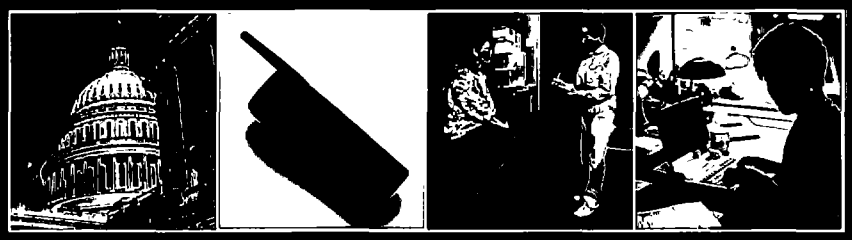
CONGRESS 6

THE PEOPLE

Nothing Sacred

THE POLITICS OF PRIVACY



THE CENTER FOR PUBLIC INTEGRITY

Nothing Sacred

THE POLITICS OF PRIVACY

THE CENTER FOR PUBLIC INTEGRITY

About the Center for Public Integrity

THE CENTER FOR PUBLIC INTEGRITY, founded in 1989 by a group of concerned Americans, is a nonprofit, nonpartisan, tax-exempt educational organization created so that important national issues can be investigated and analyzed over a period of months without the normal time or space limitations. Since its inception, the Center has investigated and disseminated a wide array of information in more than thirty published Center Reports. The Center's books and studies are resources for journalists, academics, and the general public, with databases, backup files, government documents, and other information available as well.

This report and the views expressed herein do not necessarily reflect the views of the individual members of the Center for Public Integrity's Board of Directors or Advisory Board.

THE CENTER FOR PUBLIC INTEGRITY
1634 I Street, N.W.
Suite 902
Washington, D.C. 20006
Telephone: (202) 783-3900
Facsimile: (202) 783-3906
E-mail: contact@publicintegrity.org
http://www.publicintegrity.org

ISBN: 1882583-12-4
Printed in the United States of America

THE INVESTIGATIVE TEAM

Executive Director
Charles Lewis

Director of Investigative Projects
Bill Hogan

Chief of Research
Bill Allison

Senior Editor
William O'Sullivan

Writers
Paul Cuadros
Patrick J. Kiger
Jeff Shear

Senior Researchers
David Engel
Adrianne Hari
Eric Wilson

Researchers
Lloyd Brown
Justin Buchler
Megan Chernly
Russell Eckenrod
Nicole Gill
Melanie Strong

The Center for Responsive Politics
Larry Makinson, Executive Director
Sheila Krumholz, Project Director

Contents

Summary 1

1 The Invaders 11

2 No Limit 17

3 An Unlocked Door 25

4 The Watchful Eye 39

5 The Data Octopus 51

List of Tables 55

Notes 63

Summary

In February 1998, Dr. Louis Hafken, a psychiatrist in Providence, Rhode Island, received a letter from PharmaCare, whose stock-in-trade is reviewing prescription-drug benefits for insurers and employers. Along with the letter, PharmaCare sent Hafken a printout of the prescription records of one of his patients, noting that she was taking Ativan, an anti-anxiety drug usually indicated for short-term use. The company wanted to know why the patient was being treated with the medication. Was it for alcohol withdrawal? Anxiety? Depression? Panic disorder? In addition, PharmaCare wanted to know whether Hafken intended to continue treating her with Ativan.[1]

"It's one thing to provide some general information about a drug to a doctor and make suggestions about using it," Hafken told the Center for Public Integrity. "But they wanted a reply to the letter, feedback as to what was going to be done. If the person wasn't going to be taken off the drug, they wanted to know why."

Something else worried Hafken even more. The letter identified the patient as an employee of CVS, the nation's largest drugstore chain and the parent company of PharmaCare. Hafken found it chilling that CVS was looking through its prescription databases, scrutinizing what medications an employee was taking, and telling her psychiatrist how to treat her. "Frankly," Hafken said, "it's none of their business."[2]

After Hafken went public with his complaint, a CVS spokesman told *The Providence Journal-Bulletin* that the company conducted such investigations "to improve the quality of care to our employees and to contain our benefit costs" and said there were "strict measures in place to ensure that confidentiality is maintained."[3] But those words didn't calm Hafken. His patient, he noted, was "uncomfortable" to discover that her employer had been examin-

ing records of her psychiatric treatment. Increasingly, he told the Center, many of his patients "are afraid to be completely honest in therapy" out of fear that others besides their doctor will learn their innermost secrets.[4]

Unfortunately, such privacy-related fears are justifiable.

Thirty-five years ago, social critic Vance Packard wrote in his book *The Naked Society,* perhaps the first broad-ranging investigation of privacy abuses in the United States:

> America was largely settled, and its frontiers expanded, by people seeking to get away from something unpleasant in their pasts, either oppression, painful episodes, poverty, or misdemeanors. Today, it is increasingly assumed that the past and present of all of us—virtually every aspect of our lives—must be an open book; and that all such information about us can be not only put in files but merchandised freely. Business empires are being built on this merchandising of information about people's private lives. The expectation that one has a right to be let alone—the whole idea that privacy is a right worth cherishing—seems to be evaporating among large segments of our population.[5]

At the time of Packard's expose, privacy abuses were so rampant that they posed a threat to democracy itself. Packard depicted a federal government gone paranoid in its zeal to ferret out potential traitors. Nearly 14 million Americans, he wrote, had been scrutinized in some sort of security or loyalty investigation. The U.S. Post Office routinely opened and inspected the mail of those with unpopular political views. A 1963 order by President Kennedy authorized the Internal Revenue Service to turn over citizens' tax returns to the House Un-American Activities Committee on request. The U.S. Civil Service Commission maintained dossiers containing negative information on an estimated 250,000 Americans.

But as Packard warned, Americans' privacy was being invaded not only by government agencies seeking power but also by companies seeking profit. Private credit bureaus compiled dossiers on tens of millions of Americans; in addition to their borrowing history, bureaus routinely obtained from banks the balances of subjects' savings accounts and deployed roving teams of investigators to hunt down information of any and all kinds. Three hundred dollars paid to a private investigator could obtain a person's complete hospitalization records, and $500 could buy a look at the paperwork from his or her stay in a mental institution. Corporate personnel directors sent private detectives to interview neighbors and former coworkers of job applicants and

hooked the applicants up to polygraph machines so they could ask them such questions as "Are you inclined to be homosexual?"[6]

Packard's book was the first salvo in a battle by Americans to take back their privacy, and Congress became, for a time, a key ally in that fight. In the mid-1960s, some lawmakers—jolted into action by the Johnson Administration's proposal to create a national computer database of information on citizens—began to scrutinize the government's own information-gathering activities. Over the next three decades, Congress passed more than a dozen bills that dealt in some respect with protecting citizens' personal privacy. Among them was the Fair Credit Reporting Act of 1971, which put restrictions on what sort of information businesses could gather on consumers and, among other things, gave consumers a right to challenge incorrect information.[7]

In the mid-1960s, some Capitol Hill lawmakers—jolted Into action ▪ the Johnson Administration's proposa▪ ▪o crea▪e a national computer database Or information on citizens—began to scrutinize the government's own Information-gathering activities.

Nevertheless, nearly 35 years after Packard sounded his alarm, Americans are still worried about their personal privacy. In a 1997 Harris-Westin survey for the Center for Social and Legal Research, 92 percent of the respondents said that they were "concerned" about threats to their privacy; 64 percent said they were "very concerned."[8] To be sure, many still worry about government surveillance, even though they now enjoy the protection of such laws as the Privacy Act of 1974, which limits the use of government information and entitles citizens to see some of the data gathered about them. Increasingly, however, when Americans see a shadow over their shoulders, it's one cast by business. In a 1996 Harris-Equifax survey, one of the nation's three major credit bureaus, 83 percent of the respondents agreed that consumers no longer had control over how companies collected and used their personal information.[9]

Americans' privacy is being compromised and invaded from many angles. Sensitive financial and personal data is collected, bought, and sold by thousands of companies, often without the subjects' permission or even knowledge. The most sensitive details of health-care records are similarly available to prying eyes. In the workplace, telephone conversations are often monitored, and sophisticated computer systems track everything from the number of keystrokes employees type to the frequency with which they get up from

their desks. Hidden video cameras even spy on them in locker rooms and restrooms.

In Newport Beach, California, a department-store employee was disturbed to learn that the room where she and other women changed clothes was monitored by a hidden video camera.[10] In many parts of the country, health-insurance subscribers find that to get mental-health coverage, they have to reveal intimate details of their psychotherapy sessions to an anonymous voice at the other end of a telephone line. A clerk for one insurance company discovered during his computer training that anyone at the company could access details of his treatment, including the antidepressant medication he was taking at the time." Across the nation, banks scrutinize customers' credit-card bills for certain types of transactions—such as payments to a marriage counselor or an auto-repair shop—that are viewed as warning flags of financial trouble, even if the customer has a good payment history.[12]

Despite laws on the books that address the issue, Americans' privacy is still threatened. One reason, unfortunately, is Congress. Since the 1970s, privacy advocates have urged lawmakers to enact an overarching law spelling out citizens' basic rights to privacy, as democracies in Europe and elsewhere have done. In 1995, for example, Representative Cardiss Collins, a Democrat from Illinois, introduced the Individual Privacy Protection Act, which would have created a government board to investigate privacy breaches and develop additional legislation for expanding the Privacy Act's restrictions on the handling of personal data to cover not just government but business as well.[13] Collins's proposal went nowhere.[14] Capitol Hill lawmakers seem to prefer dealing with privacy issues on a piecemeal basis, passing laws that narrowly focus on certain activities and industries. That's why federal law protects the confidentiality of the videotapes you rent and the cable-TV shows you watch but affords no protection for your psychotherapy records or what books you borrow from the library.

In many parts of the country health-insurance subscribers find that to get mental-health coverage, they have to reveal intimate details of their psychotherapy sessions to an anonymous voice at the other end of a telephone line.

While Congress took relatively strong action to curb privacy abuses by federal agencies in the 1960s and 70s, lawmakers have been much more lenient toward the gathering and use of personal data by businesses. In 1988, for instance, Congress put strict restraints on the use of polygraph testing by employers—but chose to allow employers to probe appli-

cants' minds with psychological tests, even after the federal Office of Technology Assessment presented it with a 1990 report documenting the tests' intrusive nature.[15]

As a nonprofit, nonpartisan organization that publishes investigative studies about public-service and ethics-related issues, the Center for Public Integrity does not take formal positions on legislative matters, and we certainly have no "agenda" when it comes to public-policy alternatives in the area of privacy. As with nearly all of our past 32 reports released since 1990, our interest is straightforward: examining the decision-making process of government and whether or not it has been distorted in any way.

This major Center investigation involved conducting scores of interviews and reviewing thousands of pages of data from the Federal Election Commission and the Center for Responsive Politics, House and Senate lobbying and financial disclosure reports, and congressional hearing transcripts, in addition to thousands of secondary sources.

Time and time again, we found, Congress has put big-money corporate interests ahead of the basic privacy interests of the American people.

Among the Center's principal findings:

- Congress first heard testimony on the problem of medical-records confidentiality in 1971;[16] 27 years later, it still hasn't enacted legislation to curb abuses (although this year, several medical-privacy bills again await consideration). And Capitol Hill lawmakers have been amply rewarded for rejecting efforts to apply greater privacy protections to health-care records. Since 1987, the nation's hospitals, insurance companies, and members of trade associations that oppose such protections have poured more than $45.6 million into congressional campaigns.

- Anti-privacy interests have little trouble finding Members of Congress to do their bidding. In 1995, Representative David Hobson, a Republican from Ohio, tacked an industry-written proposal for the exchange of computerized medical records onto legislation aimed at overhauling Medicare and Medicaid. "I'm flabbergasted and impressed," Thomas Gilligan, the chief lobbyist for the Association for Electronic Health Care Transactions, told a trade publication at the time. "I think Hobson has done the industry a service." Since 1987, Hobson has collected more than $65,000 from the anti-privacy lobby.

• When Congress drafted the Health Insurance Portability and Accountability Act of 1996, popularly known as the Kennedy-Kassebaum bill, it stipulated that the Health and Human Services Department would write the law's privacy-protecting regulations. Soon afterward, the Association for Electronic Health Care Transactions swung into action. "The latitude the original provision gave to HHS was just unlimited," Thomas Gilligan told the Center. "In the end, mat provision was deleted and the other one put in." The "other" provision relegates HHS to an advisory role and calls for a friendlier force—Congress—to write the rules.

