business efficiency, law enforcement, and, particularly in recent years, fighting terrorism. Because hardly anyone is against privacy in the abstract, privacy issues generally involve one side saying that privacy is being threatened and the other side saying that the threat is minimal and is justified by important social, commercial, or governmental interests.

Privacy issues are found in virtually every activity and institution of modern life. Today some of the most prominent ones include

- What should happen to the information consumers provide when they buy something in a store or online?
- Is it acceptable for web sites to track users if it enables them to provide a more "personalized" and relevant selection of goods?
- Should companies have to ask permission before they distribute customer information—or is it up to the customer to say no?
- If information can be collected only if the consumer allows it, will the availability of credit and other services decline, and costs go up?
- Who should have access to a person's medical information? Should insurers be allowed to turn down persons who have genetic risks of disease? What role, if any, should medical records play in employment decisions?
- Should employee use of e-mail, chat rooms, and web sites be monitored to avoid potential lawsuits?
- How can children be given access to the rich resources of the Internet without compromising their or their family's privacy?
- Should all e-mail and other Internet activity be digitally traceable? Would the ability to find and punish spammers, hackers, or online predators outweigh the loss of anonymity that might protect vulnerable people or whistleblowers?
- Would the use of a universal ID card, biometric passports, airline passenger screening, and integrated databases make the nation safer from terrorism? If so, would it be worth the cost in privacy and the ability to move freely without having to be accountable to a largely unseen and unknown security apparatus?
- Is it a good idea to have surveillance cameras in major public places? Does it deter crime but also deter people from associating freely? Should any restrictions be placed on the ubiquitous web cams and camera phones that allow anyone to capture images?
- Are we becoming a "surveillance society"? Should we admit that privacy is a lost cause, or give people the technical and legal tools to "watch the watchers"?

Before considering these and other conflicts over privacy, it is useful to look more closely at the idea of privacy and how it has emerged in the development of modern society.

THE IDEA OF PRIVACY

Throughout history most societies have been organized with an emphasis on communal living. In medieval Europe, many tribal societies throughout the world, and even in the America of the first colonists, people generally lived together as extended families under one roof (often in one room). The idea of a person having a private bedroom was virtually unknown. Under such circumstances, there was little that people did not learn about one another.

On the other hand, there was little need to keep track of details about individuals outside the immediate group. Written records were not generally kept, except perhaps for the church's records of birth, marriage, and death, and records pertaining to the few people who owned land. Rulers generally had little interest in the details of the lives of ordinary people.

EMERGENCE OF THE INDIVIDUAL

The Industrial Revolution, which began in the late 18th century, created a tidal wave of change in living conditions for people in Britain and Western Europe. It brought thousands of people to work together in factories and offices in huge, teeming cities. As increasing numbers of people began to change from a rural, subsistent, agricultural way of life to urban wage labor, extended families tended to break into smaller units. A young person who left a rural home in search of work in the city was likely to find a marriage partner there and raise a "nuclear" family that was likely to be out of touch with the extended family.

This more mobile but in some ways more isolated life created new social needs. The medieval world had imposed rigid social classes but offered some security in providing everyone with a well-defined status, a "place in life." The industrial world and the growth of the middle class broke down rigid barriers and offered new opportunities for upward mobility, but it also created insecurity and tensions as people from different backgrounds and with different customs were thrown together and had to find ways to live comfortably with one another. The need to enable individuals and families to establish boundaries of personal space found expression in the idea of a right to privacy. For example, the act of visiting another person's home became more ritualized, and wealthier people started to devote a special room in their house for such visits.

The emerging need for privacy also reflected cultural and even psychological changes. According to privacy expert Robert Ellis Smith, from the point of view of the individual, "The right to privacy includes a sense of autonomy, a right to develop a unique personality and living space, and a right to distinguish one's own persona from everyone else's."[5] But this is a sentence that would have made little sense more than a couple of hundred years ago.

Just as lines in a geometric polygon define an inside and an outside, the existence of a sense of self is what gives rise to the idea that some things are interior, personal, and private, while others are public, belonging to the world as a whole. To modern people, it seems quite obvious that we have an inside and an

outside—and that protecting and nurturing what's inside is of special concern. But when one looks at the literature and art our ancestors have left for us, it seems that the emergence of a modern sense of self was a gradual process. As literary scholar Alastair Fowler has noted:

> *. . . Medieval literature knew almost nothing of individual personality: its introspection proceeded along rigidly casuistic [formally logical] lines. During the Renaissance subjectivity began to stir, particularly in dramatic literature, where the feelings associated with decisions were displayed, and in sonnets, which did much to explore one range of private emotions. The 17th century epigram did more. And the inquiries of [Robert] Burton and [Thomas] Browne (in their very different ways) enlarged the possibility of self-consciousness. But it was only in the 18th century that literature made a sustained attempt to express the individual feelings of those with the leisure to discover themselves.*[6]

As art and literature began to depict the world in more realistic detail, the textures of individual personalities became a major focus of novels such as those of Jane Austen. Turning toward the 19th century, the romantic poets, such as William Wordsworth, Samuel Taylor Coleridge, and William Blake, looked at universal ideas through the bright, sharply focused light of the individual imagination.

While few people in the early 1800s had the leisure or talent to become poets or novelists, the new focus on the self in high culture reached middle-class readers, who could participate through the fashionable new practice of keeping a diary, a private space in which one could assess one's daily experience and express one's hopes and fears.

A Politics of Individuality

At the same time people were starting to define new social customs that protected privacy, the political philosophy of thinkers such as John Locke was starting to emphasize the rights and even the sovereignty of the individual in interaction with the government. In the medieval world, rights were attached to social status (most of the rights in the British Magna Carta of 1215, for example, referred to the nobility, not the common people). But 18th-century British statesman William Pitt declared in a speech before Parliament:

> *The poorest man may, in his cottage, bid defiance to all the forces of the Crown. It may be frail, its roof may shake; the wind may blow through it; the storm may enter; the rain may enter; but the King of England may not enter; all his force dares not cross the threshold of the ruined tenement.*[7]

Privacy, like freedom of speech and the press, emerged as rights that could be asserted against the government. Meanwhile the political reformers of the late 17th and 18th centuries replaced the idea of absolute monarchy with the growing

power of a Parliament that represented the people (although admittedly only males with a certain degree of economic status were truly represented).

The colonists who came to America from England shared the regard for privacy and individual rights of the English political reformers. For example, the Rhode Island Code of 1647 stated that "a man's house is to himself, his family and goods as a castle." On the eve of the American Revolution, colonist John Adams told a jury that "An Englishman's dwelling House is his Castle. The law has erected a Fortification around it."[8] Indeed, one cause of the friction that led to the American revolt was that officers of the Crown frequently broke into colonists' homes to seize papers, having only the authority of a vague "general warrant."

The U.S. Constitution that came into effect in 1789 was primarily a blueprint for the organization of government, with Congress, the executive branch, and the judiciary branch each being given specified powers. While such a structure may have implied that rights not given to the federal government remained with the states or the people themselves, a keen awareness of abuses that had been suffered under British rule had led to demands for explicit guarantees of individual rights. The result was the adoption of 10 amendments, called the Bill of Rights, in 1791.

Several of the amendments have something to say about privacy. In particular, the Fourth Amendment states:

> *The rights of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.*

This language gives specificity to the "your home is your castle" idea, declaring a fundamental right of privacy that officers of the state can overcome only by having sufficient reason ("probable cause") to believe that a crime has been committed, and that the place to be searched is likely to contain specified evidence relating to the crime.

Other amendments of the Bill of Rights also touch upon privacy. The Third Amendment prevents the government from taking over private homes to house soldiers during peacetime. Of more relevance today is the Fifth Amendment, which includes a provision that no person "shall be compelled in a criminal case to be a witness against himself." In other words, the information locked inside a person's brain is private and cannot be forced out and used against that person.

PRIVACY IN INDUSTRIALIZED SOCIETY

America at the time of the Constitution's framers was a primarily agrarian society. By the early 19th century, however, an industrial revolution was underway, reshaping daily life and the land itself, and creating new technologies that had

unpredictable social impacts. To many artists and literary romantics at the dawn of this revolution, industrialization and technology threatened to turn emerging selves into interchangeable parts of some vast and relentless machine.

In America, a land that celebrated both limitless growth and individual freedom, transcendentalist philosopher and author of *Walden* Henry David Thoreau retreated to the woods, and essayist and philosopher Ralph Waldo Emerson protested that "Society everywhere is in conspiracy against the manhood of every one of its members. . . . The virtue in most request [demand] is conformity. Self-reliance is its aversion. It loves not realities and creators, but names and customs."[9] This restated the romantic vision: the creative power of the individual versus the deadening power of conformity. In America, at least, the apparent boundlessness of the land could postpone for a time the regimentation that would characterize emerging European states such as Prussia in the latter part of the 19th century.

Just as industrialization was threatening individuality, so too was an emerging science challenging the idea of an autonomous self. A Newtonian explanation of the mechanics of the universe had already led to the suggestion that if the paths of planets could be predicted by exact mathematics, perhaps nature and human life itself were equally determined by a clockworklike interaction of forces. If accepted, such a picture of the universe threatened to make privacy irrelevant. (And thus, the romantic poet William Blake had portrayed Isaac Newton as a demonic figure of fearful power.)

At first the incredible complexity of biology seemed to resist mechanistic explanations. Biologist Louis Pasteur demonstrated that even microscopic life always comes from preceding life, rather than being generated from some mysterious "vital force." In the middle of the 19th century naturalist Charles Darwin introduced an elegant, powerful, and controversial explanation of evolution by natural selection. When Darwin examined the "human animal" and its position in the scheme of all things, he concluded that

> *The great difference in mind between men and higher animals . . . is certainly one of degree and not of kind. The senses and intuitions, the various emotions and faculties, such as love, memory, attention, curiosity, imitation, reason, etc., of which man boasts, may be found in an incipient, or sometimes in a well-developed condition, in the lower animals.*[10]

Two other great explainers of the 19th-century scientific revolution were Karl Marx and Sigmund Freud. Marx attempted to demonstrate that the conditions of human life and culture arise not from the individual will but from inexorable economic and historical forces. One might say that at least in the things that mattered, people did not make history; history made people. In this view, the inner self was peripheral, not primary.

Freud, on the one hand, actually made the private self more important. He made dream interpretation, free association, and the systematic examination of memories and feelings the key to freeing the individual from mental illness. On

the other hand, Freud, like Darwin and Marx, was a determinist. He said that human behavior was determined by forces of which the individual was usually unconscious—forces that acted according to laws not unlike the hydraulic behavior of fluids. While exploring the private self was given new importance, its privacy, its harmful secrecy, would be seen as a barrier to be pierced by the light of analysis. (Later, 20th-century behavioral psychologists would attempt to dispense with the inner world entirely, working directly on observable behavior through stimulus, response, and reinforcement.)

The Victorian individual thus lived in a world of rapidly growing complexity. Science and technology offered explanations and new capabilities—even new leisure for some people to explore their private selves. But science and technology also threatened to make the self obsolete or irrelevant—and perhaps to annihilate privacy. Thus in 1890, in a landmark law journal article on the right of privacy, Samuel D. Warren and Louis D. Brandeis noted:

> *The intensity and complexity of life, attendant upon advancing civilization, have rendered necessary some retreat from the world . . . so that solitude and privacy have become more essential to the individual; but modern enterprise and invention have, through invasions upon his privacy, subjected him to mental pain and distress. . .*[11]

THE ALL-SEEING EYE

Around the turn of the 19th century, a British social reformer and philosopher named Jeremy Bentham developed a theory of utilitarianism, which viewed life as a kind of balance sheet of pleasure and pain. For Bentham, the object of a scientific, rational society was to maximize the former and minimize the latter, crafting social policies that would create "the greatest happiness for the greatest number."

For the reformation of individuals who broke the laws designed to secure their happiness, Bentham designed a new kind of prison he called the "Panopticon." This circular prison would be carefully arranged so that its inmates could be watched everywhere and at every moment by guards, who themselves could not be seen. It was not that every prisoner would be continually observed. Rather, Bentham thought that a prisoner who *could* always be seen and thus, at any time, *might* be under observation would have no choice but to behave "rationally" and gradually be transformed into a productive, happy citizen.

No Panopticons as such were ever built, but just as 19th-century science began to put the self into troubling new perspectives, late 19th- and early 20th-century technology would change what it would mean to hear and be heard, see and be seen. The telephone, introduced in 1876, seemed magical at first but soon became indispensable. The ability to talk to people without meeting them made it possible to sustain a much larger web of business and social relationships at a much faster pace than the daily rounds of the mail carrier.

But besides being disembodied, phone conversations were not necessarily under the sole control of their participants. Besides the operators needing to connect early phone calls and the common use of party lines, according to technology writer Erik Davis, "The mere *possibility* that unknown and unseen agents are bugging your line is enough to puncture the psychological intimacy afforded by a phone call, transforming your humble handset into an insidious tentacle of unwanted and invisible powers."[12] As early as the late 1870s, telephone inventor Alexander Graham Bell's assistant, Thomas Watson, was confronted by a man who was convinced that enemies had connected his brain to a telephone circuit so they could implant fiendish suggestions. (Each new technology seems to offer an image to be seized by paranoids: Later some would wear tin foil hats to block mind-control radio waves; in recent times, some have claimed that they are under the control of implanted computer chips.)