In recent years, numerous pieces of legislation aimed at curbing various invasions of privacy have died in congressional committees. In 1991 and 1993, at the behest of various corporate interests, Congress killed legislation that would have regulated the clandestine videotaping and wiretapping of workers on their jobs.[17] In 1996, after lobbying by the direct-marketing industry, it killed a bill that would have restricted companies' gathering of information about children without their parents consent xhat same year, Congress deep-sixed legislation that would have restricted insurance companies' release of information about policyholders' claims and another bill that would have barred Internet-service providers and on-line services from releasing or selling information about customers without their permission. In 1997, legislators introduced bills to regulate the use of citizens' Social Security numbers for identification, a practice that makes it easier for thieves to obtain them and commit frauds, and to curtail the U.S. Postal Service's practice of selling patrons' names and addresses to direct-marketing firms; so far, none of those proposals has made it out of committee.[18]

Time and time again, Congress has put big-money corporate interests ahead of the basic privacy interests of the American people.

When Congress does decide to regulate, the bill that finally becomes law is often a weakened version, containing loopholes inserted at the request of privacy-invading interests. After the much-publicized 1989 slaying of actress Rebecca Schaeffer, who was killed by a stalker who had obtained her home address from driver-registration records, Congress passed the Driver's Privacy Protection Act. Although the law is supposed to prevent the disclosure of such information, it allows state motor-vehicle bureaus to continue selling addresses and other data, as long as they allow drivers a chance to "opt out" of having their data released. Additionally, the law contains exemptions that allow states to sell records to a wide range of businesses—private investiga-

tors, trucking companies, credit agencies, insurers, and direct-marketing firms. Only ordinary citizens are blocked from requesting information.[19]

Worst of all, in a number of instances over the years, Congress has turned a privacy bill into a Trojan Horse for corporate privacy invaders, inserting amendments that actually make it easier for companies to spy on their customers and workers. When Congress passed an anti-wiretapping law in 1968, at the request of industry its definition of an interception device did not include a switchboard or other equipment on the premises of a business, so that companies could continue their practice of listening in on employees' calls.[20] Eighteen years later, when Congress passed the Electronic Communications Privacy Act to extend anti-wiretapping protection to e-mail and other new technologies, it again left a legal loophole allowing companies to eavesdrop on employees' electronic communications as long as the interception was made in the ordinary course of business.[21]

In 1996, Congress passed the Consumer Credit Reporting Act, which compelled credit agencies to take quicker action to correct erroneous information on credit reports and required subjects' permission before bureaus could furnish credit reports to employers. But the same law also contained a loophole—sought by the financial-services industry—that allows a company to share information from credit reports and insurance applications with other companies, as long as all the firms are part of the same parent conglomerate. The "affiliate sharing" loophole gives those companies an exemption to use information on, say, a credit-card application for purposes that have nothing to do with the granting of credit—purposes that supposedly are banned by law. If that weren't enough, Congress preserved another loophole in the law, allowing credit bureaus to continue to sell sensitive information from an individual's credit file—the "credit header" containing one's Social Security number, mother's maiden name, phone number and recent addresses, and other key identifying information—to anyone who wants it. Thanks to Congress, that information can now be easily purchased over the Internet, not just by businesses but by abusive husbands who want to track down their fleeing spouses or by criminals who want to take over consumers' identities to commit credit-card fraud.[22]

One reason Congress may be reluctant to protect consumer privacy is that it would mean placing restrictions on a wide range of businesses, many of which are generous contributors to politicians. The financial-services industry, for instance—banks, insurance companies, and finance and credit firms—gave $32 million to congressional candidates during the 1995-96 election

cycle, according to the Center for Responsive Politics. Hospitals, health-maintenance organizations, and pharmaceutical companies gave $13 million. One of the biggest "soft money" contributors in the 1997-98 cycle has been Rick Rozar, the founder of CDB Infotek of Santa Ana, California, who gave $100,000 to the Republican National Committee in October 1997.[23] CDB is an information broker that compiles and sells information on individuals, largely from government records;[24] for $7, according to its Web site, the company will provide business subscribers with a person's full name; date of birth; and Social Security, telephone, and driver's license numbers; as well as the names of possible relatives, property holdings, tax liens, and bankruptcies.[25]

On occasion, Congress has taken decisive action to protect privacy—its own. Back in 1967, legislators were careful to exempt themselves from the provisions of the Freedom of Information Act. In 1982, Irwin Arieff, then a reporter for *Congressional Quarterly,* filed a Freedom of Information Act request seeking the names and amounts of prescription drugs supplied by the National Naval Medical Center to the Office of Attending Physician of Congress.[26] Senator Howard Baker, a Republican from Tennessee, responded angrily on the Senate floor. "The disclosure which is sought remains an intolerable invasion of personal privacy," Baker railed, even though Arieff had sought information on the drugs, not identification of the lawmakers to whom they had been prescribed. "[T]he interest of patients in the absolute confidentiality of medical information is paramount."[27] What Baker didn't mention was that "absolute confidentiality" applied only to patients who happened to be Members of Congress; lawmakers had rejected a 1980 bill that would have applied such privacy protections to the health-care records of ordinary citizens.[28]

In December 1996, a cellular-telephone call by Representative John Boehner, a Republican from Ohio, to House Speaker Newt Gingrich was eavesdropped upon and the contents revealed to newspapers. Six weeks later, the House Commerce Subcommittee on Telecommunications, Trade, and Consumer Protection called the cellular industry on the carpet to lambaste it about the lack of cell-phone privacy, angrily demanding enforcement of federal laws to protect electronic communications. "This hearing is not about that particular case," insisted Republican Billy Tauzin of Louisiana, the subcommittee's chairman[29]—even though the panel had up until then shown little interest in the problem of cellular eavesdropping, which had been reported widely in the news media for several years. Subsequently, in March 1998, the House passed a bill explicitly extending the prohibition against eavesdropping to digital telephones as well as analog models and making it illegal to listen in

on a conversation, whether or not the eavesdropper divulges the content to anyone.[30]

Now new threats to the ordinary citizen's privacy are emerging, in part thanks to Congress. In May 1998, the House narrowly passed a bill that lifts Depression-era barriers separating banking, securities, and insurance; that move potentially could allow consumers' personal data to be spread even more freely. And in the strangest irony, in recent years Congress has moved toward creating the same sort of federal data clearinghouse that frightened its predecessors of the 1960s. In 1996, as part of Republican welfare-reform legislation, Congress created a National Directory of New Hires, a computerized database that will track every worker in the nation; the information, including data on law-abiding citizens, is accessible by multiple federal agencies—and, as privacy advocates warn, will be all the more vulnerable to abuse. In the meantime, with Congress's acquiescence, personal information is already being used in disturbing ways.

"We don't know how much information is out there, or how it's being used," Senator Dianne Feinstein, a Democrat from California, warned in 1997, after an aide showed her a printout of her Social Security number, which had been obtained from the Internet. "Our private lives are becoming commodities with tremendous value in the marketplace."[31]

CHAPTER 1

The Invaders

In 1962, at the annual meeting of the American Association for the Advancement of Science, Richard Hamming, a computer scientist for Bell Laboratories, delivered a speech with an alarming message. Advances in electronic data-processing technology, he said, were rapidly enabling government and business to accumulate and easily access vast amounts of information on individuals: Social Security data, employment histories, medical records, insurance claims, even airline records. With the use of computers, Hamming warned, such data could now be electronically pooled, analyzed, and put to uses for which it had not been collected. "How can we be sure that this information will not be used against a person?" he asked.[1]

To some, Hamming's gloomy prediction might have seemed like something from a science-fiction B-movie or the ravings of a conspiracy theorist. But just a few years later, in 1966, the Johnson Administration's Bureau of the Budget (the predecessor of the Office of Management and Budget) asked Congress for money to establish a National Data Center that would collect information about Americans accumulated by twenty federal departments and agencies and put it all in one centralized mainframe computer. Under the plan, data on an individual would have been merged into a single file, including such information as the grades a person had received in school; a history of his or her military service, income over the years, and credit ratings; and even a subject's personality traits. At congressional hearings on the proposal, lawmakers responded with alarm. "The thought of [the records] neatly bundled together into one compact package is appalling," Representative Cornelius Gallagher, a Democrat from New Jersey, proclaimed.[2]

After a public outcry, the plan for the mammoth central database was abandoned[3]—although, six years later, the General Services Administration tried to

revive the idea with FEDNET, a proposed $200 million system that would have linked all of the federal government's computers and their data into a single network. After a GSA employee tipped off some Capitol Hill lawmakers to the system's privacy-invading potential, Congress eliminated funding for it.[4] Around the same time, public outrage was further stirred by revelations that federal law-enforcement and intelligence agencies had compiled massive databases on hundreds of thousands of citizens because of their political views. In 1970, a former military intelligence operative, Richard Kasson, revealed in an interview with NBC News that he had helped compile a card file on 5,000 to 8,000 residents of the St. Paul, Minnesota, area who had opposed the Vietnam war. As a probe by the Senate Judiciary Subcommittee on Constitutional Rights later disclosed, the effort was just one part of a sprawling government surveillance project, in which dossiers on hundreds of thousands of U.S. citizens were compiled by the Military Intelligence Command headquarters at Fort Holabird, Maryland.[5]

In the early 1970s, the Senate Judiciary Subcommittee on Constitutional Rights studied 858 databases of personal information about citizens compiled by various federal departments and agencies. Fewer than a third of the government agencies had notified citizens that they were collecting information about them.

But as congressional investigators determined, routine invasions of privacy at the hands of the government went even further. In the early 1970s, the Senate Judiciary Subcommittee on Constitutional Rights studied 858 databases of personal information about citizens compiled by various federal departments and agencies. Fewer than a third of the government agencies had notified citizens that they were collecting information about them, and three-fourths of them relied primarily on records obtained from other federal databases, so that information about citizens was circulated throughout the federal government with little effort to check its accuracy.[6]

Congress first responded to the government's privacy invasions by passing the Freedom of Information Act in 1967, giving citizens the right to petition federal departments and agencies for certain types of information.[7] In 1974, Congress passed the Privacy Act, which placed limits on the federal government's collection, use, and dissemination of information. The law gave citizens a right to know what files government agencies had compiled about them and how the information was used, as well as the right to examine their files and to correct mistakes.[8]

That same year, Congress passed the Family Educational Rights and Privacy Act, which limited the types of information that schools could gather about students, placed restrictions on the release of those records, and gave students and parents an opportunity to examine the records.[9] In 1976, it passed the Tax Reform Act, which restricted the Internal Revenue Service in disclosing information from federal tax returns.[10]

The federal government was far from alone, however, in its drive to gather personal data on citizens. By the 1960s, thousands of credit bureaus existed around the country to verify consumers' financial fitness for merchants; one giant in the industry, the Atlanta-based Consumer Credit Company, maintained files on 42 million Americans.[11] Insurance companies employed investigative firms to dig into the backgrounds of applicants, interviewing neighbors, for example, to determine whether a person's lifestyle or personal habits might make him or her an unacceptable risk.[12] "Insurance companies wanted to know everything about you," Kenneth McLean, who was an aide to former Senator William Proxmire, a Democrat from Wisconsin, told the Center. "Whether you drank or hung out with people of disreputable character, whether you were a neat housekeeper, and so on. Basically, they'd hire guys to go out and talk to your neighbors. But they didn't want to pay a lot of money for the information, so it wasn't always accurate."[13] Medical-records bureaus compiled data on millions of Americans without their knowledge; agents for one outfit, Factual Service Bureau, Inc., allegedly purloined patients' confidential records by posing as nurses and priests and by burglarizing hospital record sections at night.[14]

Some employers administered lie-detector tests, in which they asked a series of trick questions intended to ferret out applicants' sexual orientation. ("If you really throw the homo question to them directly while the machine is on, the needles really jump," one polygraph operator explained to Vance Packard as he was researching his book *The Naked Society.*[15]) Others hired private investigative firms such as Wackenhut Corporation, which maintained a vast database of files on individuals who had been involved in "subversive" activities; some of the information came from Barz Lag, a retired naval officer who monitored congressional hearings and other government proceedings in search of derogatory information that could be used for blacklisting purposes.[16]

The amount of grief that such large-scale invasions of privacy once caused for Americans is difficult to fully appreciate today. Consumers were routinely denied credit or insurance coverage, for example, for reasons that had nothing

to do with their worthiness as risks. In 1972, a New Jersey woman's automobile insurance was cancelled by one insurer when a credit report revealed she was living with a man out of wedlock.[17] In 1971, another auto-insurance company cancelled the policy of James Millstone, a newly hired editor at the *St. Louis Post-Dispatch,* on the basis of a private investigation firm's report that claimed Millstone was a "hippy type" who was "strongly suspected of being a drug user by neighbors." (A successful lawsuit by Millstone later revealed that the investigator in his case, who was required to produce seventy to eighty reports a week, had fabricated the information.)[18]

Thanks to the efforts of such civil-libertarians as Proxmire and the late Senator Sam Ervin, a Democrat from North Carolina, lawmakers began to take action to protect Americans from invasions of privacy by the private sector as well. In 1971, Congress passed Proxmire's Fair Credit Reporting Act, which regulated the activities of credit bureaus. The legislation allowed citizens access to information compiled about them by credit firms and gave them the right to challenge and correct misinformation.[19]

Nevertheless, as even its backers quickly realized, the new law was fairly weak. For starters, it applied only to credit bureaus, not to banks and other furnishers of information. It still allowed credit bureaus to sell credit reports to any business with a "credit, insurance, employment, or other business need" without first asking the subject's permission.[20] Consumers were entitled to learn what information was in their report, but they weren't permitted to examine or copy the complete file itself, so they had to take the bureau's word for it.[21] Two years after the passage of the law, Sheldon Feldman, the assistant director of the Federal Trade Commission, told a House hearing, "We have concluded that, as enacted, the Fair Credit Reporting Act has not fulfilled its stated goals."[22] That year, Senator Proxmire proposed amendments that would have allowed consumers to see their entire credit-bureau files and to be sent a copy of any negative information provided by a creditor, and would have required a consumer's approval each time the credit report was released to another party.[23] Thanks to a pull-out-the-stops lobbying effort by the financial-services industry, Proxmire was unsuccessful.[24]

"It was quite difficult to get though Congress," Proxmire aide Kenneth McLean recalled. "It's always difficult to enact new consumer regulation. The credit-bureau industry at that time was far different than it is today. Instead of three big companies, it was more of a mom-and-pop business. There were thousands of bureaus all over the country, and they had grassroots contact with Members of Congress. We wanted to do more on privacy. We could never

really convince members of the [Senate Banking] Committee that privacy was a big deal."[25]

In 1974, Congress created a Privacy Protection Study Commission to investigate intrusions of citizens' privacy by business; David Linowes, a professor of economics and public policy at the University of Illinois, headed the inquiry. In 1977, after more than two years of fact-finding, the commission issued a report that recommended sweeping changes to protect privacy in the private sector. The commission urged tighter controls on how the credit and insurance industries gathered and used personal information, and it recommended that medical records be released on a strict "need-to-know basis" to anyone other than the patient; it also called on employers to voluntarily adopt policies that would restrict the gathering and use of information about employees and give employees access to files kept on them.[26] Subsequently, eleven bills based on the commission's recommendations were introduced in the House by Barry Goldwater, Jr., a Republican from California (and the son of the 1964 GOP presidential nominee), and Edward Koch, a Democrat from New York, both of whom had also been members of the Privacy Commission, and in the Senate by Birch Bayh, a Democrat from Indiana. (One bill, for example, would have restricted the use of Social Security numbers for identification purposes.)[27] In addition, the commission proposed the creation of an independent, permanent agency to regulate business and government in an effort to ensure that citizens' privacy was protected.[28]

By the 1960s, thousands of credit bureaus existed around the country to verify consumers' financial fitness for merchants; one giant in the industry, the Atlanta-based Consumer Credit Company, maintained files on 42 million Americans.

Public sentiment was strongly behind such moves. In 1979, a poll by Louis Harris and Associates showed that 64 percent of those surveyed were concerned about threats to their privacy, up from 47 percent the previous year. Even in the era of Watergate, more Americans were worried about credit bureaus seeking personal information (44 percent) than were worried about the activities of the IRS (37 percent) or the CIA (34 percent).[29] A few of the Privacy Commission's recommendations ultimately became law, but some measures—such as restrictions on the use of polygraphs—took more than a decade to enact. For the most part, the commission's vision of extending the Privacy Act's restraints on government data-gathering to the private sector never came to pass.

What happened? Congress backed away from the idea of creating overarching protection for Americans' privacy. Instead, over the next decade it passed a handful of laws to protect privacy in a few narrow areas: the Cable Communications Policy Act of 1984, which made subscribers' cable-TV records confidential; the Electronic Communications Privacy Act of 1986, which made it illegal to eavesdrop on voice-mail messages or to read another person's electronic mail; and the Video Privacy Protection Act of 1988, which barred disclosure of video-rental records.[30] Congress pondered extending protection to library lending records as well but backed off at the request of the FBI, which said that it wanted to be able to continue monitoring what books foreign nationals check out from technical libraries.[31] In part, that reticence was testimony to the influence of industries that relied on Americans' personal information.

As a result, over the next two decades, the corporate gathering of personal data grew into a bigger, even more pervasive presence in American society.

CHAPTER 2

No Limit

Not long after the Fair Credit Reporting Act was passed in 1971, privacy advocates realized that it was more loophole than law. During the 1980s, as the credit-bureau industry underwent tremendous changes, the need for protection grew more acute. With the economy booming, banks and retailers were eager to extend credit, so that by 1985, seven out of ten Americans were using credit cards or other forms of credit and some 700 million accounts were active across the country.[1] At the same time, the credit-bureau business underwent consolidation, as three major bureaus—British-based Experian Information Systems, Inc. (formed when TRW Information Systems & Services merged with CCN Group); Atlanta-based Equifax, Inc.; and Chicago-based Trans Union Corporation—merged information from thousands of smaller local bureaus into their databases.[2] (Between 1981 and 1985, Equifax's operating revenues increased by 73 percent, from $379 million to $564 million.[3]) It became possible, with a few keystrokes, to amass more and more data about individual consumers all over the United States.[4] Technological advances allowed the big three to analyze information in ever-more sophisticated ways—with computer programs, for example, that analyzed consumers' finances and predicted which of them were likely to become overextended and file for bankruptcy.[5] Credit bureaus began to use their mountains of data in new ways, utilizing the information on consumers' finances and purchasing patterns to create lists of potential customers and sell them to businesses for "target-marketing" purposes.[6]

But there was a darker side to that success story, as far as Americans' privacy rights were concerned. "As a private citizen as well as a direct marketer, I'm increasingly disturbed by the companies that collect information for one purpose and then use it for another without the individual's consent,"

Jonathan Linen, the president of American Express Direct Marketing Group, acknowledged in 1988. "It's one thing for an organization to use its customer-detailed information for its own marketing purposes. It's entirely another to sell that information to anyone who wants to buy it."[7]

If consumers' privacy is defined as the right to have some control over the collection and use of their personal information, it also includes the right not to be damaged by the spread of personal information that happens to be wrong. As the credit-bureau business grew bigger, accumulating and selling increasing amounts of data on Americans, consumers began to complain not only that the scrutiny was invasive, but also that their files were rife with inaccuracies. A 1989 computer analysis of 4,500 credit reports by Consolidated Information Services, Inc., a mortgage broker, found errors in 22.5 percent of the reports, and a follow-up study in which a smaller sample of consumers was contacted revealed errors in 46 percent.[8] A Los Angeles man named Paul Rosenzweig, for example, wondered why he found it so difficult to obtain an automobile loan or rent an apartment; ultimately, he discovered that the bad debts of two other men named Rosenzweig had been merged into his credit report. It took him months to convince credit bureaus that there had been a mistake. "I have spent every moment of my free time trying to fix this mistake, and it has made my life a living hell," he wrote to the California Public Interest Research Group, a consumer advocacy organization, in 1990.[9]

A 1989 computer analysis of 4,500 credit reports by Consolidated Information Services, Inc., a mortgage broker found errors in 22.5 percent of the reports, and a follow-up study in which a smaller sample of consumers was contacted revealed errors in 46 percent.

In addition, a new problem emerged. With sensitive identifying data such as Social Security numbers being circulated more widely than ever, thieves began to victimize consumers by stealing their identities and using them to obtain credit. By 1990, Robert Ellis Smith, the editor of the publication *Privacy Journal*, had documented more than 500 such cases across the nation.[10] Victims' problems were compounded by the fact that once their credit history had been filled with bad debts by an identity thief, it was maddeningly difficult to get their names cleared; credit bureaus would remove the entries only at the request of creditors, whom the victims had to contact one by one and persuade to cooperate.[11] If the creditors chose not to be bothered and reconfirmed the information with the credit bureau, the victims had little recourse.[12]

As a result, consumer advocates began to call for an updating of the Fair Credit Reporting Act to give the public more protection. In 1990, Representative Richard Lehman, a Democrat from California, introduced a bill to toughen the law; other proposals were introduced by Representatives Charles Schumer, a Democrat from New York, and Matthew Rinaldo, a Republican from New Jersey. Lehman wanted to compel credit bureaus to reinvestigate consumers' complaints of inaccuracies within thirty days, rather than the unspecified "reasonable" amount of time under the existing law; Rinaldo wanted to require credit bureaus to track down reports that had been issued with incorrect information and correct them. Lehman wanted consumers to be notified and given an opportunity to "opt out" of having information from their credit files sold to marketers, while Schumer and Rinaldo aimed to bar such releases of data outright.[13] In the Senate, Alan Cranston, a Democrat from California, introduced similar legislation.[14]

Those bills were met with fierce resistance—not just by the credit bureaus but also by the banking and financial-services industry, which both contributed personal information to and utilized credit reports. At a hearing on the three House bills before the Banking Subcommittee on Consumer Affairs and Coinage in June 1990, chaired by Lehman, representatives of the banking, retail, and credit industries argued against updating the Fair Credit Reporting Act. One opponent was the American Financial Services Association, whose member companies held one-fourth of the nation's total outstanding consumer debt. "There seems to be no public unhappiness with the current system and no need for significant legislative change," Kenneth Hoerr, the president of USA Financial Services, speaking on behalf of AFSA, told members of the subcommittee.[15] (In fact, inaccurate credit reports had become the number-one source of complaints to the Federal Trade Commission.[16])

The industry managed to bottle up Lehman's bill that year,[17] but in the spring of 1991, he and other lawmakers tried again, introducing a half-dozen different bills to beef up the Fair Credit Reporting Act.[18] Despite small differences, the bills essentially contained the same sorts of protections—restrictions on the use of consumers' personal data without their permission, the requirement that bureaus provide consumers with free copies of their reports, quicker turnaround on correcting disputed information, and pressure on creditors to correct wrong information that they'd submitted to credit-bureau files.[19] In May 1991, Consumers Union of the United States published an expose in its magazine, *Consumer Reports*, showing that half of 57 credit reports contained errors, and one-fifth had a major inaccuracy that could

have adversely affected a credit application. "Congress has got to get the credit-reporting industry to clean up the files," Michelle Meier, Consumers Union's counsel for government affairs, said at a press conference.[20] The United States Public Interest Group followed up with a study showing that it took six months or more to have errors in consumers' reports corrected.[21] Another incident that year drove home the inaccuracy problem even more dramatically: Every property owner in Norwich, Vermont, was labeled a deadbeat when TRW mistakenly recorded tax bills as tax liens.[22]

Even so, at hearings held by Lehman in June, R. Harold Owens, a finance-industry executive appearing on behalf of AFSA, argued that the case for changing the law hadn't been made, and he urged Congress to commission a study before it approved any legislation.[23] The credit bureaus insisted that it simply wasn't possible to eliminate errors from the credit files. "As desirable as it may be to have no incomplete or inaccurate information, this Utopian state cannot be achieved in today's marketplace," Walter Kurth, the president of Associated Credit Bureaus, said.[24]

By that fall, Representative Esteban Torres, a Democrat from California and the chairman of the Consumer Affairs and Coinage Subcommittee, worked to meld the bills into a single piece of legislation.[25] Senator Richard Bryan, a Democrat from Nevada, introduced a companion bill in the Senate.[26] TRW, which by then was under legal siege by the FTC and attorneys general in nineteen states,[27] and the rest of the credit-bureau industry decided to throw in the towel and support the legislation, rather than facing the possibility of even more sweeping legislation down the road.[28] At an October 1991 hearing on the Bryan bill, in fact, Equifax and TRW both testified in favor of the bill.[29] By January 1992, consumer advocate Edmund Mierzwinski was confidently predicting that "the train is moving down the tracks."[30]

But supporters of stronger privacy protection for consumers underestimated the might of the banking and financial-services industry. At the Senate hearing, the phalanx that was aligned against tougher consumer privacy protections included AFSA, the Consumer Bankers Association, the American Bankers Association, the National Retail Federation, Visa, and MasterCard.[31] In the House, banking lobbyists worked the Democratic side in an effort to kill the bill.[32] In March, Torres's subcommittee voted to jettison the requirement that bureaus provide a free report, and approved another amendment by Representatives Chalmers Wylie, a Republican from Ohio, and Doug Barnard, a Democrat from Georgia, to make the proposed law pre-empt any existing credit-reporting laws on states' books. The latter change, reportedly inserted

at the behest of lobbyists,[33] was a favor on behalf of AFSA and other industry groups.[34] Nineteen states, including California and Massachusetts, had already enacted statutes that were stronger than the proposal Torres had designed to get through Congress, so his bill would serve to weaken, rather than strengthen, privacy protection in those places.[35] (Barnard's amendment was vigorously defended in the media by his top banking aide, Jeff Tassey, who claimed that the pre-emption provision was needed to bring clarity to the diversity of laws that many states had been passing.[36] Just over a year later, Tassey became a lobbyist for and senior vice president of AFSA.)