Until the 1930s, though, most people who were not spies or gangsters—or paranoids—did not spend much time worrying about phone tapping. But the powerful new totalitarian systems of fascism and communism used the telephone to pierce privacy and coordinate oppression, and used the invention of radio broadcasting to try to mold opinion on a vast scale. World War II demonstrated weapons of unparalleled physical destructiveness, but it also suggested the effectiveness of the increasingly sophisticated technology of social control.

BIG BROTHER

British novelist George Orwell responded to communication and technological developments by publishing in 1948 his famous novel *1984*, which seemed to be the summation of all that people had learned to fear about the use of technology to destroy liberty and even individuality itself. In Orwell's world a still newer technology, television, would realize the vision of Bentham's Panopticon. No citizen would escape the eye of Big Brother. Even the very idea of having a self separate from Big Brother would become "thoughtcrime."

Indeed this ultimate dictatorship aimed not merely to punish crime but also to render it impossible. As *1984*'s protagonist Winston Smith is informed, the media of television and the press would be used to mold minds through a specially designed language, Newspeak:

> *Don't you see that the whole aim of Newspeak is to narrow the range of thought? In the end we shall make thoughtcrime literally impossible, because there will be no words in which to express it. Every concept that can ever be needed, will be expressed in exactly one word, with its meaning rigidly defined and all its subsidiary meanings rubbed out and forgotten. . . . The whole climate of thought will be different. In fact there will be not thought, as we understand it now. Orthodoxy means not thinking—not needing to think. Orthodoxy is unconsciousness.*[13]

In the world of Big Brother, privacy cannot exist because, without consciousness, there is no sense of self.

LITTLE BROTHERS?

More than half a century after 1948 (and two decades after 1984), Orwell's vision of totalitarianism may seem as primitive and simplistic as the huge dams and power plants beloved by the leaders of the defunct Soviet Union. The "telescreen" (an early name for television) indeed became ubiquitous, but in the 1950s it showed not Big Brother but *I Love Lucy* and the resplendent wonders of modern kitchen appliances.

Social critics of the 1950s and 1960s began to see the threat to the individual as coming not from the focused propaganda of a single Big Brother but from the pressures for conformity in the corporate workplace, in schools, and in the consumer culture with its relentless display of TV commercials. Now the self could be eroded by homogenizing the individual, masking the unique inner self with a bland construct of images and desires. If privacy depends on identity, loss of any unique identity might make privacy irrelevant.

Popular culture has continued to reflect this theme. In Hollywood, for example, the 1998 movie *Pleasantville* used the metaphor of color versus black-and-white to portray a rebellion against the conformist 1950s world. However, the ultimate expression of this theme can be seen in the *Matrix* film series, where what we perceive as reality is actually a virtual-reality construction operated to serve the needs of hidden conspirators.

"The Big Brother Society that was imagined in 1970," one critic notes, "depended on coercion and fear. The society we are developing appears to be more [Aldous] Huxley-like than Orwellian. It is a Brave New World dominated not so much by tyranny as by a deadening political and cultural phenomenon that Ralph Nader calls 'harmony ideology.'"[14] Linguist and radical critic Noam Chomsky refers to this phenomenon as "the manufacture of consent." In other words, people are given a superficial individuality (defined mainly by possessions and lifestyle) and an illusion of having an inner self.

As television continued to evolve, it created increasingly immersive substitutes for community, with sitcoms giving way to the oxymoronic "reality TV." (The movie *The Truman Show* takes the trend to its logical conclusion, where a person's life is unknowingly a reality-TV broadcast.)

At the same time, the news media invades and feeds on the revelation of the private life of public people, from football player and actor O. J. Simpson, Princess Diana, and President Bill Clinton's sex life in the 1990s to pop singer Michael Jackson and Terri Schiavo in the first years of the new century. Many lesser celebrities are fed into the maw of trials as entertainment.

Perhaps people who identify with beleaguered celebrities are vicariously experiencing their own concern about their privacy as they worry about personal information being stolen by criminals or diverted, sold, or abused by institutions such as insurance companies, stores, and government agencies. As the boundary between public and private has become fluid in the media and the culture as a whole, for many people the fear is that, according to Simson Garfinkel, "The future we're rushing toward isn't one in which our every

move is watched and recorded by some all-knowing Big Brother. It is instead a future of a hundred kid brothers who constantly watch and interrupt our daily lives."[15]

THE GROWTH OF INFORMATION TECHNOLOGY

Accompanying television as postwar high tech, the mainframe computer was also seen as an ominous threat to individuality. Science fiction writers began to visualize Big Brother in a new guise as the ultimate computer. (As an old joke went: When the huge room-filling machine was asked "Is there a God?," it blinked and whirred a while and then announced, "There is one *now.*")

The ancestor of modern information technology was the card-sorting machine invented by Hermann Hollerith and first used successfully in the 1890 U.S. census—just as Warren and Brandeis were sounding their warning about new technological threats to privacy. Card tabulators grew increasingly sophisticated through the 1920s and 1930s. World War II brought the first electronic digital computers, giving the capability not only to sort information but also process it into new information.

Computers of the 1950s and early 1960s had several characteristics that suggested an unsettling threat from these new "electronic brains." They were large and complicated-looking, their method of operation was unknown to most people, they were tended by a white-garbed "priesthood" of operators, and they were too expensive for anyone except big corporations and the government. The punch card soon became a symbol of an individual life reduced to a pattern of holes. Increasingly, decisions about everyday life seemed to be coming not from a human clerk one could talk with but from a machine animated by mysterious programming.

The three big TV networks and IBM thus became emblems of a power that dazzled and disturbed, promised and threatened, seeming to point at the same time to the ultimate in modern lifestyle and an emptying out of the inner self. TV seemed to replace the stuff of life with manufactured images. The computer might complete the abolition of privacy by turning the uniqueness of life into mere data. But the technology would prove to be both much more fertile and more ambiguous than the doomsayers could have imagined.

INSIDE THE WEB

Just as the early 19th century had spawned a cultural rebellion against industrialization, the new managed society of the 1950s and its information machines provoked a new flare of romanticism in the 1960s. The counterculture rejected both the computerized, managerial State and the blandishments of consumerism on TV. But the rebellion did not reject science and technology entirely: Indeed, much of it was fueled by electric guitars, a growing sophistication in electronic sound and visual effects, and hallucinogenic chemistry.

Privacy in the Information Age

At the same time that the 1960s cultural and political movements were getting underway and targeting government institutions and their technological trappings, one loosely knit group of explorers and activists were seeking not to destroy the computer but to reinvent it. Their name for themselves, "hackers," today has come to mean people who break into computers to destroy them or to steal valuable information. Originally, though, the hackers were brilliant though obsessive programmers who took advantage of a new generation of smaller, transistorized machines called minicomputers. They created the first video games, generated electronic music, and in general stretched the capabilities of the machines to the limit.

By the mid 1970s experimenters had shifted their attention to the microprocessor, or computer chip. They built primitive desktop computers and wrote about their revolutionary possibilities. One such visionary, Ted Nelson, proposed

> *a screen in your home from which you can see into the world's hypertext libraries . . . offer high-performance computer graphics and text services at a price anyone can afford . . . allow you to send and receive written messages . . . [and] make you a part of a new electronic literature and art, where you get all your questions answered.*[16]

Today we know this system as the World Wide Web. Even while the personal computer was being born, the 1970s also saw the creation of what would become the Internet. In the early 1990s Tim Berners-Lee invented the protocols for linking and transmitting text over the growing networks. By the middle of the decade, graphical browsing software such as Netscape made it possible for users of ubiquitous personal computers to participate in the Web.

While the economic possibilities of e-commerce took center stage at the end of the century, the social effects of the Internet have been at least as important. The primitive bulletin boards and commercial online services of the 1980s gave way to chat rooms and instant messaging. Millions of young (and not so young) people began to play in elaborate game worlds where a person's character or alter ego could build a house, carry on a profession, and even "marry" and raise a family. Meanwhile e-mail became ubiquitous at home and in the office. In the online world a person can take on many roles: a character in an elaborate game, a parent or a child, an employee, a customer, a patient, a citizen. In each of these roles information is exchanged with others, sometimes explicitly, sometimes implicitly, behind the screen as it were.

Cyberspace is a far cry from the Panopticon or the world of Big Brother's dictatorship. Big Brother projects his wishes into minds that have been so formed that they can hold nothing else. Television has been accused of being an instrument for imprinting conformity on millions of passive eyeballs. But in coining the word *cyberspace*, science fiction author William Gibson conveys a different vision. In the world of his novel *Neuromancer:* "The sky above the port was the color of television, tuned to a dead channel."[17]

Cyberspace is "inside" the TV set: There are no watchers, only characters. The choice of whether to be active or passive lies, as in "real life," with each individual. For Gibson and the other authors who created this postmodern science fiction, cyberspace is an exciting but not necessarily healthful place. In "cyberpunk" fiction, cyberspace is filled with violent conflict, techno gangsters, and the exploitation of the slow or unlucky by the fast and efficient. The world of cyberpunk, like the real information society it portrays, is a place where privacy and identity can be quite precarious.

INFORMATION PRIVACY AND THE DATA EXPLOSION

Back in the present-day world, the gathering, processing, and reuse of information continues to grow as the storage and processing capacity of computers and networks has steadily increased.

Our modern economy depends on massive exchanges of information, such as the details found in billions of checks and credit card charges. Most people would probably think that such details should not be accessible to the government without a court order. However, in *United States v. Miller* (1976) the Supreme Court ruled that checks and bank records were not private because they flow between banks as a part of commerce, and many people will have legitimate need to see them. The same has been held to be true of phone numbers, whose impulses must travel through many parts of the phone network. In other words, if something has to be seen by a number of people, it cannot really be private.

At minimum, one is faced with the question of how privacy principles should be applied to each new technology of communication, information processing, or surveillance. Constitutional scholar Lawrence Tribe has proposed a constitutional amendment that would read as follows:

> *This Constitution's protections for the freedoms of speech, press, petition, and assembly, and its protections against unreasonable search and seizures and the deprivation of life, liberty, or property without due process of law, shall be construed as fully applicable without regard to the technological method or medium through which information content is generated, stored, altered, transmitted, or controlled.*[18]

However, coping with the privacy implications of the "data explosion" is a formidable challenge. Just as developments in telecommunications and the processing of transactions have caused struggles over information privacy, so has the development of new ways of collecting, analyzing, and integrating data. The explosive growth of computer databases beginning in the late 1960s has particularly increased the threat to privacy by creating large amounts of information about the details of peoples' lives while providing little control over how this information might be used.

At first, much of the growth in databases came from government agencies that both needed and could afford huge mainframe computers for processing

records for tax, Social Security, and a growing number of welfare programs. Large banks and insurance companies soon followed suit. Computerization offered governments the ability to manage an increasingly complex system of regulations and entitlements, while private business sought cost savings by replacing labor-intensive manual record-keeping systems with automated ones.

Public concern about an electronic Big Brother grew during the 1970s. But while the popular image was of a giant government computer stockpiling every scrap of data about every person, the real threat was more complex and subtle. In 1977 the U.S. Privacy Protection Study Commission warned that "The real danger is the gradual erosion of individual liberties through the automation, integration, and interconnection of many small, separate record-keeping systems, each of which alone may seem innocuous, even benevolent, and wholly justifiable."[19]

In other words, the most likely threat was not Big Brother but a swarm of "little brothers" who spend 24 hours a day gossiping with one another. The development of the personal computer and the Internet would vastly increase the number of ways in which information could be collected and shared.

In 1972, when the personal computer did not exist and networking was still confined to a handful of researchers, the Advisory Committee on Automated Personal Data Systems to the Secretary of the Department of Health, Education, and Welfare proposed some basic principles for protecting privacy in the new Information Age:

1. There must be no personal data record-keeping systems whose very existence is secret.
2. There must be a way for an individual to find out what information about him/her is on record and how it is used.
3. There must be a way for an individual to correct or amend a record of identifiable information about him/her.
4. There must be a way for an individual to prevent information about him/her that was obtained for one purpose from being used or made available for other purposes without his/her consent.
5. Any organization creating, maintaining, using, or disseminating records of identifiable personal data must guarantee the reliability of the data for their intended use and must take precautions to prevent misuse of the data.

These are still the guiding principles for privacy advocates today, and they have been embodied in important legislation such as the Privacy Act of 1974, the Electronic Communications Privacy Act of 1986, and earlier in the Freedom of Information Act of 1966. However, the struggle to get government and business use of personal data truly to conform to these principles has been long and complex.