This pre-emption clause is "a fatal flaw . . . a poison pill that will kill this bill if an antidote is not administered," Torres complained.[37] But his words did little good. The bill went to the House Banking Committee, where conservative Democrats aligned with Republicans to block Torres from stripping away the pre-emption provision, 27 to 24.[38] Democrat Henry Gonzalez of Texas, the chairman of the committee, also railed against the change. "We must not forget that we have a massive lobbying force arrayed against us—the big credit-card companies, the national retailers, the banks, finance-company conglomerates, and the credit-reporting cartel," Gonzalez told a reporter for Gannett News Service.[39] In September, after Torres lost a floor vote to remove the pre-emption amendment to the House bill on credit reporting, 203 to 207, he persuaded the House to withdraw the bill from consideration.[40]

Supporters of stronger privacy protection for consumers underestimated the might of the banking and financial-services industry. At a 1992 Senate hearing, the phalanx that was aligned against tougher consumer privacy protections included AFSA, the Consumer Bankers Association, the American Bankers Association, the National Retail Federation, Visa, and MasterCard.

In the spring of 1993, the reformers gave it another try. Torres reintroduced his bill to toughen the Fair Credit Reporting Act, this time without the pre-emption amendment;[41] in the Senate, Bryan and Christopher Bond, a Republican from Missouri, introduced their own version of the legislation. That fall, Bryan tried to negotiate with the banking lobbyists to come up with legislation that the industry could accept, but to no avail.[42] A similar battle took place in the House Banking Committee in February 1994, where Representative Joseph Kennedy, a Democrat from Massachusetts, the new chairman of the Consumer Affairs Subcommittee, struggled to fend off amendments offered on behalf of the banking

industry to weaken the bill. Kennedy and Gonzalez, in an effort to make peace with banking-industry lobbyists, agreed to insert an amendment that shielded banks from legal liability in situations where they submitted incorrect data on consumers to credit agencies. Even so, the industry and its supporters weren't satisfied. Representative Richard Baker, a Republican from Louisiana, summed up their stance: "Access to credit is not part of the Bill of Rights. It is something that the free market has worked out."[43]

Senator Phil Gramm, a Republican from Texas, had been one of only ten Senators to vote against strengthening the Fair Credit Reporting Act. As the Senate was racing to finish business before the end of the session, Gramm employed a procedural maneuver known as a "hold" to essentially kill the bill.

Ultimately, Kennedy and Gonzalez prevailed in committee, 29 to 20." To win passage by the House in June, however, they had to accept an industry-supported amendment that pre-empted states from passing tougher laws for an eight-year period. ("Federal law usually sets a floor, not a ceiling, for consumer protection," Kennedy noted with disappointment.[45])

The Senate had passed its own version of the legislation as well, and that fall Senate and House staffers worked out a compromise version of the bill But if privacy advocates figured they finally had achieved victory, they figured a bit too soon. Senator Phil Gramm, a Republican from Texas, had been one of only ten Senators to vote against strengthening FCRA. In October, as the Senate was racing to finish business before the end of the session, Gramm employed a procedural maneuver known as a "hold" to essentially kill the bill. A spokesman for Gramm later explained that the Senator opposed the provision limiting credit bureaus to charging a consumer $3 for a copy of his or her credit report, because it would be too expensive for bureaus to comply. It seemed like an odd stance, since Associated Credit Bureaus, the industry lobby, had already said it could live with the $3 fee. (TRW already was offering consumers one copy a year at no charge.)[46] *The Wall Street Journal,* in a subsequent analysis of Gramm's political fund-raising, suggested another possible motivation: The bill had been opposed by Texas-based retailer J.C. Penney, whose political action committee had contributed $11,000 to Gramm's Senate campaigns. Gramm, for his part, insisted it was "outrageous" to suggest such a connection.[47] But in the year and half after Gramm's action, J.C. Penney's PAC gave him another $9,000, more than it gave any other Member of Congress.[48]

In 1996, consumer-privacy advocates gave it one more try. But by then, with a Republican-controlled Congress that was sympathetic to business's calls for deregulation, the banking and financial-services lobby was in a position to call the shots. "Updating the Fair Credit Reporting Act had taken six years, because industry had so much clout," Evan Hendricks, the publisher of *Privacy Times,* a journal on privacy issues, told the Center. "Finally, the bill had to be watered down to get it through."[49]

Not surprisingly, the compromise bill that made its way through Congress in late 1996 contained the eight-year pre-emption of tougher state laws sought by the industry, and it limited the liability of banks and other creditors that provided incorrect information. But more important, the industry also took the opportunity to slip into the reform legislation two other items that actually *reduced* consumers' privacy. One was a provision allowing a practice known as "affiliate sharing." A company that obtained a consumer's personal information—say, from an application for a credit card or a car loan—now could share it with other companies, as long as they were all subsidiaries of the same parent company, without the consumer's permission or government regulation.[50]

Just as significant was a part of the old law that Congress declined to toughen. The original Fair Credit Reporting Act contained an apparent loophole that allowed credit bureaus to peel certain key identifying information about consumers—the so-called "credit header" that includes a person's name, Social Security number, mother's maiden name, phone number, and recent addresses—and sell the information to whomever they wanted, without restriction. During the 1990s, a flourishing trade in the sale of such information had developed, and officials of the Federal Trade Commission worried that it made consumers vulnerable to thieves who wanted to steal their identities and tap into their credit. In a September 20, 1996, letter to Senator Bryan, Robert Pitofsky, the chairman of the FTC, recommended closing the loophole and expressly restricting the sale of credit headers, noting that the potential abuses "outweigh the limited legitimate uses of this information for locating individuals."[51] But Congress declined to follow that advice, and the amended version of FCRA enacted that fall still contained the loophole. Today, such sensitive information—which can be used to locate a battered wife in hiding or to impersonate an individual and gain access to his or her credit—can be purchased over the Internet from a variety of information brokers.[52]

"In order to win the accuracy provisions we wanted, we had to eat some truly outrageous ones—the affiliate sharing and failure to close the credit header," Ed Mierzwinski of U.S. PIRG, who lobbied Congress on the bill, said

in an interview with the Center.[53] Since then, Senator Dianne Feinstein, a Democrat from California, has introduced a bill to close the credit-header loophole,[54] but she'll have long odds against intense industry opposition.[55] "Basically, the history of privacy legislation is a history of industry dominance, of legislation that's been controlled by industry," Mierzwinski told the Center. "And that isn't going to be easy to change."[56]

CHAPTER 3

An Unlocked Door

The letters "RPR" are seared in Vertis Ellis's mind. She remembers them as clearly as the day she opened the envelope containing her workplace medical records in 1994. There, branded at the top of one form was the three-letter medical code designating that a syphilis test had been done on her. But Ellis had never authorized such a test.[1]

If Ellis was shocked to see the code on her form, she was floored when she discovered that her employer, the Ernest Orlando Lawrence Berkeley National Laboratory at the University of California-Berkeley, the country's oldest national research laboratory, had also tested her for the sickle-cell gene and for pregnancy. And not just once, but at each of her six company exams during the previous 29 years. She had never received the results of any of the tests.

"I felt so violated," Ellis, an administrative assistant at the lab, told a reporter in 1997. "I thought, oh my God, do they think all black women are nasty and sleep around?"[2]

It turned out that thousands of employees of the lab were tested for these traits without their knowledge or consent and, what's more, that much of the testing was done under the guidance and approval of the Energy Department, which funds the facility. Workers say they had thought the exams were for more routine health information such as high cholesterol and other problems. But they now claim that all new hires were tested for syphilis and that African Americans were screened for the sickle-cell trait and women for pregnancy.[3] According to a June 1997 article in *U.S. News & World Report,* lab documents show that black and Latino employees were retested for syphilis during periodic exams and that blacks continued to be tested for sickle cell, despite the fact that the results of one sickle-cell test don't differ from those of subsequent ones on the same person. Women were also routinely tested for pregnancy.

Seven of the workers filed a class-action lawsuit in September 1995, charging that the lab had invaded their privacy and violated their civil rights.[4] They also claimed that repeated testing had not been performed on the blood samples of white male employees, with one exception: A white man married to a black woman was repeatedly screened for syphilis.

More than a fourth of the respondents in 1993 poll said that health information about them had been improperly disclosed at one time or another. A 1996 survey found that 35 percent of the Fortune 500 companies surveyed used employees' medical records in making employment-related decisions.

The lab argues that it is not liable because employees had consented to the physical exams.[5] In January 1996, a federal district judge in San Francisco agreed with the lab and threw out the case.[6] The workers appealed the decision, and in February 1998 the U.S. Court of Appeals for the Ninth Circuit in San Francisco unanimously ruled that such medical exams performed without the knowledge or consent of workers were unconstitutional.[7] According to laboratory spokesperson Lynn Yarns, the parties are negotiating a settlement.[8]

How long had the lab been conducting these unauthorized tests on its employees?

"Decades," Vicki Laden, the lawyer who is representing the workers, told the Center. "The oldest record that we had was from 1968, indicating that someone had been tested for sickle cell, one of the main plaintiffs. There was no knowledge on the part of the employees." Laden said that some of the plaintiffs didn't even work at the lab itself. "The workers, who I represent, were actually clerical workers and administrative workers, so there wasn't even an arguable explanation that they were exposed to anything—not that that would have been persuasive in this case anyway," she told the Center. "Some of them worked in office buildings in downtown Berkeley."