PRIVACY IN THE MARKETPLACE

Of all the transactions involving personal identification and information, the vast majority involve individuals in their role as consumer. After all, the average

person deals only occasionally with a health care provider or a government agency, but he or she makes dozens of purchases each week. Many small purchases are anonymous, such as putting a quarter into a rack and taking out a newspaper or buying a quick latté at a local Starbucks. But most purchases involving more than a few dollars are accomplished with a check or, much more often, a credit card.

Until after World War II, credit cards were issued by a particular business such as a department store or an oil company, and could be used only for purchases from that vendor. In 1949, however, Diners Club introduced the first general-purpose credit card, which could be conveniently used by travelers at a variety of restaurants, hotels, and other establishments. By the 1950s the Carte Blanche and American Express cards had been introduced, and the 1960s brought Bankamericard (later Visa), and Master Charge (later MasterCard). With the 1970s came the debit card in the form of the automatic teller machine (ATM) card and, later, debit cards for use in stores.

Cash purchases require no information except a simple receipt. Checks are more complex, but essentially the only requirement is a way to verify the identity of the check writer and, if necessary, the sufficiency of the bank balance. Use of credit cards, however, represents an open-ended series of loans. People who make loans want to make sure they will be repaid, and that means keeping track of information such as the following:

1. *Identifying information:* name and spouse's name, Social Security number, address, and telephone number
2. *Financial status:* amount of income (past and present), employer (present and past), occupation, sources of income
3. *Credit history:* previous type, extent, and sources of credit granted
4. *Existing lines of credit:* payment habits, outstanding obligations and debts, extent of current lines of credit
5. *Public record information:* lawsuits, judgments, tax liens, bankruptcies, arrests [in some cases], and convictions
6. *Prior requesters:* names of subscribers who requested information on the individual in the past[20]

Only an extensive computer network has the capacity to track these details and others for millions of borrowers in almost "real time," over a telephone or data network that enables merchants to accept the credit card and receive instant credit verification. This is only possible because the network taps into huge databases maintained by the major credit agencies: Experian (formerly TRW), Equifax, and Trans Union, which collectively maintain more than half a billion records on about 200 million people.

There are two significant vulnerabilities to the credit network, however. The first is that it depends on accurate identification—the person requesting the credit has to be the actual owner of the account. In recent years identity theft[21] has reached near epidemic proportions. The earliest route to illicit

credit card use was by stealing mail with Social Security or account numbers or a dishonest waiter or clerk copying down a card number for later use. However, starting in the later 1990s, a wide variety of techniques have been used to find personal information online or to trick users into revealing it to a fraudulent web site. Some thieves deal not in single accounts but obtain thousands by posing as legitimate users with a need for the information.

The same convenience that allows online purchases using only a card number (not the card itself) also affords cyber-thieves an easy way to take advantage of illicitly obtained credit information. The real prize for any data thief is the Social Security number. Besides retrieving credit records directly, the Social Security number can also be used to pull together all the records on a given person from a variety of public and private databases, many accessible via the Internet. (Ironically, Social Security cards, until the 1970s, carried a warning that read "For Social Security Purposes—Not for Identification.")

Identity theft for financial gain is not the only intrusion to which databases make people vulnerable. The personal information of politicians and celebrities is fair game for opponents or the tabloid media. When today's high-tech private investigators want to track someone down, they use a keyboard or a mouse, not shoe leather. Carole Lane, the author of a book about finding personal information online, boasts:

> *In a few hours, sitting at my computer, beginning with no more than your name and address, I can find out what you do for a living, the names and ages of your spouse and children, what kind of car you drive, the value of your house, and how much you pay in taxes on it. From what I learn about your job, your house, and the demographics of your neighborhood, I can make a good guess at your income. I can uncover that forgotten drug bust in college.*[22]

Even an ordinary person can fall victim to a stalker or abusive spouse who can use a Social Security number or other identifying information to get the target's address—or simply hire an illicit "data broker" or hacker to obtain the information. There are, of course, legitimate reasons for police and private investigators to use databases to track down individuals, such as to determine a person's assets in a divorce or in some other legal action, or to get someone to pay child support. The main problem is that there is little to stop the illegitimate user from accessing the same data resources. The sources of data and the ways to obtain it are many, and the existing regulations and safeguards, although slowly improving, remain far from comprehensive. Data in a networked computer is only as secure as the weakest link in the chain of users, a fact exploited every day by the creators of computer viruses, deceptive e-mail, and spyware.

As the world becomes increasingly wireless, new vulnerabilities have emerged. Cordless telephones are actually low-power radio transmitters, and calls on them can be picked up several hundred feet away. Cell phone calls can be picked up by scanners, although digital encryption now offers considerable

protection. The wireless (Wi-Fi) networks now popular in homes, businesses, and public places have only limited security, which is often left disabled.

The second vulnerability of the credit system is that like all databases, it is only as good as the accuracy of the information it contains. Surveys have shown that about a third of all credit records contain mistakes. Sometimes credit information for two people with similar names can become intermixed. Errors can have serious consequences, ranging from failure to obtain a home mortgage to being turned down by a prospective employer as a "deadbeat."

Recognizing the seriousness of this problem, federal law as of late 2005 requires that the three major credit reporting agencies provide one free credit report per year. Privacy and consumer advocates urge everyone to check their record at least this often, both to correct erroneous and potentially harmful information and to spot signs of possible identity theft. The credit-reporting agencies are also required to accept and verify corrections of erroneous information.

DATA BREACHES

In recent years there have been a number of cases where personal data stored in the computer systems of financial institutions or even universities has been obtained by hackers or by criminals operating under false pretenses. These "data breaches" have aroused considerable anxiety and anger on the part of the public.

For example, in February 2005 ChoicePoint, a company that holds an estimated 19 billion consumer records, revealed that a ring of identity thieves had bought 144,000 records by posing as legitimate marketers. Apparently, though, the only reason the breach became public was that one state, California, had recently passed a law requiring disclosure of such incidents.

The records in question included information gleaned from public records including marriages, property transactions, and arrest records—all organized by Social Security number. Even ChoicePoint itself declared that it was in favor of tighter regulations that would balance the commercial value of information against privacy rights. There are many other stories of lost or stolen data, ranging from the loss by Bank of America of a tape containing account information for 1.2 million Americans, the loss of more than 300,000 LexisNexis records to hackers, and even the theft of a laptop containing data about University of California, Berkeley, students. These stories have fueled public anxiety and led to demands for legislation requiring stricter security practices and prompt disclosure of data breaches.

If it is hard to deal with the consequences of domestic data breaches, some observers have pointed to the even greater risks when data is processed outside the jurisdiction of the United States. In recent years many activities such as billing and customer support have been outsourced to workers in countries such as India, where well-trained, English-speaking workers are available for much less cost. Although there is little evidence that personal information is at greater risk of illicit diversion abroad than it is at home, when a breach of privacy does

occur, U.S. federal or state regulations cannot be applied. Because of growing unease and a few well-publicized cases (such as one where a worker in India held some American records "hostage" in a wage dispute), Congress and more than 40 state legislatures have pending proposals to restrict the outsourcing of personal data. Some bills would allow consumers to opt out of having their data sent overseas.

Meanwhile, at home, the "outsourcing" of personal-data processing to a growing prison industry has also resulted in litigation. When a woman learned that a stalker who seemingly knew everything about her including her favorite magazines had received that information while working in prison for the data-profiling company Metromail, she successfully sued Metromail to stop the practice.

AN APPETITE FOR INFORMATION

Credit records are far from the only personal information generated in the modern economy. Anyone who belongs to a popular supermarket "savings club" creates a record of every item purchased, combining the information from the bar codes on the items scanned with the person's identifying information in the store's computer. The supermarket can use this information to create coupons instantly to entice someone who likes Kellogg's corn flakes to try the house brand instead. The information can also be used to target the customer for direct-mail campaigns. This same process can occur at a visit to a "big box" store, an auto dealer, or any time a consumer fills out a product registration or warranty card.

Why is so much information collected about everyone's daily purchases? Because, as one observer has noted, "Laws on privacy may vary from country to country, but the laws of economics do not. The laws of economics in the information age say that information has value—it is a product that can be sold, just like socks, cars, and toothpaste."[23]

Marketers suggest that by analyzing buying habits and making better fits between advertisers and consumers, both benefit:

> *Consumers benefit from receiving information that is targeted to their interests, as well as from not receiving information that is not of interest to them. Apartment dwellers don't want information about aluminum siding, for example, and childless couples don't need to learn about infant formula specials. Similarly, marketers have an interest in not sending messages to consumers who aren't interested.*[24]

In turn, according to correspondent and free-market advocate Declan McCullagh, the market as a whole will become more efficient and productive:

> *It's easy to complain about a subjective loss of privacy. It's more difficult to appreciate how information swapping accelerates economic activity. Like many other*

aspects of modern society, benefits are dispersed, amounting to a penny saved here or a dollar discounted there. But those sums add up quickly.

Markets function more efficiently when it costs little to identify and deliver the right product to the right consumer at the right time. Data collection and information sharing emerged not through chance but because they bring lower prices and more choices for consumers. The ability to identify customers who are not likely to pay their bills lets stores offer better deals to those people who will.[25]

Just about every shopper likes bargains. Designers of targeted advertising (starting with the first specialized mail-order catalogs) have argued that the more advertising can appeal to a person's particular interests, the more enjoyable and useful the ads will be. But with that, there is also a growing unease about loss of privacy.

Privacy concerns are most aroused because the information gathered from one type of transaction is often sold to other businesses or to agencies that package it and sell it to other direct-mail marketers. While the compiling and use of mailing lists is not new, modern database technology makes consumer information a much more valuable product because it can sort, select, and customize it in so many ways. For example, a mail-order catalog company can target just those women who might be interested in a new line of larger-size clothes. However, data from supermarket loyalty cards has also occasionally been sought in criminal or civil cases. An activist group called CASPIAN (Consumers Against Supermarket Privacy Invasion and Numbering) has sought to publicize potential abuses and argues that supermarket cards yield little in the way of real savings for consumers.

The reselling of personal information first came to public attention through a few high-profile cases in the late 1980s and early 1990s. The LexisNexis database company, for example, admitted that it paid credit bureaus for Social Security numbers and credit information on millions of Americans, which they packaged and sold to direct marketers. LexisNexis was sued in a consumer class action suit and was required to remove the Social Security numbers, as well as remove anyone from their database on request.

In 1991 software developer Lotus Development Corporation and Equifax, a major credit bureau, announced plans to market a CD-ROM database called Households that contained names, addresses, and marketing information on 120 million consumers. But after 30,000 people wrote or called demanding that their names be removed, the companies abandoned their plans.

The marketing of personal information, however, usually goes on below the surface. For example, New York State investigators discovered that the credit bureau TRW had been taking the records it received from American Express transactions and reselling the information to direct mailers. Such undisclosed reselling of information has become a major focus for regulatory action and legislation.

THE MALL IS WATCHING

Visualize this scene from a not very distant future:

> *Johnny Q. Consumer walks into a national chain store, picks up diapers, pays in cash. He does not walk alone. One store camera captures his face, while another network of cameras traces his stroll through the aisles. The pressure-sensitive floor panels note how he lingers and nervously shifts his feet while browsing in the diaper section.*
>
> *At the store's national headquarters, perhaps a thousand miles away, a machine quietly notes in Johnny's file that he may be a new father. That bit of data goes into an algorithm that a few days later cross-references birth records and finds that, indeed, Johnny has just become the proud father of twins. A card is sent out and special discounts will be offered the next time he enters the store.*[26]

All the pieces for this scenario are coming into focus: cameras, face-recognition software, and data-mining algorithms. So far, no store has implemented all these features, but it may be only a matter of time. In the movie *Minority Report*, there is an even more advanced (albeit fictional) version of this system: A shopper walks through a mall. He is instantly recognized by the computer system and advertising holograms appealing to his particular interests are projected into the air as he passes by.

Meanwhile, radio frequency identification (RFID) tags are beginning to be used to track merchandise in warehouses and during shipping—Wal-Mart began to use them in April 2004. The tags contain stored information (such as tracking numbers) that is transmitted when the package is scanned with an appropriate device. That device only needs to be brought within a few feet rather than requiring a close-up hand scanner as with bar codes.

Besides increasing shipping efficiency and reducing theft of goods by employees, RFID tags may also help stores monitor their displays and perhaps remove expired or recalled products. Privacy advocates fear that the ability to identify someone's possession could easily be abused. For example, private detectives or government agents might use RFID scanners to learn whether a person has bought a pornographic book, a radical Islamic text, or a bomb-making manual. Supporters of RFID suggest that reliable signals can only be received within a short distance of the object, reducing the ability of someone to scan surreptitiously.

RFID may be just the beginning of a future world in which all objects have embedded information and even "intelligence," communicating with one another over what Internet pundits have called "an Internet of things." For example, futurists point to packages of meat that can alert the refrigerator they have reached their expiration date—the refrigerator might then dispose of the item and order a replacement from an online store.