"Now they'll think twice before running these embarrassing types of tests on employees," Ellis said upon learning of the appeals-court decision.[9]

Such unauthorized tests are only one aspect of the increasingly pervasive invasions of privacy in the medical realm. At a hearing of the Senate Labor and Human Resources Committee in February 1998, legislators learned about the case of Betty Jane Gass, who had been fired from her job as an occupational-health nurse for "insubordination," because she had objected when the com-

pany's human-resources manager wanted to examine the records of employees' physical examinations. The lawmakers were also told of an Orlando woman who had gone to her doctor for some routine tests; a few weeks later, the woman received a letter from a pharmaceutical company that had obtained access to her medical data and wanted her to try its new cholesterol medication. And they were reminded about the infamous cases of the late tennis star Arthur Ashe, whose HIV status had been leaked to a newspaper by a hospital worker, and Representative Nydia Velazquez, a Democrat from New York, whose psychiatric records detailing a suicide attempt had been disclosed and published on the eve of an election.[10]

Those stories, privacy advocates argue, dramatized the need for a federal law to protect the privacy of personal medical information and of health-care records, which contain some of the most intimate and sensitive information about an individual—data that may reveal everything from sexual orientation to genetic predisposition to various diseases. Since the time of Hippocrates, doctors have sworn to keep what they learn about a patient to themselves. But in the modern world, an oath alone is no longer sufficient to prevent that information from being distributed far and wide in electronic databases and perused by scores of people—hospital employees, insurance companies, pharmaceutical firms, medical researchers, employers, and even police.[11] Often, the only ones who can't get access to the intimate information are the patients; only 28 states require that patients be allowed to see their own records.[12]

More than a fourth of the respondents in a 1993 poll by Louis Harris and Associates said that health information about them had been improperly disclosed at one time or another.[13] What's more, a 1996 survey by David Linowes, a professor at the University of Illinois, found that 35 percent of the Fortune 500 companies he surveyed used employees' medical records in making employment-related decisions.[14] In 1992, a worker for the Southeast Pennsylvania Transportation Authority was told by the agency's medical director that management had figured out he was being treated for HIV, after an administrator doing a cost-benefit review had obtained a list of employees who spent $100 or more a month on prescriptions and what drugs they were taking. Although the employer didn't do anything with that knowledge, the man said that he felt "consumed" by fear.[15]

Not surprisingly, the public overwhelmingly favors strict protection of its medical privacy; a 1996 poll for *Time* magazine and CNN showed that 87 percent of Americans thought they should be asked permission before any release of information from their health records.[16]

But except in states that have enacted their own laws to give a measure of protection, Americans don't have such medical privacy rights. To the contrary, in the era of managed care, there are plenty of horror stories about health insurers prying into consumers' most delicate secrets and then handling the information carelessly. The *Portland Press Herald* in Maine reported the case of a woman who called the 800 number of her husband's health-insurance provider to ask permission to see a psychiatrist in order to check the performance of a new medication she'd been prescribed. At the other end of the line, an employee began grilling her about her mental-health history—not only the dates she had received treatment at psychiatric hospitals but also the details of previous suicide attempts. "What would you have used to cut your wrists?" the insurance-company employee asked. "Would it be a switchblade? Would it be a butcher knife?"[17] In 1994, a Texas woman was horrified when her ex-husband told her that an insurance-company clerk had slipped him pages from her health-insurance records, including the record of treatment she'd received in the months after their divorce.[18]

Mark Hudson, a former employee of a health plan in Massachusetts, told *The New York Times* in 1996 of his own shock when, during a computer training class, he discovered that he could call up the records of any subscriber on his screen—including the records of his own psychiatric treatment and the amount and type of antidepressant medication he was taking. "I can tell you unequivocally that patient confidentiality is not eroding—it can't erode, because it's simply nonexistent," he warned.[19]

Even celebrities don't have the clout to protect their privacy. When country-music star Tammy Wynette checked into the University of Pittsburgh Medical Center in 1995, she registered under a pseudonym. That didn't keep the *National Enquirer* from reporting the details of her medical condition. The hospital investigated and found that an employee had peeked at the singer's file in the hospital's computer system.[20]

But such stories were all the more disturbing because Congress had been hearing about the problem of medical-records confidentiality for a quarter of a century. In 1973, John Gregg, a former FBI agent turned consumer advocate, told the Senate Banking Subcommittee on Consumer Credit that medical information on millions of Americans had been secretly gathered in data banks used by insurance companies. Gregg, who chastised the insurance industry for its "utter disregard for the personal privacy of human beings," charged that inaccuracies in the data often caused people to be unfairly turned down for health insurance.[21] And while patients were denied access to

their own information, it was available to a wide range of others—employers, credit bureaus, and government agencies.[22]

Gregg proposed amending the Fair Credit Reporting Act to give consumers the right to examine the records kept on them in medical databases. The proposal was opposed by the Medical Information Bureau, the Connecticut-based repository of medical data for 700 insurance companies. Its database contained entries on 11 million Americans—not just information about surgeries or illnesses but also codes for categories such as "sexual deviations" and "social maladjustment," as well as other codes indicating whether the person had a history of reckless driving or had dabbled in a hazardous sport such as skydiving.[23] Joseph Wilberding, the executive director of the Medical Information Bureau, told the subcommittee that the public didn't need to be told what was in their records. When pressed by Senator William Proxmire, a Democrat from Wisconsin, to explain why, Wilberding said that telling insurance applicants about the database "could possibly interfere with the sale of the policy by the salesman, and would result in more paperwork."[24]

An employee of a health plan in Massachusetts told of his shock when, during a computer training class, he discovered that he could call up the records of any subscriber on his screen—including the records of his own psychiatric treatment and the amount and type of antidepressant medication he was taking.

By the late 1970s, the Medical Information Bureau had relented somewhat, eliminating some of the more derogatory codes and requiring insurance companies to inform policyholders that their information went into the database. It also began to allow patients to request their files.[25] (It was not until 1995 that the FTC negotiated an agreement with the Medical Information Bureau under which insurance companies that rejected consumers' applications or charged them higher premiums would be required to disclose the fact that negative information in an MIB report had been a factor. In addtion, insurers were required to inform consumers that they could contact MIB to obtain a copy of their file and then request that any mistakes in the file be corrected.[26])

MIB vice president James Corbett told the Center for Public Integrity that the bureau provides 50,000 to 60,000 consumers with their coded files each year, and that although the organization resisted disclosure decades ago, it now sees openness as a plus. "I can't tell you how helpful it is to us," Corbett said. "[Seeing their files] helps consumers understand the reason why we keep these

records and allows us to correct records if there's a mistake, which benefits everyone."[27]

Even so, the public wanted more control over their information. In a January 1979 poll by Louis Harris and Associates, 91 percent of the respondents said that they should have a right to examine medical data collected about them.[28] That June, the Senate Governmental Affairs Committee heard witnesses describe the harm that these hidden records sometimes caused. One told of a thirteen-year-old orphan placed in a psychiatric hospital for six months when no other home could be found; years later, as an adult, he was denied a license to drive a taxi because a credit report noted his hospital stay. After a woman's incorrect diagnosis as an epileptic was entered into her file, she was unable to get insurance, even after obtaining a letter from her doctor explaining the mistake. Richard Beattie, counsel for the Department of Health, Education, and Welfare (now the Department of Health and Human Services), warned legislators that the problem was only getting worse. With the advent of large computer networks, he explained, "the maintenance, use, and disclosure of medical information has become a national business. . . . Information is transferred, with or without the patient's consent, from one state to another."[29]

The invasion of a Member of Congress's own privacy finally helped get lawmakers' attention. Representative Nydia Velazquez got an unpleasant wake-up call in 1992 when information about mental-health care she'd received following a 1991 suicide attempt was leaked to the *New York Post.*

Congress, however, didn't agree. In December 1980, the House rejected, by a 97-259 vote, a bill sponsored by Richardson Preyer, a Democrat from North Carolina, that would have given patients the right to inspect their health-care records and to control whether or not they were released to anyone else. The American Hospital Association and other opponents of the legislation had some help from an unlikely source: the FBI and government intelligence agencies.[30]

For the next decade, the issue of health-records privacy remained dormant in Congress, with the exception of an unsuccessful attempt in 1984 by Representative Ron Wyden, a Democrat from Oregon, to make it a federal crime for computer hackers to break into medical-records databases.[31] The invasion of a Member of Congress's own privacy finally helped get the attention of Congress. Democratic Representative Nydia Velazquez of New York got an unpleasant wake-up call in 1992 when information about mental-

health care she'd received following a 1991 suicide attempt was leaked to the *New York Post.* Velazquez still managed to win the election, but the disclosure "caused me a lot of pain, especially since my parents didn't know," Velazquez told *USA Today.*[32] Meanwhile, abuses of health records continued. A Midwestern banker who served on a state health commission checked the names of his bank's borrowers against the commission's list of cancer patients, and then called in the mortgages of those he found on both lists, according to an American Hospital Association report to the Health and Human Services Department.[33]

Not long afterward, in 1993, President Clinton unveiled his administration's plan for health-care reform, which envisioned the creation of a massive "Health Information System"—a nationwide network of health-records databases as a tool for increasing efficiency and controlling health-care costs. Privacy activists warned that without a federal law protecting patients' privacy, the potential for abuse was enormous.[34] That fall, in a poll by Louis Harris and Associates, 68 percent of the workers surveyed said that they were worried about a national health-care plan that would have a computerized data bank containing the medical records of all citizens, and 91 percent felt it was important to have a law specifying who would have access to those records.[35]

The Clinton Administration and the then-Democratic-controlled Congress rushed to find a solution, commissioning a study by the Office of Technology Assessment. Its report, issued in September 1993, concluded that the "patchwork of state and federal laws addressing the question of privacy in personal medical data is inadequate to guide the health-care industry with respect to obligations to protect the privacy of medical information in a computerized environment."[36] In April 1994, Representative Gary Condit, a Democrat from California, introduced legislation to set confidentiality rules for the handling of health-care information. Condit's proposal was incorporated into the Administration's health-care reform package and died along with it in 1994.[37]

The following year, Congress again pondered the question of health-records privacy. But by then, the game had begun to change. Although the Clinton plan was dead, private industry was moving to wire its own nationwide data network. For years, the health-care industry had opposed federal privacy legislation, preferring instead to deal with state regulation that, with few exceptions, was weak or nonexistent. But now, with computer networks and insurance plans and health-care companies whose business stretched across state lines, it was inconvenient to have a hodgepodge of different state regulations. In addition, some states were moving to pass stronger privacy

laws of their own.[38]

Thus, by 1995, health-care providers and insurers that for years had opposed federal privacy regulation now wanted it. In October 1995, Senator Robert Bennett, a Republican from Utah, introduced the Medical Records Confidentiality Act. Bennett's bill attracted wide bipartisan support; the twenty cosponsors included the Senate leadership of both parties as well as Democrat Carol Moseley-Braun of Illinois on the left and Republican Orrin Hatch of Utah on the right.[39] Based on model language from the American Health Information Management Association, a professional organization of health-data specialists,[40] it was favored by industry representatives as well, including many hospital and insurance groups, and even the American Hospital Association,[41] which had been a key opponent of privacy legislation fifteen years before.[42]

Bennett's bill contained some privacy milestones. It gave patients the right to read and obtain a copy of their records (although institutions were allowed to charge a fee) and to correct errors in their files. It also required hospitals and insurers to make their records policies available in writing and to keep track of any access to the records that was not related to treatment. It sought to restrict disclosure of information to the minimum amount necessary for the purpose, and it set criminal penalties for illegal disclosures.[43]

But, as privacy advocates and consumer activists pointed out, Bennett's bill sounded stronger than it was. The bill, they complained, contained numerous exceptions under which patients' information could be disclosed without their consent—to parties ranging from medical researchers to law-enforcement officials. It didn't restrict the number of people who could gain access to the information within the hospitals, insurance companies, and other authorized "trustees" of data, and it didn't give patients any power to limit what such trustees did with the information once they obtained it.[44] "The devil is in the details," complained Dr. Denise Nagel, the executive director of the Coalition for Patient Rights of New England. "As it's currently written, this bill allows greater, not less, access to medical records."[45]

And the bill contained a key provision eagerly sought by industry: It preempted state privacy laws. As privacy advocates noted, it would wipe out special rules that some states had enacted to protect particularly sensitive information,[46] such as a recently enacted Massachusetts statute that placed tight restrictions on the release of information about patients with HIV.

However well intentioned the legislation, even a supporter such as Lawrence Gostin, the director of law and public-health programs at Georgetown University, readily admitted to *The Boston Globe* that the primary bene-

ficiary was business. "To suggest to the public that this bill is a championing of the doctor-patient relationship and medical privacy is misrepresenting what's really going on," he said. "What this bill does is legitimize the development of these large health databases that are intended to hold vast amounts of medical information about individual Americans."[47]

According to disclosure records examined by the Center, 77 lobbyists—most of them representing health-care insurers, pharmaceutical manufacturers, and other industry groups—sought to influence Congress on the bill.[48] Even so, the vociferous criticism from privacy advocates helped erode some of the support for the bill in the Senate. Meanwhile, the industry still wasn't quite satisfied; it began pressing for language that made it clear that patient approval wasn't required each time information was handed over from one corporation to another. "We want that explicit," said Thomas Gilligan, a lobbyist for the Association for Electronic Health Care Transactions, a Washington-based organization representing the health-care industry.[49] As a result, that spring Bennett began reworking the bill.[50]

Senator Robert Bennett's Medical Records Confidentiality Act contained a key provision eagerly sought by industry: It pre-empted state privacy laws, wiping out special rules that some states had enacted to protect particularly sensitive information, such as a recently enacted Massachusetts statute that placed tight restrictions on the release of information about patients with HIV.

Another event increased the urgency of passing privacy protections. That summer, Congress passed the Health Insurance Portability and Accountability Act, sponsored by Senator Edward Kennedy, a Democrat from Massachusetts, and then-Senator Nancy Kassebaum, a Republican from Kansas. The Kennedy-Kassebaum bill ensured Americans access to health insurance, even if they changed or lost their jobs, and helped individuals with pre-existing conditions obtain coverage.[51] The legislation clearly benefited millions of Americans, but privacy advocates also noticed a downside: The new law called for the creation within eighteen months of a national computer network that would link health-care companies and allow them to exchange records.[52] The bill set criminal penalties for "wrongful disclosure of individually identifiable health information,"[53] but it didn't specify what that actually meant. Instead, Congress was given two years to write privacy regulations; at that point, if legislators hadn't been able to agree

upon rules, the Health and Human Services Department would establish them instead.[54]

Where did the privacy-threatening component of Kennedy-Kassebaum come from? Credit for that piece of the action goes to Representative David Hobson, a Republican from Ohio, who in 1993 began championing an idea euphemistically known as "administrative simplication" as part of his Health Information Modernization and Security Act—a way, in his words, to "help simplify and modernize health-care financial transactions by using high-tech communication networks." Hobson's idea was to assign a "unique personal identifier" to each American who receives any form of paid health care. Think of the identifier as a dog tag that you wear from cradle to grave. The tags would allow every provider in the health-care industry—doctors, hospitals, insurers, nursing homes, and the like—to employ one common number for billing.

In the fall of 1997 the Health and Human Services Department submitted proposed privacy regulations to Congress, describing a "national identification number" that would be assigned to each patient, making it possible to track the history of medical care received by the patient anywhere in the country. The more apt title should have been "Permitting New Access to Medical Records Without the Requirement of Patient Authorization," wrote one critic.

One oddity of the situation, however, was that Hobson's idea wasn't really Hobson's idea. He, in fact, didn't even draft the Health Information Modernization and Security Act. He presented it, championed it, and fought for it, but it was written by a coalition of private interests with billions of dollars at stake, including the American Health Information Management Association, the American Hospital Association, the American Medical Association, the Association for Electronic Health Care Transactions, Blue Cross and Blue Shield Association, Electronic Data Systems, International Business Machines Corporation, the Working Group for Electronic Data Exchange, and the Center for Democracy and Technology, which is financed by Equifax, Dun & Bradstreet, and other purveyors of credit and financial information.

The group chose the right man in Hobson, for he was relentless on its behalf. At least a dozen times since 1993, he tried to hang his bill onto important bills before Congress.[55] He did it twice in 1996—once with the annual budget bill, the other time with Kennedy-Kassebaum.

Kennedy's staff took little notice of the Hobson rider; aides to Kassebaum, however, played a key role in paving the way in the Senate for the passage of his bill. (At least one member of Kassebaum's staff who worked on the Hobson bill was investigating career opportunities even as the measure was moving toward fruition. As the bill advanced, Dean Rosen, Kassebaum's health-policy counsel, was negotiating to become the director of government affairs in Washington for Glaxo Wellcome, the giant international pharmaceutical firm, which had a key interest in the legislation. Rosen told the Center that he made clear to the Senate Ethics Committee that he was in job talks with the firm and recused himself from issues revolving around administrative simplification.[56] Another Kassebaum aide, Christin Welsh, left the committee's staff after the legislation passed to join the staff of the Health Insurance Association of America.)

Beverly Woodward, a research associate at Brandeis University, has described these tags as a dangerous attack on privacy. "Such identifiers will make it possible to track the individual patient in all of his or her encounters with the health-care system," she wrote in *The Washington Post.* "They will make it virtually impossible to obtain confidential medical care."[57]

Hobson's chief aide on the administrative-simplification issue, Greg Moody, acknowledged the problems associated with the new law. "The critics are right," Moody, who's now the director of the Dean's Office in the College of Medicine at Ohio State University, told the Center. "There is a real threat here to privacy in administrative simplification. The key is finding a way to handle it responsibly."[58]

Hobson was amply rewarded for his efforts. He collected more than $28,000 in contributions from health, insurance, and information interests that favored the legislation for his 1996 re-election campaign. His largest such contribution came from the American Hospital Association, a member of the coalition that wrote the bill bearing his name.[59]

The enactment of Kennedy-Kassebaum triggered a push by lobbyists to influence the new privacy rules.[60] The Healthcare Leadership Council, an alliance of managed-care providers, pharmaceutical companies, and hospitals, worked to keep the new federal privacy restrictions as limited as possible.[61] Representatives of the council had testified to Congress in 1997 that the sharing of more information among various players—health plans, employers, hospitals, pharmaceutical companies—benefited patients; moreover, strict regulation was unnecessary, since health plans and providers already had their own accrediting bodies that required written confidentiality policies as a condition of membership. The Healthcare Leadership Council wanted all

information to be treated equally; it opposed tighter restrictions on sensitive information such as genetic data. Additionally, it wanted the federal government to override state privacy laws.[62] ("The pre-emption provisions are critically important to HLC membership, and we urge the strongest possible pre-emption language," the organization said in a 1998 statement to Congress.[63])

In keeping with the process outlined in Kennedy-Kassebaum, in the fall of 1997 the Health and Human Services Department submitted proposed privacy regulations to Congress. The proposal described a "national identification number" that would be assigned to each patient, making it possible to track the history of medical care received by the patient anywhere in the country.[64] Industry groups liked the proposal,[65] but privacy advocates were disturbed to see that the eighty pages of guidelines gave only the most general requirements for protecting patients' confidentiality and guaranteeing access to records.[66] The more apt title should have been "Permitting New Access to Medical Records Without the Requirement of Patient Authorization," wrote one critic, Dr. Jennifer Katze of the American Psychiatric Association Committee on Confidentiality.[67]

In late 1997 and early 1998, Congress continued to ponder what to do about health-care confidentiality, with a split developing among the Members who had backed Bennett's 1995 bill. Senator Patrick Leahy, a Democrat from Vermont, and Kennedy introduced a new bill, the Medical Information Privacy and Security Act. The Leahy-Kennedy bill would allow states to have stricter privacy laws than the federal government and, unlike the Bennett bill, require police to obtain a warrant before they could gain access to health-care records, except in life-threatening situations.[68] Senator James Jeffords, a Republican from Vermont who chairs the Labor and Human Resources Committee, worked with Bennett in early 1998 to craft a new draft of his bill. In April, however, Jeffords teamed with Senator Christopher Dodd, a Democrat from Connecticut, to introduce a new measure, the Health Care Personal Information Nondisclosure Act. The Jeffords-Dodd bill is essentially a compromise between Bennett and Leahy-Kennedy; it would pre-empt state confidentiality laws for the most part, but would allow states to impose tighter restrictions in especially sensitive areas such as mental-health treatment and HIV status.[69]

But Jeffords-Dodd's requirement that patients authorize any release of medical information quickly aroused vehement opposition from the insurance industry. Thomas Taylor, the chief executive officer of Arnica Mutual Insurance

Company and the chairman of the Alliance of American Insurers, insisted that insurers needed to be able to tap into patients' records without their permission in order to estimate risk and costs in workers' compensation and automobile insurance, and warned that companies might have to delay paying claims or obtain patients' records through litigation if the bill became law. "We can't afford to have any surprises come to us," Taylor said.[70] *National Underwriter,* an insurance-industry publication, complained that by allowing states to go further in protecting the privacy of psychiatric patients or those with HIV, the legislation created a "patchwork quilt of differing standards."[71]

A number of health-records privacy measures have been introduced in the House as well. In May, Representative Christopher Shays, a Democrat from Connecticut, introduced the Consumer Health and Research Technology Protection Act, a proposal similar to Jeffords-Dodd. Representative James McDermott, a Democrat from Washington, has a bill, the Medical Privacy in the Age of New Technologies Act of 1997, that goes even further, restricting insurance-company use of medical information to billing purposes only. "Insurance companies want as much information as possible so they can cherry-pick," McDermott told *National Journal.*[72] (Ironically, McDermott is simultaneously a key figure on another side of the privacy battle. In March of this year, Representative John Boehner, a Republican from Ohio and the chairman of the House Republican Conference, filed suit against him for violating the Electronic Communications Privacy Act by making public the tape of a conference call involving Boehner, House Speaker Newt Gingrich, and other Republican leaders; the call had been intercepted on a police scanner by a Florida couple and illegally recorded.[73])

In addition to the August 1999 deadline imposed by Kennedy-Kassebaum for enacting privacy rules, Congress faces another pressure: October 1998 is the starting date of the European Union's privacy directive, which requires that individuals have the right to control their health records and which blocks transmission of European health data to countries that don't have similar privacy policies.[74] With that dual pressure, it seems likely that, after 25 years of inaction, Congress may finally pass a medical-records privacy law. What remains undecided is whom that law will benefit the most—the health-care industry or the consumer. As Leahy explained to a Senate hearing in February: "It comes down to one question: Who controls our medical records, and how freely can others use them? All of us are health-care consumers—our families and we as individuals. And we have to ask as we go forward with this: What are the privacy interests of the American public? They are going to be at odds with

some very big economic interests. . . . [But] if Americans' privacy interests don't win out, we've failed our job. As I've said before, well-funded and sharply focused special interests might win a match-up like this. We can't allow that."[75]

CHAPTER 4

The Watchful Eye

Like many office workers across the country, Gail Nelson, a secretary in the Small Business Development Center at Salem State College in Salem, Massachusetts, was in the habit of bringing to work an extra set of clothes to change into for the gym, the walk home, or a dinner engagement. At the end of the day, Nelson would be the last one in the office. The restroom, located a floor below, was often locked by then, so she would change behind a partition in the back of her storefront office. She sometimes also used the divider to attend to other private needs. "I recall I got a severe sunburn where I needed a prescription ointment, and I would go behind the divider and open my blouse and put it on," she told the Center.

What Nelson didn't know was that her activities, not only after work but throughout the day, were being videotaped by a hidden camera. The only person who knew she was being taped was her boss. A coworker who was changing lightbulbs one day in October 1995 stumbled on the camera, lying on a newly installed shelf near the ceiling. He pulled the tape from it and watched the video with Nelson, who was shocked to see herself changing clothes. She later learned that the college had installed the camera in June of that year.

"At first I was frantically thinking of a good reason why they would do it," she said. "We had a work-study student in our office who had been stalked by a neighborhood person, and since we were a storefront, a public office, he would come in and harass her. So I thought, Maybe that's why the camera's up. But then I thought, Why didn't they tell me that? What reason would be good enough not to tell me? I concluded that there was no reason good enough not to tell me they were taping the office unless it was about me."

Nelson has been an employee of Salem State College for eight years, although she now works in a different office. She has filed an intention to sue

the college, alleging invasion of privacy.

"I think the single most important thing Congress could do is require that, if an area is under surveillance, there should be a sign, a notice. People should know," Nelson told the Center. "There are laws about how closely satellites can look at us, so everybody out on the street has better protection from surveillance by satellite than they do where they work."[1]

What Gail Nelson didn't know was that her activities not only after work but throughout the day, were being videotaped by a hidden camera. The only person who knew she was being taped was her boss.

"Apparently, the college thought someone was using the building after hours doing computer work or Xeroxing," Jeffrey Feuer, Nelson's attorney, told the Center. "To catch this person, they began videotaping 24 hours a day." Feuer, who has represented other victims of workplace privacy invasion, said that companies have a greater need to control their employees today and that spying on them is increasing. Part of that effort involves using videotape with no sound to get around the laws restricting wiretaps and eavesdropping. "In terms of videotaping, that's a loophole in our surveillance laws," Feuer said. "There are no federal laws on it. As long as they use video and are not capturing sound, they are not covered by the eavesdropping and wiretaps statutes."[2]

It's not only legal loopholes that work to employers' advantage in monitoring their workers. One of the few laws affecting workplace privacy, the Electronic Communications Privacy Act of 1986, contains language that explicidy guarantees employers the right to listen in on workers' telephone calls—an action that would be a crime if anyone *except* an employer did it.

Most people assume that federal laws protect Americans from being spied upon in the workplace. To the contrary, over the years Congress has rejected legislation spelling out basic privacy protections for employees. In fact, in many ways, employers have leeway to routinely scrutinize Americans to an extent that even police can't, unless they first go to court and obtain a warrant.[3] A 1997 survey by the American Management Association of 906 large and medium-sized companies found that 35 percent of the respondents occasionally used some form of electronic surveillance on their employees.[4] Workers spend their shifts under the scrutiny of hidden video cameras, typing at computers with special software that allows supervisors to monitor everything from the number of errors they make to how often they take breaks. Their phone calls may be eavesdropped upon, their e-mail messages and the

content of their computer hard-drives perused. And the scrutiny extends beyond on-the-job activities. They may be compelled to give urine samples for drug testing or submit to psychological testing, and their credit histories and health records are accessible to their employers as well.