E-COMMERCE AND PRIVACY

In many ways the Internet is a shopper's dream come true. By surfing the Web, a consumer can obtain detailed information on just about any product or ser-

vice, even using a variety of services that automatically compare prices and identify the best deals. Items can be ordered with a credit card number and a few keystrokes. (There is little risk in dealing with a known company that uses a secure web server that encrypts credit card information, but information can be stolen by bogus sites or when sent by e-mail.)

As the 1990s ended, it seemed that e-commerce would supplant virtually all existing businesses, even the local grocery store. And although the "dot-com boom" was followed by a "dot-bust" in 2000–01, online stores and services that offer real value are here to stay—indeed a survey by market research firm Jupiter Research reported that total e-commerce sales during 2004 reached $66.5 billion, up 26 percent from the preceding year. Although this still represents only 4 percent of total retail sales, the impact of e-commerce is disproportionately greater because it involves some of the newest, fastest-growing business models. Further, it was estimated that another $355 billion in retail sales involved goods purchased in physical stores by customers who had previously researched their purchase online.

But the Internet and Web also adds another way to scoop up huge amounts of information from and about consumers. Many web sites store a small identification file called a "cookie" on a user's hard drive. They can then combine that information with the web server's log of all the web pages the user views. The result is a detailed profile of what the user has bought and is likely to be interested in. The use of cookies can save the user time (by making it unnecessary to resubmit credit card and address information for each order) and can also be used to customize the site with the user's preferences and to offer shopping suggestions. (Amazon.com, for example, has an elaborate system for offering recommendations based not only on what books one has bought before but also on what books have been bought by other people who bought those same books.)

Recently Google, the world's premier search engine, developed a free e-mail service called Gmail. The service is free because it is supported by advertising. To sell that advertising, Google ensures that it is targeted to the interests of each Gmail user. It does this by a process called "content extraction," in which the user's incoming and outgoing e-mail is scanned for keywords that might indicate an interest in particular types of products or services. The keywords are then used to generate targeted advertising.

Google has made it clear that no human actually reads the e-mail: The extraction is done completely automatically. However, privacy advocate Chris Jay Hoofnagel in testimony before Congress pointed out some troubling aspects of this technology. If the practice is routinely accepted, does it mean that e-mail users will no longer have an expectation of privacy under the Fourth Amendment? This could make it easier for police to use evidence from e-mail. Hoofnagel argues that "if companies can view private messages to pitch advertising, it is a matter of time before law enforcement will seek access to detect criminal conspiracies. All too often in Washington, one hears policy wonks asking, 'If credit card companies can analyze your data to sell you cereal, why can't the FBI mine your data for terrorism?'"[27]

REGULATION AND CERTIFICATION

The Federal Trade Commission (FTC) has been increasingly active in going after businesses with questionable information practices. The first well-publicized case came in 1998 when the FTC settled a complaint with GeoCities, a popular web-hosting service that offered free e-mail and web pages to individuals and families. As part of the settlement, GeoCities agreed to post a clear privacy settlement to explain its policies, and it also agreed to obtain parental consent before collecting information from children under 12 years of age.

Reacting to growing calls for explicit regulation, industry groups began to call for voluntary privacy standards. The best-known organization, TRUSTe, certifies web sites that provide clear privacy statements that explain what information is gathered and what will be done with it, as well as what a consumer can do if he or she is not satisfied.

Unfortunately, surveys have suggested that most Internet users do not understand privacy policies posted on web sites, nor use them effectively. In one survey,

- Fifty-seven percent of U.S. adults who use the Internet at home assumed that the existence of a privacy policy for a web site automatically meant that it would not share information with other companies.
- Forty-seven percent of users think privacy policies are "easy to understand," but about two-thirds of those users actually misunderstand the meaning of privacy policies.
- Sixty-four percent have not used the Web to get information about how they can better protect their privacy.
- Eighty-six percent would like to see regulations that standardize the format of privacy policies to make them easier to understand.[28]

Industry advocates have pointed out that the market has responded in some cases to privacy concerns of consumers by discontinuing unpopular practices. For example, America Online canceled plans to sell users' phone numbers to telemarketers, while Yahoo! removed a reverse-number look-up feature that could have been used by marketers. Perhaps the best-known case occurred when Internet advertising company DoubleClick ended its plans to combine information from web cookies with a large database called Abacus—which would have, in effect, data-mined Web users.

IS PRIVACY GOOD BUSINESS?

One approach to strengthening privacy is to use regulation (or the threat of regulation) to get companies to change their practices. But some experts suggest that protecting privacy can actually bring business advantages to companies that get out in front on the issue, such as by agreeing to use information only if they receive permission from the customer. According to Ann Cavoukian and Tyler J. Hamilton,

> *An opt-in marketing strategy does more than simply earn the trust of consumers. By allowing consumers to control the uses of their personal information, permission marketing increases the likelihood that the customer data being collected and used is accurate and up-to-date. Both consumers and businesses suffer when data is full of errors. When an individual's personal profile is inaccurate or incomplete, there is a greater likelihood of that person being judged out of context or treated unfairly. Meanwhile, there is a high cost to businesses when their customer databases are riddled with errors.*[29]

Libertarian free-market supporters have suggested that the ultimate solution is for companies and customers to negotiate individual privacy agreements. A free-market contractual approach would rely on accurate privacy statements to inform consumers who would then decide whether to do business with a given marketer. Some marketers might choose to offer a range of "privacy plans," with consumers who are willing to let their information be shared receiving lower prices or other benefits. However, according to legal expert Jerry Kang, the individual

> *would face substantial research costs to determine what information is being collected and how it is being used. That is because individuals today are largely clueless about how personal information is processed through cyberspace. [Companies] do not generally provide adequate, relevant notice about what information will be collected and how it will be used. What is worse, consumers' ignorance is sometimes fostered by deceptive practices.*[30]

Kang proposes that personal information be considered to be property belonging to the individual. This would mean that if a company wants the information, it must negotiate with the customer, rather than the customer having to stop unwanted use of information.

Other advocates see privacy as more like the inalienable rights proclaimed in the Declaration of Independence. According to Katrin Schatz Byford, "since the [property] model treats privacy as a quasi-material possession external to the individual, it cannot take account of privacy's function as an inalienable precondition of personal identity and social existence."[31] If privacy is an inalienable right (as life and liberty are inalienable), it means that no one can negotiate away their privacy.

In practice there is likely to be a mixture of approaches: regulations to prevent abuses that the majority find to be unacceptable, industry certification, the use of privacy assurances as a marketing tool, and consumers deciding for themselves whether the benefits of a company's policies outweigh the disadvantages.

PRIVACY AND THE HEALTH CARE SYSTEM

In recent years we have learned that privacy problems can be just one more thing wrong with America's troubled health care system. Consider these examples based on actual or potential cases:

A man goes into the hospital for treatment of prostate cancer. A month later he receives mail from a drug company touting their cancer treatment drug.

An employer searches employees' pharmacy records looking for expensive prescriptions that might indicate fraud or drug abuse. He finds that someone has a prescription for Retrovir, a drug used only to treat AIDS.

A woman's genetic testing reveals that she has a gene that indicates a high risk of her developing breast cancer. What happens if the test results are seen by her insurer? Her employer?

Employers provide most private health care and thus have a strong incentive to reduce what seem to be spiraling medical costs. One way is to try to have healthier employees in the first place. According to a 2004 survey by the American Medical Association, nearly 63 percent of U.S. companies require medical testing of current employees or new hires. This figure, however, is down from 70 percent in 2000, which may suggest that regulations and public pressure may be having an effect.

According to a recent survey reported by the Institute for Health Care Research and Policy's Health Privacy Project,

- One in every five people believes their health information has been used or disclosed inappropriately.
- One in six people tries to protect their privacy in some way, such as paying out of pocket for health care using multiple providers to try to avoid creating a single unified health record.
- Two out of three U.S. adults don't trust private health plans or government programs to maintain confidentiality all or most of the time.[32]

Clearly there is a high level of anxiety and distrust on the part of the public where privacy and the control of one's medical decisions is involved.

WHOSE MEDICAL RECORD?

Since ancient times doctors have professed a code of ethics that goes back to the Hippocratic Oath: "Whatsoever things I see or hear concerning the life of men, in my attendance on the sick or even apart therefrom, which ought not be noised abroad, I will keep silence thereon, counting such things to be as sacred secrets."[33]

The doctor-patient relationship is central to this ethic, which assures people that they can seek medical treatment without having the details of their medical condition revealed to other parties. Today, however, the doctor is only one of a large number of people and institutions involved in the delivery of health care. The tremendous growth in the cost of medical treatment has resulted in third parties—employer and insurance companies or the government—paying for

most health care. This in turn means that a bewildering variety of nonmedical personnel are also involved in viewing or reviewing medical records.

The flow of information is crucial to health care today. Doctors and pharmacies believe that access to comprehensive medical records is essential for providing better care and for protecting patients from taking dangerous combinations of prescription drugs. The managers of the government-run Medicare program need to track medical records to ensure quality of care and to prevent fraud. Insurance companies and health maintenance organizations (HMOs) claim they can use information systems to improve efficiency and hold down costs by eliminating wasteful and unnecessary treatments.

Further, uniform medical records and integrated databases offer a cornucopia to medical researchers. Recently the Mayo Clinic and IBM announced a pilot project combining the clinic's extensive patient database with IBM's data-mining technology to create the Mayo Clinical Life Sciences System. This would allow researchers to view at a glance every treatment and outcome for a patient in order to better understand how people with a given condition respond to a specific treatment. And when combined with the growing amount of genetic knowledge, Nina Schwenk, a doctor and chair of the clinic's information technology committee, notes:

> *When I see someone with high blood pressure, I have a choice of 20 to 30 drugs that I can choose from. There is some literature out there that will say, "If you're diabetic, this drug is better than that one." But most of the time, the only way you can tell for sure is to start the patient on the drug. It's almost trial and error to see how well it works for an individual and whether there are side effects. Not so far in the distant future we'll know the various types of genetic difference that cause people to metabolize drugs in different ways. So I know that if you try drug X, it's not going to work on you, and drug Y will have a heightened effect, while drug Z will have side effects. We'll be able to know all that up front.*[34]

As a result of both payment systems and the needs of medical research and quality control, so many people have joined the chain along which medical records pass that one writer suggested revising the Hippocratic Oath to read as follows:

> *Whatever I see or hear in my attendance on the sick or even apart therefrom will be divulged to physicians, nurses, aides, surgeons, anesthesiologists, dieticians, physical therapists, admitting clerks, billing clerks, utilization review personnel, discharge planners, records coders, medical records filing staff, chaplains, volunteers, performance evaluators, insurers, medical transcriptionists, accrediting agencies, public health officials, other government officials, social workers, and employers. AND to whomever else requests them for whatever reason.*[35]

The principal clearinghouse for medical records is the little known Medical Information Bureau (MIB), which has a role similar to a credit-reporting agency. The government also runs its own huge database for Medicare patients.

The Clinton administration proposed a single national databank in which every person would have a "universal healthcare identification number." But the existence of a single central database accessible by a single key number would put all a person's privacy eggs in a single potentially vulnerable basket. Although privacy concerns led to the proposal being withdrawn, there is continuing pressure to tie together all medical records and make them electronically accessible.

FROM HIPPOCRATES TO HIPAA

Passed in 1996 but not implemented until 2003, the Health Insurance Portability and Accountability Act (HIPAA) primarily seeks to make it easier for workers to retain their insurance when changing jobs. However, the law also includes some significant privacy protections. Most people learned about the law when they went to their doctor's office for a routine visit and were asked to sign forms allowing their medical records to be disclosed for certain purposes. The law also gives patients the right to see their medical records and to submit corrections.

Free-market critics argue, however, that HIPAA and other regulations mainly miss the point. They believe that

> *true health privacy relies on empowered patients choosing among options made available to them by providers competing to serve them. This happens in hearty markets, where sellers vie with one another to discover and deliver whatever consumers want. But the American health care system is not well. Concerns about health privacy are a symptom of a much larger disease.*[36]

Given the complex, highly regulated nature of modern health care, however, it is not clear how a true free market could develop in which most people have meaningful choice between competing providers. Most employers offer only a limited number of options, and choices for the self-employed are even fewer.

Adoption of a single-payer, government-run health care system like that found in many other industrialized democracies might remove some privacy issues by eliminating the role of private providers and insurers. However, the government itself would then be both provider and guarantor of privacy.

GENETIC PRIVACY: THE NEW FRONTIER

For many people the deciphering of the human genome announced at the beginning of the 21st century marked a tremendous achievement—the biological equivalent of NASA's Apollo project. However, the growing ability to identify hereditary health problems and risks has lent a new urgency to the struggle for health privacy.

Nancy Wexler, a leading genetic researcher studying the inherited degenerative condition called Huntington's disease, has warned that "All of us have something or other in our genes that's going to get us in trouble. . . . We'll all

be uninsurable."[37] What adds to the poignancy of her observation is that Wexler's own mother had Huntington's.

What does genetic testing mean for workers? If everyone has a susceptibility to some disease or another, one expert asks,

> *Do we want employers to be able to rely on dicey predictions about future health, to search for only perfectly healthy employees, and as a by-product keep Americans from their rightful place in the workforce? Such is the specter of genetic testing in the workplace—invasions of privacy, discrimination, and unwarranted control of individual conduct.*[38]

There are two potential sources of legal protection from genetic discrimination. The Americans with Disability Act (ADA) may apply to otherwise healthy people who have a genetic background that leads employers to view them as disabled, but the case law is mixed and the Supreme Court has yet to make a direct ruling. (In February 2001 the Burlington Northern Santa Fe Railroad agreed to settle a case where they had secretly tested workers for a genetic predisposition to carpal tunnel syndrome, a repetitive stress injury to the hand and wrist.)

The other possible legal protection comes from HIPAA, which forbids employer group insurance plans from denying insurance based on preexisting genetic conditions. However, employees or employers who are self-insured are not covered, and companies are not prevented from charging higher rates on the basis of genetic information.

Fundamentally, genetic information (together with more sophisticated medical testing) threatens to unravel the system of private medical insurance. Insurers traditionally put people in broad categories such as by age and a few other factors such as smoking. Rates were based on the overall average risk of medical problems for the group. However, to the extent an insurance company can learn about individuals, it has an incentive to "skim the cream" of healthy patients by offering them lower rates. People at higher risk would be turned down, accepted at much higher rates, or accepted only with the exclusion of preexisting conditions or risks. Although regulations can help protect against misuse of genetic information, it may be that only a fundamental restructuring of the health care system could truly solve the problem. (And, it must also be noted, if the government ran the health care system, the government itself might have an incentive to discover and misuse genetic information.)

PRIVACY AT WORK

After health and family, work is probably the next highest priority for most people. In the work force, though, many of the same driving forces—such as cost reduction and efficiency—are driving employers to monitor employees in ways that raise serious privacy concerns.

Questionable practices often begin before a person even enters the workplace. Most people would consider it reasonable that claims of education,

employment history, and references on résumés are subject to verification. Potential criminal records are also a concern—employers want stable, reliable employees and try to weed out potential "problem hires" who might expose them to legal liability. (For example, a store would not want to hire security guards who have a record of violent incidents.)

However, other types of inquiry can raise privacy concerns. Should a potential employee be screened out because civil court records show she has sued a previous employer for sex discrimination or harassment? (As noted earlier, screening for actual or potential health conditions is also a concern.)

Psychological tests or "personality inventories" are often given in an attempt to judge the suitability of an employee to a given position, or to detect proclivities for dishonesty or violence. But some tests can ask questions about religious beliefs and sexual practices that have no connection with job duties. (Some of these tests were attempts to replace the use of polygraphs, or lie detectors, which have been banned for most kinds of employment.) Psychological tests have generally been upheld in the courts, although antidiscrimination laws do regulate collection and use of information relating to protected status such as race, gender, disability, and in some jurisdictions sexual orientation.

MONITORING E-MAIL AND THE WEB

Once on the job, workers who talk to the public on the phone (such as airline reservation agents or technical support specialists) often have their calls monitored for "quality control" purposes. Sometimes, however, personal phone calls are also listened to by supervisors. Video surveillance of employees such as store clerks is also common.

Most workers today use desktop computers connected to an internal network (LAN) and to the Internet. Some workplaces install software that can keep track of how fast clerical workers type and how long they let the machine sit idle. In many offices software also makes a record of what locations users visit on the Internet.

Many employers see monitoring as a way to reduce theft, embezzlement, or sabotage by employees. Indeed, most misappropriation of computer data comes not from outside hackers but from disgruntled or greedy employees. (Ironically, laws intended to protect customer privacy and the response to recent data breaches may add impetus to the use of computer-monitoring systems.) In other cases employers may simply want to reduce the amount of work time lost to online shopping, chat, and playing of online games.

Most such monitoring is legal, but it may have a negative effect on the morale of workers who feel they are "living in a fishbowl." Unions have sometimes made workplace privacy an issue in contract negotiations.

E-mail raises particularly thorny issues. The ubiquitous use of e-mail has replaced the telephone for many purposes. Back in the early 1990s, when Epson employee Alana Shoars discovered printouts of her e-mail on her supervisor's desk, she sued Epson America for breach of her and her fellow workers' privacy.

She argued that she had an "expectation of privacy," the key test used by courts. She said that since workers had to use private passwords to access the e-mail system, it was reasonable for them to think that their messages would be kept private. Epson, on the other hand, argued that its e-mail system was just another business tool like a phone or a copier. Since it was provided only for business purposes, workers had no reason to assume they could use it for private personal messages. In July 1992 the court agreed with Epson's position and threw out the lawsuit. This decision was in keeping with the general trend in workplace privacy issues: Generally, workers do not have an expectation of privacy in the office, and employers can monitor activities (including e-mail) as long as the monitoring has a reasonable, business-related purpose.

Many employers point to the legal system itself as the reason they need to monitor employees' e-mail and Web usage. Employees have been held liable for sexual harassment or "creating a hostile workplace environment," such as when some employees print out or display pornographic material from the Internet. Additionally, a harassing e-mail sent by one employee to another might turn into a million-dollar liability problem for the employer. (Many companies may also be concerned about revelation of proprietary or "inside" information in e-mail.)

Roger Matus, CEO of Audiotrieve, a company that makes e-mail-filtering software, reports that his company had studied e-mail retrieved during the Federal Energy Regulatory Commission's investigation of Enron Corp. The study found that "one out of every 25 messages contained offensive or inappropriate content. Nearly one in five was personal in nature. I read many of these messages and a few of them were quite amazing." Matus further observed that "Already, 30.7 percent of companies with more than 1,000 employees employ staff to read and monitor employee e-mail. This is a fascinating area because employees seem to have no idea that e-mail does not provide any privacy."[39]

One possible defense to such suits is to show that the employer has been duly diligent in discovering potential abuses and correcting them. But the same practices that may prevent harassment claims may also become the subject of a lawsuit for invasion of privacy. Employers can make the best of a difficult decision by making sure their monitoring activities are related to legitimate business needs, are fully disclosed to employees, and assuring employees that any information gathered will not be disclosed to other parties.

In turn, employees should make sure they understand their employer's policies, ideally refrain from using the employer's equipment for personal messages, and, in general, avoid including any information in e-mail that might cause trouble if disclosed—keeping in mind that "deleted" e-mail is not truly gone and can be recovered by system administrators or computer forensic specialists.

PRIVACY AND YOUNG PEOPLE

As most parents know, children seem quite comfortable with high tech and the information society—more so perhaps than most adults. Junior high and older kids keep in touch with each other with rapid-fire instant messages, download and

share music files for their iPods and MP3 players, and confidently search the Web for information for school assignments when they are not online chatting or playing games. However, like many adults most children give little thought to privacy or worry about what might be done with the information they disclose online.

MARKETING TO CHILDREN

Although one wouldn't think children would be a major target of online marketers, older children often have access to the family's credit card numbers—or could persuade their parents to buy things for them online. Further, web sites that collect information from children can sell it to other marketers. In 1999 the web-hosting service GeoCities was stopped from collecting information from children without parental consent. Although there was no law against the practice at the time, the FTC was able to rule that the company was engaging in "deceptive acts or practices" in violation of federal law.

In 1998 Congress enacted the Children's Online Privacy Protection Act (COPPA). Since the enabling regulations were enacted in April 2000, web sites that wish to contact children have had to post a privacy policy that explains how information will be collected and used, and obtain explicit information from parents before accepting any information from their children. A year later the FTC found that most web sites were posting the required privacy policy, but only about half were properly notifying parents of their right to review, delete, or refuse the further collection or use of their children's personal information. In February 2003 the FTC imposed civil penalties on Mrs. Fields Cookies and Hershey Foods for failing to obtain parental consent before collecting information from children.

LIMITED PRIVACY AT SCHOOL

For at least the first 18 years of their lives, children spend a good many of their days in school, and whether it be middle school or college, educational institutions have their share of privacy issues. These include

- drug testing
- monitoring or filtering Internet use in schools
- administration of possibly intrusive psychological tests or surveys

Drug testing and Internet monitoring or filtering have generally been upheld by the courts, which have ruled that children have only limited Fourth and First Amendment rights compared to adults. However, intrusion into family information by school personnel has been limited by the Family Education Rights and Privacy Act of 1974 (FERPA), which limits schools' disclosure of student records outside the educational context (with exceptions such as for subpoenas from law enforcement agencies). Parents also gained the right to see and correct their children's school records.

Since the Columbine High School shootings in 1999, there have been a number of cases where diaries, e-mail, and web sites created by students have been identified as containing alleged violent threats. In the aftermath of each tragedy, it is always asked why school officials had seen no signs of the impending attack. On the other hand, much of the threatening material would probably be protected under First Amendment free-expression rights if it had been created by adults, and overreaction is always a danger.

The most intimate and delicate privacy issue comes between parents and their children, and here laws and public policy can be of little help. Children indeed face some serious dangers online, including harassment and even sexual exploitation. Some parents have installed software to monitor their children's Web surfing and e-mail. Children who discover the monitoring are likely to react to it as a betrayal, a lack of trust, and a denial of privacy just at the time when they are discovering what it means to have a private self. Whatever parents decide, it is best done openly after discussion with the children, with an explanation and agreement on the "ground rules." As one child psychologist and media expert suggests:

> *Somewhere between the two extremes is the prudent parent. For example, a parent shouldn't go off the deep end if their 15-year-old son visits a porn site. But if he starts spending hours at porn sites and chat rooms, they need to know about it.*[40]

As young people transition to adulthood, they will find that universities are an Internet-rich environment. Student records, like other personal records, are vulnerable to hacker attacks and criminal diversion. An additional issue arises from the subpoenas requested by the Recording Industry Association of America (RIAA) in an attempt to identify students who have illegally shared copyrighted music files. Some schools such as the Massachusetts Institute of Technology (MIT) have declined to hand over the requested information, citing FERPA.

PRIVACY, LAW ENFORCEMENT, AND NATIONAL SECURITY

Some of the most crucial privacy issues arise in connection with the government itself—particularly with regard to law enforcement, where liberty and even life are often at stake. The government is in a paradoxical position with regard to privacy. On the one hand, legislatures and courts have provided a growing number of privacy guarantees in some areas. On the other hand, the government itself is the largest gatherer and user of information about individuals, and its own practices have long been a concern of privacy advocates. As the Privacy Protection Study Commission reported back in 1977:

> *Accumulations of information about individuals tend to enhance authority by making it easier for authority to reach individuals directly. The voracious appetite*

of investigators for information causes [authorities] to collect and retain virtually any personal data uncovered unless the collection or retention is clearly illegal. This attention to avoiding what is improper, rather than accomplishing only what is necessary and proper, leads investigative agencies into abuses of citizens' rights.[41]

As with commercial information gatherers, the threat to privacy does not come only from isolated abuses but from the pervasiveness of the system as a whole and the lack of built-in safeguards. Many bureaucrats themselves see the systems as being unmanageable. The problem of keeping up with the information needs of government agencies has a tempting solution in the creation of a giant, centralized database for all information about an individual that could be constantly updated and placed at the disposal of each government agency for its own particular needs. In 1965, still back in the mainframe era, a limited version of this idea, the federal Data Service Center (also called National Data Bank), was proposed as a means to correlate all government data to allow for statistical research.

GOVERNMENT DATABASES AND INVESTIGATIONS

Such proposals have always been met by strong opposition. During the 1960s and 1970s, the FBI conducted secret but extensive counterintelligence programs (or COINTELPRO) that spied on Martin Luther King, Jr., and other civil rights and antiwar leaders. The Watergate scandal revealed that the Nixon White House was routinely using government agencies ranging from the CIA to the IRS to spy on or coerce political opponents. Such events made many people suspicious of any further centralization of government record keeping.

In 1972 Supreme Court Justice Lewis Powell noted in a ruling:

Security surveillances are especially sensitive because of the inherent vagueness of the domestic security concept, the necessarily broad and continuing nature of intelligence gathering, and the temptation to utilize such surveillances to oversee political dissent. We recognize, as we have before, the constitutional basis of the President's domestic security role, but we think it must be exercised in a matter compatible with the Fourth Amendment.[42]

The tendency to "federalize" crimes and social problems nevertheless continued to lead to expansion of government information systems and thus of threats to privacy. Examples have included the cross-matching of state and federal records to find persons who have failed to pay child support, verification and investigation of firearms purchasers, and investigations of Medicare or welfare fraud. In each case proponents have argued either that there was no true privacy problem or that the goals of the legislation justified a minimal invasion of privacy. Privacy advocates, however, remained concerned that the accumulation of seemingly minor intrusions on privacy would reach a point where the in-

dividual would lose confidence in both privacy and the ability to hold the government accountable.