"The question we ask ourselves is: How are these abuses possible? Isn't this America? I thought we had I had a right to privacy," Lewis Maltby, the director of the American Civil Liberties Union's Workplace Rights Project, told the House Education and Labor Subcommittee on Labor-Management Relations in 1993. "And the answer when it comes to the workplace is no, there is no right to privacy. The confusion that arises comes because when people think about the right to privacy, what they are really thinking about is the right to privacy found in the federal Constitution, in the Fourth Amendment of the Bill of Rights. This right is real. It is very important. But like all constitutional rights, it only applies to the government. The Constitution and Bill of Rights simply do not apply to any private organization, including not applying to any private corporation.

"When most Americans go to work in the morning, they might just as well be going to a foreign country, because they are equally beyond the reach of the Constitution in both situations. And unfortunately, federal law does very, very little to fill this void."[5]

The surveillance of workers isn't anything new. In the nineteenth century, factory owners often intruded into many aspects of their workers' lives, even imposing upon them nightly curfews and requiring that they attend church. Ford Motor Company, in its early years, employed a team of investigators who scrutinized employees' homes and personal finances to determine if they were worthy of profit-sharing bonuses.[6]

In the early twentieth century, management theorist Frederick Taylor's concepts of "scientific management" became increasingly popular. The Taylor philosophy took decision-making away from workers and required management to continually, systematically measure workers' performance—an approach that led some companies to equip typewriters with devices that measured the number of keystrokes made.[7] "Throughout the previous century and up through the 1950s, the right of employers to inquire into any aspect of an employee's life was virtually undisputed," a 1987 report by the Office of Technology Assessment noted. "Employers could choose their employees in any way they wished and were quite free to say, 'We want only this kind of per-

son working.' . . . [E]mployers compiled psychological profiles, employment histories, and other files of personal data quite unrestrainedly."[8]

When civil libertarians exposed the government's surveillance of citizens in the 1960s, private employers began to receive more scrutiny as well. After Congress passed the Privacy Act in 1974 to rein in data-gathering by the federal government, it created a Privacy Protection Study Commission to determine the degree to which the private sector needed regulation as well. In 1977, the commission described the scrutiny to which companies routinely subjected workers. "The individual may be examined by the company physician, given a battery of psychological tests, interviewed extensively, and subjected to a background investigation. After hiring, the records the employer keeps about him will again expand to accommodate attendance and payroll data, records concerning various types of benefit, performance evaluations, and much other information gathering—including, we might add, medical records where the employer provides medical insurance."[9]

The commission recommended that before the government stepped in, companies should try self-regulation and adopt formal privacy policies. In particular, the commission advocated informing and gaining prior consent from employees before information was gathered about them, separating sensitive medical and health-insurance information from regular employment files, discarding old information about employees that no longer had a justifiable purpose, and curbing polygraph testing and other intimidating modes of surveillance.[10]

Some companies gave it a try. In 1976, even before the commission's formal recommendations were released, Equitable Life became one of the first companies to institute a privacy policy. Edward Cabot, the company's vice president and associate counsel, explained at a Labor Department hearing in 1980 that Equitable's trust in its employees helped build morale and motivation: "Our concern for privacy," he said, "is an important element in our larger effort to develop and maintain the sort of relationship with our workers which is essential if our employees are to realize their full potential for themselves as well as for the Equitable."[11]

For the most part, however, self-regulation failed. When the privacy commission's chairman, David Linowes, a professor at the University of Illinois, did a follow-up study of 74 Fortune 500 companies in 1979, he found that few had followed the commission's advice. Three-quarters of the companies, for example, used information from employees' medical records in making decisions affecting their careers. Linowes cited the case of a woman who was denied a promotion after her employer learned that the woman's mother had

been treated by a psychiatrist—which the employer took as a sign that mental illness ran in the family.[12] (Ten years later, Linowes repeated his survey, with similarly discouraging results. Most companies still used medical information in making decisions about employees, and 85 percent routinely shared information from personnel files with their creditors.[13])

In 1980, Richard Neustadt, then a White House domestic policy adviser, noted that such practices as monitoring employees' conversations, using polygraphs and cameras on assembly lines, and denying employees access to records were common in both the manufacturing and service sectors.[14] But in the decade that followed, aided by advances in computing, employers subjected workers to monitoring on an unprecedented scale. According to a 1987 report prepared for Congress by the Office of Technology Assessment, between 4 million and 6 million American workers[15] were monitored at their desks by computer programs that tracked everything from the number of keyboard errors they made a day to the duration of their breaks.[16]

In addition, companies were testing employees in ways that probed not just their on-the-job performance but also their attitudes, beliefs, and activities outside the workplace. By 1987, employers were administering nearly 2 million polygraph tests a year to job applicants and employees; some included questions about employees' religious or political beliefs, their sex lives, and their union affiliations. Millions of employees were required to produce urine samples under observation for drug testing,[17] although the tests were frequently inaccurate.[18] (The report also noted that some of these tests "reveal information that is not only personal but is arguably not relevant to the employment situation.") At one company, management used video surveillance cameras to prevent more than one worker from going to the restroom at a time, as a way of hindering attempts to organize a union.[19]

The surveillance of workers isn't anything new. Ford Motor Company, in its early years, employed a team of investigators who scrutinized employees' homes and personal finances to determine if they were worthy of profit-sharing bonuses.

In its study, the Office of Technology Assessment also noted that companies generally had few safeguards to keep information gathered about employees confidential; once negative information was gathered about an employee, it could conceivably follow the person for the rest of his or her career. The report concluded: "The intensity and continuousness of computer-based monitoring raises questions about privacy, fairness, and quality of work life."[20]

The OTA's 1987 report spelled out for Congress a pervasive problem that affected millions of American workers. The following year, after an intense lobbying effort by the American Civil Liberties Union, labor unions, and other privacy advocates, Congress passed the Employee Polygraph Protection Act, which barred the use of lie detectors to screen new hires; employers could test employees only if there was a "reasonable suspicion" of wrongdoing. Additionally, employers had to advise employees of their rights, including the right not to take a test, and employees couldn't be dismissed on the basis of the results unless there was other evidence of wrongdoing as well.[21]

By 1987, employers were administering nearly 2 million polygraph tests a year to lob applicants and employees; some included questions about employees religious or political beliefs, their sex lives, and their union affiliations.

In 1991, Delta Airlines hired Equifax to conduct background checks on thousands of Pan American World Airways employees who sought jobs after Delta's takeover of Pan Am's European routes. The applicants were required to sign waivers that allowed Equifax to interview friends and coworkers and probe the applicants' personal lives. (A friend of one applicant told *Newsday* that interviewers asked him not only about whether the applicant had drug, alcohol, or financial problems but also about his sexual orientation.[22])

Otherwise, Congress did nothing about the problems cited in the OTA's report. An investigation by *Macworld* magazine in 1993 estimated that 20 million American workers were being monitored on the job through the computers on their desktops. In large companies, 30 percent of managers surveyed by the magazine admitted that they had perused employees' computer files and e-mail communications or listened to their voice-mail messages. Only 18 percent of companies had a written policy regarding electronic privacy.[23]

The effect of this culture of suspicion upon its targets was subsequently documented in a 1990 study by researchers at the University of Wisconsin-Madison. They found that workers who were electronically monitored by their bosses experienced tension, anxiety, and depression to a greater degree than non-monitored workers and also reported more physical problems, such as sore wrists, back problems, and headaches.[24]

In 1991, Cindia Cameron, an organizer for 9-to-5, a national working women's group, told the Senate Labor and Human Resources Committee about numerous abuses that members of her organization had reportedly suf-

fered. One woman's boss overheard her making an appointment to interview for another job; subsequently, he not only fired her but also called her prospective employer and offered false derogatory information about her work record. A reservation clerk at an airline cursed under her breath after a difficult customer hung up; no one heard the remark except for her eavesdropping supervisor, who berated her and forced her to sign a letter documenting the incident, which then went into her personnel file.[25]

Renee Maurel, an airline reservation sales agent, described for a Senate subcommittee how sophisticated computer monitoring had changed the very nature of her work: "Monitoring became the job. How long I was on a phone call, how long between phone calls, how many minutes I was on a break or at my desk became the focus. Not wanting to be the robot I was becoming, I had to create an alter ego—another person who did the work, did what the company demanded, sat there on the assembly line. The company, delighted that we could be tracked so completely, took the monitoring capabilities to the most negative limit. I was disciplined or harassed on several occasions for non-business-related conversations that took place between business calls. I was written up every time I was two or more minutes late from a break. I have always felt that there was someone else in my headset, someone in my keyboard, waiting to punish me for the smallest infraction. Stress and tension brought physical problems—eye, ear, and neck strain among the most persistent. Because the statistics were so important, that is exactly what I passed along to the customers. I would unnecessarily keep them on the phone so I could finish my typing. I would cut them short if they became too chatty. I looked forward only to my fifty minutes of break time, and then worried that I might be late getting back to my desk. Emphasis on statistics made me play games, try to outwit the monitoring devices. None of this did much to help the customer, who, of course, was being monitored also. . . . [T]he customer became a statistic."[26]

Such monitoring of employee phone calls was identified by the OTA in 1987 as a particularly worrisome type of workplace surveillance. Employers argued that listening in on employees' conversations was a valuable tool in managing them and that the ability to do it without employees' knowledge was essential. The OTA noted that one company was so obsessed with keeping surveillance surreptitious that supervisors were required to wear their headsets all day so that employees would not be able to guess whether they were listening or attending to other duties.[27] In 1986, AT&T pressured the state of West Virginia to repeal a three-year-old law requiring that companies alert workers to mon-

itoring with a beep; the telephone giant threatened to build a new credit-management center in another state if the privacy law remained in force.[28] OTA noted that such monitoring "invokes feelings of invasion of privacy, even though the conversation involved is not really a private one. One operator interviewed for OTA said, 'When they are listening to me, I'm very upset, because you can't stop it.' The privacy aspect applies more clearly to the customer's side of the conversation. Some people may object to third parties overhearing their conversations."[29]

Congress, however, has been careful over the years to preserve employers' right to eavesdrop. Title III of the Omnibus Crime Control and Safe Streets Act of 1968 barred the interception of telephone calls; even law-enforcement agencies had to obtain a judicial warrant before they could listen in.[30] At the request of industry, however, Congress exempted switchboards and other equipment on businesses' premises from the definition of "interception devices."[31] Two decades later, Congress passed the Electronic Communications Privacy Act of 1986, which extended the anti-wiretapping ban to e-mail, voice-mail, and other new technologies. In many other ways a victory for privacy advocates, the law contained one subtle but significant defeat: It again allowed a company to intercept employees' electronic communications as long as the interception was done "in the ordinary course of its business."[32] The courts have placed some restrictions on employer eavesdropping—for example, employers may listen in to establish that an employee is making a personal call, but once that goal is accomplished, they're not supposed to listen to what the employee is saying.[33] In practice, privacy advocates say, such distinctions have often gone by the wayside.[34]

In 1991, then-Senator Paul Simon, a Democrat from Illinois, sought to rectify the situation with the Privacy for Consumers and Workers Act,[35] which would have given workers some protection from phone monitoring and other types of surveillance. Electronic monitoring of all sorts, including videotaping, would be allowed only to the extent that it was relevant to job performance, and employees would have access to the data compiled about them. Employers would be required to notify employees when and how they were being monitored; if phone monitoring wasn't continuous, a beep or a flashing light would be required.[36]

Simon's bill and a companion bill introduced in the House by Pat Williams, a Democrat from Montana,[37] were vigorously resisted by the industry. One opponent was the National Association of Manufacturers, an organization representing. 12,500 American companies, whose assistant vice president,

Barry Fineran, testified that "random and periodic silent monitoring is a very important management tool," and that spying on workers helped produce productivity gains that enabled U.S. companies to keep pace with foreign competitors. "Otherwise, the United States may as well let the information age pass it by," he warned. Fineran also argued that signaling employees when they were under surveillance would actually be more stressful for them. "I am sure there are employees who are probably functioning quite well right now, and that light comes on, and they aren't going to function as well as they do right now," he explained. "And I think that if you think it all the way through, their evaluations will probably be somewhat affected, to the detriment of those employees."[38] Similarly, corporate America objected to restrictions on surreptitious videotaping. In the words of Vincent Ruffolo, the president of Security Companies Organized for Legislative Action: "An employer would be put in the absurd position of having to advise suspected thieves when they are being monitored."