THE PRIVACY ACT OF 1974

The privacy concerns of the Watergate era culminated in the passage of the Privacy Act of 1974. The act embodied fundamental principles that were intended to make government agencies disclose their information-gathering and distribution activities and to give citizens the ability to learn what information had been collected about them and to correct any errors. But over the past three decades privacy advocates have pointed to what they consider poor implementation and enforcement of this law. Since the act did not appropriate any funds for privacy enforcement, most major government agencies did not at first appoint anyone to oversee implementation. Without an enforcement mechanism, agencies were essentially the judges of their own compliance. As ACLU legislative director John Shattuck remarked during congressional hearings in 1983, "the rule disclosure of personal information without the subject's consent has been all but swallowed up by its exceptions, particularly the broad exception for 'routine uses.'"[43]

Nevertheless, the Privacy Act did provide citizens who suspect the government has inaccurate or inappropriate information about them with a useful if cumbersome tool. The citizen can try to determine which agency may have the information and file a request for it. Information involving law enforcement or intelligence activities, however, may be blocked from disclosure.

THE FREEDOM OF INFORMATION ACT OF 1966

One effective defense against government invasion of privacy is the ability to find out what the government is doing with the information it collects. The Freedom of Information Act (FOIA) of 1966 has allowed intrepid reporters, activists, and ordinary citizens to uncover important information about controversial government activities such as medical experiments and the handling of radioactive waste. The FOIA does allow the government to refuse to release information related to national security, intelligence activities, criminal cases, and other areas. As a result documents obtained by FOIA requests sometimes arrive with many areas blacked out. Critics of the FOIA point to frequent delays in obtaining information and the difficulty of appealing when requests are refused.

PRIVACY AFTER SEPTEMBER 11, 2001

The devastating terrorist attacks of September 11, 2001, brought shock, fear, and a resolve to uncover what appeared to be an extensive and deadly international terrorist network. In this atmosphere, at least at first, the warning cries of civil libertarians and privacy advocates seemed to be drowned out. As former FTC commissioner Robert Pitofsky noted, the dominant feeling was that "September 11

changed things. Terrorists swim in a society in which their privacy is protected. If some invasions of privacy are necessary to bring them out into the open, most people are going to say, O.K., go ahead."[44]

The USA PATRIOT Act was passed by Congress only six weeks after September 11, with little deliberation. A number of its provisions potentially weakened privacy protections. Section 215 allowed for the searching of books, records, or documents if government agents believed they might be related to an intelligence investigation. The agents did not have to provide specific grounds for their suspicions as with a normal criminal subpoena. Given that the Federal Intelligence Surveillance Act (FISA) already established secret courts for granting such subpoenas, the combination of secrecy and lack of strict standards has greatly alarmed civil libertarians, privacy advocates, and the library community.

Another USA PATRIOT provision, Section 213, allows for so-called sneak and peak warrants where the police can conduct a search without notifying the suspects and giving them a chance to contest the subpoena in court. The only requirement is that the judge agrees that there is reasonable cause to believe the secret search is necessary to protect the safety of police or bystanders or "the integrity of the investigation."

Generally, advocates of these provisions have argued that they are necessary because of the particular nature of terrorism investigations where suspects operate in secret and have potentially deadly capabilities. However, civil libertarians have pointed out that these USA PATRIOT provisions are already being used in some cases for crimes such as money laundering that are not believed to be linked to terrorism. At the same time, government officials have been hard-pressed to name even a few terrorism suspects who were apprehended using the more controversial provisions of the new law.

During 2005 a number of key provisions of USA PATRIOT are coming up for renewal. The administration has tried to minimize fear about abuses. Attorney General Alberto Gonzales has declared: "The department has no intention of rummaging through the library records or medical records of Americans. We do have an interest in records that help us catch terrorists."[45]

Going on the offensive, Gonzales notes:

> *Libraries currently are not safe havens for criminals. Neither should they be safe havens for international terrorists or spies, especially since we know that terrorists and spies have used libraries to plan and carry out activities that threaten our national security.*[46]

Meanwhile, FBI director Robert Mueller has assured Congress that the agency has not actually searched any libraries. However, many privacy advocates and perhaps a growing number of people in Congress are not willing to accept such assurances. The Security and Freedom Enhancement (SAFE) Act has been introduced as a modification to USA PATRIOT. It would require that agencies provide specific reasons to justify sneak and peak warrants or to allow searches of library or bookstore records.

THE NATIONAL ID DEBATE

In many respects the requirement for identification has become a normal part of modern life. Identification is needed to cash a check or (in most cases) to check into a hotel or rent a car. In this country, driver's licenses already serve as de facto universal identifiers, but their format varies from state to state, and many are fairly easy to fake.

One of the proposals for fighting terrorism is to develop a secure national identification system that might make it harder for terrorists to penetrate and move within our society. More than a hundred countries (including most of the European democracies) already have national identification systems. Besides its potential value against terrorism, a national ID might also help the nation get a handle on immigration, particularly if the system included a way to regularize the status of undocumented immigrants.

Culturally, identification, however, has long been a symbol of regimentation, of everything un-American. "Show me your papers" (often in a bad German accent) is a staple of World War II movies. As one observer notes:

> *The need to identify oneself may be intrinsically distasteful to some people. For example, they may regard it as demeaning, or implicit recognition that the organization with whom they are dealing exercises power over them. Many people accept that, at least in particular contexts, an organization with which they are dealing needs to have their name. Some, however, feel it is an insult to human dignity to require them to use a number of a code instead of a name. Some feel demeaned by demands, as part of the identification process, that they reveal information about themselves or their family, or embarrassed at having to memorize a password or PIN.*[47]

Another commentator offers a cultural critique:

> *For the purposes of a national ID card, identity is a unique, unchanging set of distinguishing characteristics: the flecks in one's iris, the ridges of one's left thumb. It's what sets us apart from others and from the mass. As Americans, though, we have a higher identity: free agent, self-legislator, citizen. It's a common identity held individually. It's what allows us to bond and make a nation or, if necessary, dissolve our bonds. This identity can't be captured on a card, but there is a risk it could be supplanted by one.*[48]

What is the relationship between identification and privacy? Two writers think they are closely intertwined:

> *There is an inherent tension between authentication and privacy, because the act of authentication involves some disclosure and confirmation of personal information. Establishing an identifier or attribute for use within an authentication system, creating transactional records, and revealing information used in authentication to others with unrelated interests all have implications for privacy.*[49]

But when is identification truly necessary for security? Recently cyber-activist John Gilmore has challenged the requirement that airline passengers show ID before boarding. Although he lost the first round of his legal challenge and seems unlikely to prevail, Gilmore points out that the combination of rather easy-to-fake IDs and a hidden "terrorist watch list" of dubious accuracy seems unlikely to be an effective deterrent to terrorists:

> *There is good reason to believe that any list of "known terrorists" contains "suspected" terrorists, not actual terrorists, and is full of errors besides. Particularly when the list is secret and neither the press nor the public can examine it for errors or political biases.*
>
> *"Johnnie Thomas" was on the watch list because a 28-year-old "FBI Most Wanted" man, Christian Michael Longo, used that name as an alias. But Longo was arrested two days after joining the "Most Wanted" list for murdering his family. After he had been in custody for months, 70-year-old black grandma "Johnnie Thomas" gets stopped every time she tries to fly.*[50]

Nevertheless, few people believe there is something inherently wrong with having to show ID before entering a sensitive area such as an airport. Ken Scheidegger of the Criminal Justice Legal Foundation points out that: "The Fourth Amendment forbids not searches that you don't like, it forbids unreasonable searches. Nothing could be more reasonable at this time than to know who you're flying with."[51]

Public support for a national ID peaked shortly after the September 11 attacks, when a poll by the Pew Research Center showed 70 percent of respondents supporting the idea. Only a few months later, though, a survey by Gartner Inc. showed only 26 percent in favor. However, support varied with the proposed use of the ID: A majority supported the use of IDs and databases in airports, but much fewer supported using the national ID to access routine services such as banking and health care. This suggested, according to Julia Scheeres, "that people would only support a national ID for very specific, very limited purposes and that they're suspicious of what government agencies will do with their information,"[52]

This idea of a universal ID with a carefully limited application may seem paradoxical. But a closer look might lead to a more flexible system that provides security with a minimal intrusion on privacy. According to Jim Harper.

> *We need to take the focus off of identification and move it to authorization. Systems are available that could communicate, "This person is OK to enter your building" or get on your plane or whatever, without saying "This is Joe Smith." Through a diverse array of privately issued cards, people should be able to access goods, services, and infrastructure that they are qualified to access without giving up identifying information.*[53]

DNA Databases

In recent years science and technology have continued to offer new technologies for identifying people. One of the most familiar today is the use of

DNA in criminal investigations. While the matching of suspects' DNA to that found at a crime scene does not seem to involve widespread privacy concerns, the compilation of DNA databases is more problematic to many privacy advocates.

The first such efforts are focusing on violent felons (or all felons), sex offenders, drunk drivers, and other persons who have already entered the criminal justice system. In 2004 California passed a ballot proposition allowing for collecting DNA from arrested felons. However, the law has been challenged because it lacks a clear procedure by which an arrested person who is not charged (or is acquitted) can have his or her DNA removed from the database.

Biometrics: The New Face of ID?

Biometrics is the use of physical characteristics to identify individuals uniquely. While fingerprints are thus a form of biometrics, most recent attention has been focused on such technologies as facial scanning and recognition. Systems using eye (retinal or iris) scanning have also been in use at high-security installations.

A number of programs in development will bring large numbers of people in contact with biometric scanning and databases. By 2004 most major countries had incorporated scannable fingerprints, facial recognition, or other biometric features in their passports in response to pressure from the United States—although not without some opposition. In turn, the U.S. government has begun compiling a database of visitors' fingerprints as part of the US-VISIT program. By 2005 this program was already in use in 115 airports and 14 seaports in the United States. The program integrates 20 existing databases into a system that compares entrants' fingerprints, digital photographs, and other particulars with stored biometric, biographical, and travel data to determine who should be allowed to enter the country. Together with the database screening program being developed for use with domestic airline passengers (CAPPS II, now called Secure Flight), it is likely that the majority of people who travel will soon find information about them stored in vast government databases.

Critics of the widespread use of biometric and other data in such screening databases believe that all such systems must satisfactorily answer the following questions:

Storage: How is the data stored, centrally or dispersed? How should scanned data be retained?

Vulnerability: How vulnerable is the data to theft or abuse?

Confidence: How much of an error factor in the technology's authentication process is acceptable? What are the implications of false positives and false negatives created by a machine?

Authenticity: What constitutes authentic information? Can that information be tampered with?

Linking: Will the data gained from scanning be linked with other information about spending habits, etc.? What limits should be placed on the private use (as contrasted to government use) of such technology?

Ubiquity: What are the implications of having an electronic trail of our every movement if cameras and other devices become commonplace, used on every street corner and every means of transportation?[54]

Many critics believe that programs such as Secure Flight fail under a number of these criteria. Concerns about the quality of the data used were exacerbated for many civil libertarians when the TSA initially denied that it had quietly obtained passenger data from a number of airlines for test purposes. (It turned out the agency had obtained at least 12 million records without passengers' knowledge or permission from six airlines.)

Security expert Bruce Schneier believes the database is likely to generate two kinds of errors: "the Ted Kennedy problem, [in which] I'm not on the list but my name is or a name similar to mine is," and "the Cat Stevens problem, [in which] I'm on the list, but we have no idea why."[55]

The Transportation Security Agency argues it cannot release details about how the database works because of the fear that terrorists will be able to "game the system." However, without assurance that the data is accurate and without a specific way for innocent persons to be removed from the list, the ACLU and a number of critics in Congress continue to oppose the system.

Smart Cards and Chips

Another possibility for identification is to carry it in one's body rather than on it. For some time one has been able to have an identification chip implanted in one's pet to aid in its recovery at animal shelters. However, some humans are also starting to get "chipped." VeriChip is about the size of a grain of rice and is implanted in the arm. It is read using a special scanner. Starting in March 2004 a nightclub in Barcelona, Spain, began giving its VIP customers VeriChips they could use to bypass entry lines and keep track of their bar tabs. Developers see future uses for VeriChip as a means for making secure credit card and ATM transactions as well as for entry into airports, government buildings, and other secure areas.

The concerns about VeriChips are similar to those for "smart cards" and the previously discussed RFID chips—misuse of the data by its collector or misappropriation by other persons.

A SURVEILLANCE SOCIETY?

Most of the systems discussed so far are used (at least ostensibly) for specific, well-defined purposes such as commercial transactions, entry into secure areas, or travel. But another set of privacy concerns arise through the ubiquitous use of cameras to watch people in public or sometimes private places.

CAMERAS EVERYWHERE

At home, surveillance cameras at entryways and around the perimeter are a popular option for security-conscious upscale homeowners. Parents concerned that their child's sitter is being neglectful (or worse) can install "nannycams." Their use seems legal, as with other forms of workplace monitoring. In a 2003 survey by *Parenting* magazine, 82 percent of respondents said they would install cameras only if they had reason to suspect their children were being abused.

Out on the street, public surveillance cameras have been used in Great Britain for a number of years. There is now about one camera for every 14 citizens. The reason given is normally public safety—in particular, reducing crime. However, most studies have so far failed to show that the cameras are actually effective in reducing the crime rate. A recent study by the British Home Office of 14 camera systems throughout the country found that only one was associated with a significant fall in the crime rate. Cameras may make people near the cameras feel safer, though perhaps more self-conscious.

Defenders of camera surveillance such as policy analyst Eugene Volokh suggest that the technology, by removing the human element, might reduce police harassment of individuals:

> *The camera . . . saw only what any passerby, and any police officer who might have been at the intersection, could lawfully see. I avoided any possibility of being pulled out and frisked, or my car being searched. I didn't have to wonder if I had been stopped because of my sex or race or age.*[56]

However, Volokh admits that if the cameras are connected to face-recognition software and the resulting recordings are stored indefinitely in a database, there would be a potential for abuse.

Critics such as libertarian columnist Jacob Sollum see intangible but significant social and psychological costs to the widespread use of camera surveillance:

> *. . . knowing you are being watched by armed government agents tends to put a damper on things. You don't want to offend them or otherwise call attention to yourself. . . . People may learn to be careful about the books and periodicals they read in public, avoiding titles that might alarm unseen observers. They may also put more thought into how they dress, lest they look like terrorists, gang members, druggies, or hookers.*[57]

There is an important distinction to be made between camera systems that work in more-or-less real time, with persons monitoring them and dispatching police where indicated, and systems that store images for later comparison to digital photographic or biometric data. The combination of cameras and face recognition software offers the potential of identifying persons without any cooperation on their part. An experimental system was first used in the 2001 Super Bowl. Such systems raise the question of when the line between crime

prevention and the possibly chilling surveillance of lawful activities (such as political protests) might be crossed.

The bomb attacks on the London transit system in July 2005 brought renewed attention to the possible value of public surveillance cameras in the fight against terrorism. Proponents of the cameras pointed out that within days of the attacks a review of camera footage had identified the bombing suspects. Critics, however, have suggested that the cameras would be unlikely to actually deter such attacks. A would-be suicide bomber, after all, would presumably not care if he or she might be identified after the attack. As for non-suicidal terrorists; they might simply seek other targets that lack camera surveillance.

Turning the Cameras Around

Today one does not have to be a big corporation or a police agency to conduct video surveillance. Cyberspace pundit Howard Rheingold notes that "You can bug people the way spy agencies used to do 20 years ago—really cheap now. The Orwellian vision was about state-sponsored surveillance. Now it's not just the state, it's your nosy neighbor, your ex-spouse and people who want to spam you."[58]

Thousands of webcams in a wide variety of settings now beam their pictures to web sites. Most ubiquitously, camera-equipped cell phones now provide more than a way to show one's friends what one's doing. They can also be used to surreptitiously capture images, whether to help catch criminals or terrorists or to further an enterprise such as blackmail. Futurist Paul Saffo notes that:

> *There are two dangers to being an amateur snoop. The first is, you'll find out something that you really would have been much happier not knowing. The second is, what happens when the subject finds out that you have been snooping? My advice is: Think twice before you do it. You may really regret it.*[59]

While surveillance technology in citizens' hands can of course be misused, it does offer a potential way to hold authorities accountable for abuses such as police brutality. For example, a camera could be set to capture images continuously and beam them wirelessly to a secure site on the Internet. In such a case, even if a criminal (or the police) seizes and destroys the camera, that very act becomes part of a record of evidence that has been placed out of reach.

We Know Where You Are

One of the fastest-growing technologies combines geographic information systems (GIS) with location systems (Global Positioning System, or GPS). These technologies are undoubtedly very useful. They make it possible to select a destination and get a route with just a few clicks, complete with detailed driving directions. Companies can route their delivery trucks more efficiently and track the movement of valuable goods from warehouse to destination. Government agencies can generate maps showing the best disaster response

and evacuation routes, or use computer models to predict the likely extent of a toxic spill.

However, when the movement of people rather than that of goods is the object of a tracking and monitoring system, how does that effect privacy—or the sense of privacy? So far the people who have been tracked have been those who for different reasons are generally viewed as having diminished rights. For example, it was proposed that public school children in Sutter, California, wear RFID tags around their necks, but parents objected—though children in Osaka, Japan, have had similar tags for some time. However, one does not have to wait for school: Individual parents can buy GPS/radio "kid trackers" for about $200.

Many people may not realize their location is already being tracked continuously. Originally GPS capability was added to cell phones to make it easier to find people who have made a 911 call, but some companies have required that their workers carry them. Now the manager can tell at a glance where construction crews are working—and whether a worker has snuck home early. Of course, there are other uses, as Greg Shields, proprietor of the Spygear Store in Cincinnati, notes: "I would say that 60 percent of my sales are to women who say, 'I think my husband is cheating on me.'"[60]

Soon new cars may come with built-in trackers and recorders. The National Transportation Safety Board has proposed that event data recorders (EDRs) be installed. The devices, much like the "black box" recorders in aircraft, would maintain a record of a car's speed and driving characteristics. Stolen cars could be tracked, as with the already used "Lo-jack" devices. Already services such as OnStar (now becoming available in midrange cars) feature the ability to call for help to someone who will be able to tell police or ambulance services exactly where the driver is located. The car can also be unlocked remotely—a boon to someone who has lost his or her keys.

Such devices raise privacy concerns. Could law enforcement officers or cruising hackers listen in on a driver's calls? At any rate there is already a case where a federal appeals court told authorities they couldn't install a wiretap in the car systems of a suspect. However, the judges rejected the request not for privacy reasons but because of the possibility that the wiretap would prevent the driver from being able to obtain emergency service.

The growing desire and ability to track peoples' movements has given rise to a new term: "locational privacy." As one policy analyst notes:

> *While one must expect to surrender some privacy in public spaces, location surveillance and processing technology has the potential to invade an individual's privacy to such a degree that even maintaining anonymity becomes impossible. To attempt to understand what the reasonable expectation of privacy in the case of location-tracking technology, one can ask these three questions: (1) Would it have been possible to obtain the same information without using the technology in question?: (2) If so, would it have been possible to use the data without additional computer processing?: and (3) If the alternate means of obtaining this information had been employed, or if the additional data processing had been performed, would either have constituted unreasonable surveillance?*[61]

PROSPECTS AND ALTERNATIVES

The growing sophistication and pervasiveness of identification, surveillance, and tracking systems may suggest that the effort to preserve privacy is doomed to failure in the long run. However, there are a number of tools and technologies that may prove helpful for privacy protection. But how do Americans feel about their alternatives?

PRIVACY AND ACCOUNTABILITY

One important strategy to protect privacy is to enhance the ability of people to know what the government is up to. This means access to the information the government generates about its own activities. A survey by the American Society for Newspaper editors reported in 2001 some relevant public attitudes:

- Six in 10 Americans see public access as "crucial" to good government.
- Sixty-one percent are "very concerned" about personal privacy; 28 percent "somewhat concerned."
- Thirty-eight percent very concerned about government secrecy; 34 percent somewhat concerned.
- Forty-eight percent believe there is too little access to government records; 30 percent "just the right amount."

The same survey suggests how people might want to balance the right of access to government information and the privacy of government officials and employees themselves: 30 percent believe laws guaranteeing public access to government records should be strengthened, even if it means Americans may lose some privacy in the process. However, 54 percent believe that laws guaranteeing personal privacy should be strengthened, even if it means Americans may lose public access to some records held by the government. About half of respondents agreed that citizens have "no control" over how personal information about them is used by the government and that consumers have no control over how personal information about them is used by private companies.[62] These results suggest an ongoing deep concern with loss of control of personal privacy but less consensus on what to do about it.

PRIVACY TOOLS: ENCRYPTION AND ANONYMITY

Technology itself offers powerful tools to protect privacy. One important tool is encryption, which makes information unreadable except by its owner or intended recipient. Until the 1990s, the use of encryption was pretty much restricted to the government and to certain businesses with powerful computers and special communications systems. A much more user-friendly encryption system was offered in 1991 by a programmer-activist named Phil Zimmermann.

He released a program called Pretty Good Privacy, or PGP. This program uses a kind of coding called public key cryptography in which the decoding keys come in pairs that have a special relationship: Text encoded using one of the keys can only be read using the other key.

A user can distribute one key in the pair, called the public key. Anyone can use the public key to encode a message that can be read only by the person holding the corresponding private key. The private key itself need never be sent anywhere, so it is hard to steal. Further, if one receives a message encoded with a person's private key, one can be sure that it was sent by that person. The private key can thus serve as a "digital signature" that verifies the identity of the sender.

Throughout the 1990s a battle raged between activists such as Zimmermann and self-proclaimed "cypherpunks" and government agencies who did not want powerful encryption to get into the hands of foreign nations. Law enforcement agencies were also faced with a problem: What good was a search or wiretap warrant if the message seized was encrypted and couldn't be read?

Federal authorities first tried to use export restrictions to prevent the distribution of PGP and similar programs. It soon became clear that nothing could stop the spreading of computer code through the worldwide Internet. (Later, another programmer, Daniel Bernstein, would win a court decision overturning the export regulations concerning computer code.)

The government then suggested a compromise: have all computers and communications equipment include a device called the Clipper Chip. This device would provide powerful encryption, but with a catch: The government would retain a key that it could use to read any message encrypted by the device, presumably after obtaining a court order. Privacy advocates, however, argued that there was no independent proof the proposed encryption system was secure, and no way to make sure the government did not abuse its ability to read the code. Further, industry observers questioned whether people would use a government-provided encryption chip in place of software such as PGP.

Eventually, the government dropped the Clipper Chip in favor of a proposal to allow users to employ the encryption software of their choice provided that they deposited a copy of the encryption key with a third-party "escrow" agency. The government, after obtaining a court order, could then obtain the key from the agency. This proposal, too, failed to win public or industry support.

Today encryption is routinely and seamlessly used for online transactions and to protect wireless networks (to some extent). Individuals can also use PGP and other programs to encrypt data on their hard drives.

While encryption hides the data, anonymity conceals the identity of persons involved in communications or transactions. Anonymity can be harder to find than encryption, because people leave so many "tracks" online that could be used to identify them. This is particularly true, as we have seen, when "profiles" of individuals are created and databases accumulated. Thus, according to Catherine Crump,

> *Data retention aims to change the context of Internet activity. The context change that data retention renders makes it easier to link acts to actors. Data*

> *retention "rearchitects" the Internet from a context of relative obscurity to one of greater transparency. This manipulation of context influences what values flourish on the Internet. Specifically, data retention, by making it easier to link acts to actors, promotes the value of accountability, while diminishing the values of privacy and anonymity.*[63]

There are some tools that promote anonymity, such as the use of "digital cash," services that allow payments to be authenticated without passing identification information, and the use of services that allow e-mail to be sent without address information that can identify the sender. However, these tools are relatively obscure and not widely used.

There is an inherent conflict between anonymity and accountability: If people can act anonymously, how can they be identified and held responsible if they do something wrong? Law enforcement agencies want access to the records of Internet Service Providers in order to be able to investigate online crime, for example. And some experts suggest that the only way to address the scourge of spam is to redesign the e-mail system so that each user will be identified and authenticated before being allowed to send messages. Yet our courts have recognized a right to anonymous activity that traces its roots in the pamphleteers of colonial times. Anonymity can protect the right of the vulnerable to speak out without repression.

RETHINKING PRIVACY

The struggle between competing interests of privacy, anonymity, security, and accountability is likely to be with us for the foreseeable future. Perhaps, though, some new ways of thinking about privacy might allow for better solutions.

Privacy was first tied to place (such as one's home) and then to reasonable and customary expectations. There has remained a sense, however, of privacy as being all or nothing: In a given situation one either has it or not. But Justice Thurgood Marshall, dissenting in *U.S. v. Miller*, suggested a different approach. He noted that just because

> *a phone company monitors a call for internal reasons, it does not follow that they expected this information to be made available to the public in general or the government in particular. Privacy is not a discrete commodity, possessed absolutely or not at all.*

In this view privacy is a dynamic concept: It requires that one look not simply at whether one can expect in a given situation never to be observed or to have one's information used but also at what happens when that observation or information is taken out of context and used for another purpose.

Another voice from the legal community urges that the complexity of the information society requires an equally sophisticated notion of privacy:

> *Privacy in the information age is best conceived as the maintenance of metaphorical boundaries that define the contours of personal identity. Identity is complex; different circumstances reveal different aspects of our nature. Each of us wears many masks wherein each mask reflects a different aspect of who we really are. We do not want our entire natures to be judged by any one mask, nor do we want partial revelations of our activities to define us in a particular situation as other than who we want to be. In short, we want to choose the masks that we show to others; any such loss of choice is painful, amounting almost to a physical violation of the self. When we are secretly watched, or when information that we choose to reveal to one audience is instead exposed to another, we lose that sense of choice.*[64]

As difficult as it might be, the protection of privacy seems to require that we develop a way of thinking about social interaction and the use of information that is at least as sophisticated as the technology we have embraced. This may involve a number of efforts such as:

- using regulation to create "firewalls" around the most serious forms of misuse of private information,
- where people might reasonably choose to trade privacy for convenience or other values, allowing them to do so by ensuring they have accurate knowledge and can hold businesses accountable to keep their part of the bargain,
- encouraging technologies such as the Platform for Privacy Preferences that allow users to screen for web sites that meet their privacy expectations,
- trying to ensure that identification and database systems used to protect infrastructure and national security are used only for those purposes,
- making such systems as transparent and accountable as possible, at minimum ensuring that Congress has continual, vigorous oversight over them, and
- encouraging a robust, ongoing debate on the privacy implications of new technologies and programs while there is still time to shape their implementation.

If these and other efforts are pursued, the result might be, paradoxically, a world in which although we may have to give up more of our abstract privacy because of the increasing interdependence and fragility of our society, we may have greater assurance of privacy where it counts. In the words of Travis Charbeneau,

> *A simultaneously more open and open-minded society [that] enables us to shrink our respective privacy spheres. A smaller, more manageable privacy sphere, safeguarding only those issues that remain genuinely sensitive, [that] means more certain protection irrespective of technological advance.*[65]

The complexity of privacy issues and the inevitable presence of compelling, conflicting concerns make achieving a comprehensive solution to all privacy concerns unlikely. However, society may be able to reach a consensus on certain

principles and create mechanisms to ensure that they be applied as each new technology emerges.

---

[1] Robert Ellis Smith, *Ben Franklin's Web Site*. Providence, R.I.: Privacy Journal, 2000, p. 6.

[2] Lewis Brandeis, dissent in *Olmstead v. United States* (1928).

[3] Alan F. Westin, quoted in Fred H. Cate, *Privacy in the Information Age*. Washington, D.C.: Brookings Institution Press, 1997, p. 22.

[4] Jeffrey Rosen. *The Unwanted Gaze: The Destruction of Privacy in America*. New York: Random House, 2000, p. 7.

[5] Robert Ellis Smith, quoted in David Brin, *The Transparent Society*. Reading, Mass.: Addison-Wesley, 1998, p. 77.

[6] Alastair Fowler, *A History of English Literature*. Cambridge, Mass.: Harvard University Press, 1987, p. 184.

[7] William Pitt, quoted in Philippa Strum, *Privacy: The Debate in the United States Since 1945*. Fort Worth, Tex.: Harcourt, 1998, p. 116.

[8] John Adams, quoted in Strum, *Privacy*, p. 116.

[9] Ralph Waldo Emerson, "Self-Reliance," *The Works of Ralph Waldo Emerson*. Available online. URL: http://www.rwe.org (link under Complete Works/Essays).

[10] Charles Darwin, quoted in Jack Meadows, *The Great Scientists*. New York: Oxford University Press, 1987, p. 167.

[11] Samuel D. Warren and Louis Brandeis. "The Right to Privacy." *Harvard Law Review*, vol. 4, December 15, 1890, p. 193ff. Also available online. URL: http://faculty.uml.edu/sgallagher/Brandeisprivacy.htm

[12] Erik Davis, *Techgnosis: Myth, Magic + Mysticism in the Age of Information*. New York: Harmony Books, 1998, p. 67.

[13] George Orwell, *1984*, quoted in Harold Bloom, ed., *George Orwell*. New York: Chelsea House, 1986, p. 136.

[14] Cited in Simon Davies, *Big Brother*. London: Pan Books, 1996, p. 53.

[15] Simson Garfinkel, "Privacy and the New Technology: What They Do Know Can Hurt You," *The Nation*, vol. 270, February 28, 2000, p. 11ff.

[16] Ted Nelson, quoted in Vince Juliano, "Computer Lib (& Dream Machines) by Ted Nelson: A Review." Available online. URL: http://cla.uconn.edu/reviews/cmptrlib.html. Posted in November 1996.

[17] William Gibson, *Neuromancer*, excerpted in Larry McCaffrey, ed., *Storming the Reality Studio: A Casebook of Cyberpunk and Postmodern Science Fiction*. Durham, N.C.: Duke University Press, 1991.

[18] Lawrence H. Tribe, "The Constitution in Cyberspace." Available online. URL:.http://www.epic.org/free_speech/tribe.html. Posted in 1991.

[19] Quoted in Robert B. Gelman and Stanton McCandlish, *Protecting Yourself Online*. San Francisco: Harper/Edge, 1998, p. 35.

[20] From the Federal Privacy Commission, quoted in American Civil Liberties Union, *Your Right to Privacy*. Carbondale: Southern Illinois University Press, 1990, p. 119.

[21] For extensive coverage of identity theft, online frauds and scams, and other information-related crime, see the Library in a Book volume *Internet Predators*, by Harry Henderson. New York: Facts On File, 2005.

[22] Carole A. Lane, *Naked in Cyberspace: How to Find Personal Information Online*. Wilton, Conn.: Pemberton Press, 1997, p. 3.

[23] William Wresch, *Disconnected: Haves and Have-Nots in the Information Age*. New Brunswick, N.J.: Rutgers University Press, 1996, p. 93.

[24] Paul H. Rubin and Thomas M. Lenard, *Privacy and the Commercial Use of Personal Information*. Boston: Kluwer Academic Publishers, 2002. Also available online. URL: http://www.pff.org/issues-pubs/books/010701privacyandpersonalinfo.pdf. Posted in July 2001.

[25] Declan McCullagh, "The Upside of 'Zero Privacy,'" Reason Online. Available online. URL:http://www.reason.com/0406/fe.dm.database.shtml. Posted in June 2004.

[26] Erik Baard, "Smile, You're On In-Store Camera," Wired News. Available online. URL:http://www.wired.com/news/print/0,1294,54078,00.html. Posted on August 8, 2002.

[27] Chris Jay Hoofnagel, "Privacy Risks of E-mail Scanning," Electronic Privacy Information Center. Available online. URL:http://epic.org/privacy/gmail/casjud3.15.05.html. Posted on March 15, 2005.

[28] For more survey material, see Joseph Turow, *Americans & Online Privacy: The System Is Broken*. University of Minnesota Annenberg Public Policy Center, June 2003. Also available online. URL:http://www.asc.upenn.edu/usr/jturow/internet-privacy-report/36-page-turow-version-9.pdf. Posted in June 2003.

[29] Ann Cavoukian and Tyler J. Hamilton, "Privacy Payoff: Better Customer Data," *Computerworld*, March 15, 2004, n.p. Also available online. URL: http://www.computerworld.com/printthis/2004/0,4814,90126,00.html.

[30] Jerry Kang, "Information Privacy in Cyberspace Transactions." *Stanford Law Review*, vol. 50, 1998, p. 1193ff.

[31] Katrin Schatz Byford, "Privacy in Cyberspace: Constructing a Model of Privacy for the Electronic Communications Environment," *Rutgers Computers & Technology Law Journal*, vol. 24 (1998), p. 1ff.

[32] "New Federal Health Privacy Regulation: Questions and Answers." Available online. URL:http://www.healthprivacy.org/usr_doc/Q&A2000.pdf. Downloaded on April 4, 2005.

[33] Quoted in Electronic Privacy Information Center, "Medical Records." Available online. URL:http://www.epic.org/privacy/medical/. Updated on July 8, 2004.

[34] Nina Schwenk, quoted in Steven Johnson, "Trading Privacy for Health," *Discover*; vol. 25, December 2004, n.p. Also available online. URL: http://www.discover.com/issues/dec-04/departments/emerging-technology. Posted in December 2004.

[35] Dale Miller, quoted in Beth Givens, "Ten Privacy Principles for Health Care," Privacy Rights Clearinghouse. Available online. URL: http://www.privacyrights.org/ar/privprin.htm. Posted on November 6, 1998.

[36] "Health Privacy in the Hands of Government: HIPAA Privacy Regulation—Troubled Process, Troubling Results," Privacilla.org. Available online. URL: http://www.privacilla.org/releases/HIPAA_Report.pdf. Posted in April 2003.

[37] Nancy Wexler, quoted in Lauren Picker, "All in the Family," *American Health*, March 1994, p. 24.

[38] Christine Godsil Cooper, "Your Genes or Your Job: Genetic Testing in the Workplace," *Employee Rights Quarterly*, vol. 3, Fall 2002, pp. 1ff.

[39] Roger Matus, quoted in Andrew E. Taslitz, "The Fourth Amendment in the Twenty-First Century: Technology, Privacy, and Human Emotions," *Law and Contemporary Problems*, vol. 65, Spring 2002, p. 125ff.

[40] Quoted in Anne Kandra, "Should Parents Become Big Brother? New Software Allows Parents to Control Virtually Everything Children Do Online," *PC World*, vol. 22, January 2004, p. 59ff.
[41] Quoted in Strum, *Privacy*, p. 148.
[42] *United States v. United States District Court*, 407 U.S. 297, 320 (1972).
[43] John Shattuck, quoted in Strum, *Privacy*, p. 154.
[44] Robert Pitofsky, quoted in K. Curran, "War on Terror Worries Privacy Advocates," NewsMax.com. Available online. URL: http://www.newsmax.com/archives/articles/2001/10/30/162113.shtml. Posted on October 31, 2001.
[45] Alberto Gonzales, quoted in Edward Epstein, "White House Willing to Scale Back Patriot Act," *San Francisco Chronicle*, April 6, 2005, pp. 1, 11.
[46] Alberto Gonzales, quoted in Epstein, "White House Willing to Scale Back Patriot Act."
[47] Roger Clarke, "Human Identification in Information Systems: Management Challenges and Public Policy Issues," *Information Tech and People*, vol. 7, December 1994, pp. 6–37. Also available online. URL: http://www.anu.edu.au/people/Roger.Clarke/DV/HumanID.html. Posted in December 1994.
[48] Walter Kirn, "The Mother of Reinvention: The Real Reason Americans Detest the Idea of a National ID Card," *The Atlantic Monthly*, vol. 289, May 2002, p. 28ff.
[49] Stephen T. Kent and Lynette I. Millett, eds., *Who Goes There? Authentication Through the Lens of Privacy*. Washington, D.C.: National Academies Press, 2003, p. 6.
[50] John Gilmore, "Gilmore v. Ashcroft—FAA ID Challenge FAQ." Available online. URL: http://cryptome.org/gilmore-v-usa-faq.htm. Posted on July 20, 2002.
[51] Ken Scheidegger, quoted in Richard Willing, "Airline ID Requirement Faces Legal Challenge," USA Today.com. Available online. URL: http://www.usatoday.com/news/nation/2004-10-10-privacy_x.htm. Posted on October 10, 2004.
[52] Julia Scheeres, "Support for ID Cards Waning," Wired News. Available online. URL:http://www.wired.com/news/print/0,1294,51000,00.html. Posted on March 13, 2002.
[53] Jim Harper, "A National ID: Government Initiatives and the Private Sector," Privacilla.org. Available online. URL: http://www.privacilla.org/releases/CDIA_Remarks_01-27-05.html. Posted on January 27, 2005.
[54] "Biometric Identifiers." Electronic Privacy Information Center. Available online. URL:http://www.epic.org/privacy/biometrics. Updated on March 30, 2004.
[55] Bruce Schneier, quoted in Kim Zettner, "A CAPPS by Any Other Name," Wired News. Available online. URL: http://www.wired.com/news/print/0,1294,67015,00.html. Posted on March 25, 2005.
[56] Eugene Volokh, "Big Brother Is Watching—Be Grateful!" *Wall Street Journal*, March 26, 2002, p. A2.
[57] Jacob Sollum, quoted in Barry Steinhardt, testimony before the Committee on the Judiciary, Council of the District of Columbia, Washington, D.C., December 12, 2002. Available online. URL:http://www.aclu.org/Privacy/Privacy.cfm?ID=13505&c=130. Posted on December 12, 2002.
[58] Howard Rheingold, quoted in Janet Kornblum, "Prying Eyes Are Everywhere," *USA Today*, April 14, 2005, p. 1D.
[59] Paul Saffo, quoted in Kornblum, "Prying Eyes Are Everywhere," p. 10.
[60] Greg Shields, quoted in David Colker, "Go Ahead, Just Try to Disappear," *Los Angeles Times*, December 27, 2004, p. A1.

[61] James C.White, "People, Not Places: A Policy Framework for Analyzing Location Privacy Issues," Terry Sanford Institute of Public Policy, Duke University. Available online. URL: http://www.epic.org/privacy/location/jwhitelocationprivacy.pdf. Posted in Spring 2003.

[62] For these and other results of public opinion surveys on private issues, see Electronic Privacy Information Center, "Public Opinion on Privacy." Available online. URL: http://www.epic.org/privacy/survey. Updated on July 15, 2004.

[63] Catherine Crump, "Data Retention: Privacy, Anonymity, and Accountability Online," *Stanford Law Review*, vol. 56, October 2003, p. 191ff.

[64] Andrew E. Taslitz, "The Fourth Amendment in the Twenty-first Century: Technology, Privacy, and Human Emotions," *Law and Contemporary Problems*, vol. 65, Spring 2002, p. 125ff.

[65] Travis Charbeneau, "The Future of Privacy: Moot?" ItmWeb.com. Available online. URL: http://www.itmweb.com/f010501.htm. Posted on January 5, 2001.