The American Insurance Society, the Risk and Insurance Management Society, and other groups also lobbied against the legislation. They managed to get an amendment to the bill that allowed employers to conduct off-site covert surveillance of employees, which the insurers argued was necessary to prevent workers'-compensation fraud.[39]

Even with such changes, business opposition was sufficiently strong to keep the bills stalled in committee. In 1993, Simon and Williams tried again, this time making significant concessions to employers. Williams's 1993 version of the Privacy for Consumers and Workers Act, for example, no longer required employers to use beeps or flashing lights; instead, it was sufficient to inform employees they were subject to electronic monitoring and to specify what type. Employers were allowed to conduct electronic surveillance without any notification, if they had a "reasonable suspicion" that the employee was breaking laws or doing things harmful to the employer. Surveillance in locker rooms and restrooms was barred, but with the same "reasonable suspicion" exception. In addition, companies were allowed to monitor new employees without restriction during their first sixty days.[40]

An investigation by *Macworld* magazine in 1993 estimated that 20 million American workers were being monitored on the job through the computers on their desktops.

Even so, the legislation was again opposed by a broad range of businesses, ranging from manufacturing and insurance to airlines and telecommunica-

tions. Household Finance Corporation, a consumer credit provider, warned that the law would "impose unrealistic, onerous, inefficient, and counterproductive measures on the modern paperless workplace."[41] The Security Industries Association argued that the inability to monitor employees would make brokerages and their customers vulnerable to fraud.[42] Associated Builders and Contractors worried that video monitoring of strikers' picket lines would be prohibited.[43] The director of corporate security for FMC Corporation, James Royer, even admonished Congress that if the bill, with its restrictions on video surveillance, were passed "your safety, the safety of citizens entering these premises, and the assets of this government would be at risk."[44]

"Monitoring became the job," an airline reservation sales agent testified. "How long I was on a phone call, how long between phone calls, how many minutes I was on a break or at my desk became the focus."

Those arguments won considerable sympathy from Capitol Hill lawmakers. "The notion that electronic monitoring has become a valuable tool of management is evidenced by the diverse universe of companies that use it," noted Representative Marge Roukema, a Republican from New Jersey,[45] who had offered an amendment to the previous version of the bill, exempting financial institutions from regulation. (According to an analysis by the Center, Roukema received $250,000 from banks and financial-services companies from 1988 to 1996.[46])

Representative Peter Hoekstra, a Republican from Michigan, was blunter. "I believe the key question for discussion here is: What is the expectation of privacy in the workplace?" he said in a statement. "Given the information glut that has been produced by new technology, how far can business go to use electronic devices to improve productivity and performance quality? What level of privacy can an employee expect when on company time, using official phones, or using company computers or cash registers?"[47]

In the Senate, the most vigorous opponent of Simon's bill was Strom Thurmond, a Republican from South Carolina, who maintained that "businesses are finding it essential to use electronic monitoring as a means of staying competitive in the 1990s and into the next century," and that employees' privacy "must be balanced against the need of businesses to maintain quality services in a competitive market."[48]

Ultimately, both the Simon and Williams versions of the bill were killed in committee. Since then, no new workplace-privacy legislation has surfaced in

Congress and the surveillance of employees continues. Eighty percent of American companies now test employees for drug use, compared with 21 percent a decade ago. A 1996 survey of Fortune 500 companies found that 70 percent gave personal information about workers to credit grantors and 47 percent to landlords.[49] An Arlington, Virginia, company markets an artificial-intelligence software program that can automatically scan employees' e-mail for offensive language.[50] In place of polygraphs, businesses now compel job applicants to take psychological tests that not only purport to reveal whether the person is dishonest but also give detailed scores for an array of traits, from compassion to stubbornness.[51] (According to a 1990 OTA report, in addition to direct questions about whether or not a person thinks stealing is wrong, such tests also contain "veiled purpose" questions such as "On the average, how often a week do you go to parties?" or "How often do you blush?"[52]) Video surveillance in restrooms and locker rooms is legal in all but three states (although the California legislature is considering legislation to bar it[53]). Thanks to Congress, when millions of Americans go to work each day, they leave their privacy rights at home.

CHAPTER 5

The Data Octopus

In April 1997, Senators Dianne Feinstein, a Democrat from California, and Senator Charles Grassley, a Republican from Iowa, introduced the Personal Information Privacy Act, which if enacted would prevent credit bureaus from selling individuals' key identifying information—Social Security numbers, unlisted telephone numbers, dates of birth, past addresses, and mothers' maiden names—without their consent. To dramatize the need for such a law, Feinstein told her fellow legislators how she had been alarmed to discover that her own Social Security number and other information were easily accessible from the Internet sites of information-brokerage firms. "My staff retrieved it in less than three minutes," she explained.

Feinstein decried a growing trade in sensitive personal information, gleaned from the identifying header attached to credit reports. That trade, she noted, was just part of a larger marketplace for Americans' personal data. Companies, she said, were using advances in computer technology to compile vast amounts of information on consumers' activities—from what they bought in stores to the medicines they used—and merging it with financial, demographic, and other data to create detailed profiles. "Now, with networked computers, multiple sets of records can be merged or matched with one another, creating highly detailed portraits of our interests, our allergies, food preferences, musical tastes, levels of wealth, gender, ethnicity, homes, and neighborhoods," she said. "These records can be disseminated around the world in seconds."

Feinstein warned that "people are losing control over their own identities. We don't know where this information is going or how it is being used. We don't know how much is out there and who is getting it. Our private lives are becoming commodities with tremendous value in the marketplace, yet we,

the owners of the information, often do not derive the benefits. Information about us can be used to our detriment."[1]

Like a similar measure introduced in the House of Representatives by Jerry Kleczka, a Democrat from Wisconsin, Feinstein's bill sought to close a loophole in the Fair Credit Reporting Act of 1971. It was a loophole that Congress had allowed to remain when it updated FCRA in 1996, despite an admonition from the Federal Trade Commission that the availability of such information "may facilitate identity fraud, credit fraud, and other illegal activities."[2] The FTC's warning, of course, was not the first that Congress had heard about the dangers of identity fraud. In October 1991, during a hearing on proposed revisions to FCRA, Senator Alan Dixon, a Democrat from Illinois, submitted for the record several letters from consumers who had been victimized by credit imposters.

"Our private lives," Senator Dianne Feinstein of California said, "are becoming commodities with tremendous value in the marketplace, yet we, the owners of the information, often do not derive the benefits.

A man in Denver, for example, had written to Dixon to describe how in January 1991 "a person unknown to me changed the billing address on most of my credit-card accounts. The altered accounts reflected a new address in San Diego. Whoever changed my billing address ordered a duplicate card from one credit-card company and began making thousands of dollars in unauthorized charges to my account. I didn't receive any invoices, so I didn't know what was happening until March, when the credit-card companies tracked me down to pay. It apparently didn't seem to odd to them that they traced me to a Denver address when the accounts were showing a San Diego address." Even though the San Diego police quickly verified that a fraud had taken place, it took the victim many months and numerous calls and letters to clear his record. "Con artists can gain access to credit histories with relative ease," he complained in frustration, imploring Congress to take action.[3]

But Congress failed to heed the man's warning, just as it again failed in 1996 to heed the FTC, letting the Feinstein-Grassley and Kleczka bills languish. A May 1998 report by the General Accounting Office, the investigative arm of Congress, at Kleczka's request showed the consequences of that inaction. Credit-bureau officials admitted to the GAO that the problem of identity fraud was on the rise. The precise number of such crimes was difficult to determine, in part because the bureaus didn't systematically track them.[4] However, a Trans Union executive told the GAO that consumer inquiries about possible

identity fraud had increased from 35,000 in 1992 to 522,000 in 1997.[5] In the first six months of fiscal 1997, the Social Security Administration logged almost 4,900 allegations of fraudulent use of Social Security numbers—more than twice as many as in the previous entire year.[6] In a particularly alarming case, a temporary worker hired in January 1998 by a Baltimore subsidiary of Equifax allegedly stole $100,000 in computers and other electronics equipment by accessing the credit records of unsuspecting consumers. (Despite an arrest record, *The Washington Post* reported, the worker had slipped through Equifax's background-check procedures.)[7]

According to the GAO, the Secret Service estimated that identity thieves stole at least $750 million in 1997 alone.[8] Although much of that damage was absorbed by credit-card companies as a risk of doing business, the report noted that "on an individual level, the 'human' costs of identity fraud can be quite substantial. These costs include emotional costs, as well as various financial and/or opportunity costs. For example, the victims may be unable to obtain a job, purchase a car, or qualify for a mortgage."[9]

In March 1997, Senator Jon Kyl, a Republican from Arizona, introduced the Identity Theft and Assumption Deterrence Act, which would make identity theft a federal crime and mandate restitution to victims. Kyi's bill, although supported by privacy advocates such as U.S. PIRG, stops short of what those groups say would be the most effective remedies: a ban on the separate selling of credit headers, a requirement that bureaus match at least four identifying details on an application before verifying it, and notification for consumers each time their credit reports are accessed. But the credit bureaus, which earn tens of millions of dollars annually selling credit headers[10]—the identifying information that appears at the top of credit reports—oppose such restrictions, according to the GAO; if the sale of identifying data were restricted, they argue, it would be more difficult to verify consumers' credit—even though consumers could authorize use of that information if they wished.[11]

But given the antiregulatory climate in Congress and the clout of the industries that use credit bureaus, privacy advocates aren't optimistic about getting those things. Evan Hendricks, the publisher of the journal *Privacy Times,* puts it bluntly: "The conventional wisdom is that if you try to expand the theft-of-identity bill and expand the duties of credit agencies to combat theft, that would kill the bill."[12]

But identity theft is just another example of Congress's reluctance to protect consumers' privacy if it means clamping down on business. The result has been a society whose ever-diminishing privacy seems to bewilder even the

legislators who have presided over that loss. "Big Brother has turned out to be private industry's immense, computerized network for gathering information," complained Representative Marge Roukema, a Republican from New Jersey, at a September 1997 hearing of the House Banking and Financial Services Subcommittee on Financial Institutions and Consumer Credit. (Four years earlier, Roukema had sided with business interests in criticizing the Privacy for Consumers and Workers Act.) "And the irony is that we invite him into our homes and workplaces every time we sit down at a computer, use our credit cards, purchase goods, or simply make a telephone call. . . . It's our job to keep Big Brother under control."[13]

Unfortunately, time and again, it's a job at which Congress has failed.

List of Tables

Top Contributors to Congressional Campaigns, 1987-96
Insurance Interests 56
Medical Interests 57

Top Senate Recipients of Campaign Contributions, 1987-96
Insurance Interests 58
Medical Interests 59

Top House Recipients of Campaign Contributions, 1987-96
Insurance Interests 60
Medical Interests 61

Information in tables is based on the Center for Public Integrity's analysis of data from the Federal Election Commission and the Center for Responsive Politics.

Top Contributors to Congressional Campaigns 1987-96

INSURANCE INTERESTS

Contributor	Location	Amount
Travelers Group	New York	$1,817,605
CIGNA Corporation	Philadelphia	1,092,487
Torchmark Corporation	Birmingham, Ala.	855,204
ITT Corporation	New York	827,905
Mutual of Omaha Insurance Company	Omaha, Neb.	763 799
American International Group	New York	742,147
American General Corporation	Houston	632,506
Equitable Companies, Inc.	New York	629,950
American Insurance Association	Washington	521,648
Allstate Insurance Company	Northbrook, Ill.	420,480

Top Contributors to Congressional Campaigns 1987-96

MEDICAL INTERESTS

Contributor	Location	Amount
American Hospital Association	Chicago	$3,460,501
Prudential Insurance Company of America	Newark, N.J.	2,176,964
AFLAC, Inc.	Columbus, Ga.	1,801,150
Blue Cross and Blue Shield	Washington	1,755,178
Pfizer, Inc.	New York	1,178,273
Eli Lilly & Company	Indianapolis	987,245
Health Insurance Association of America	Washington	858,201
Merck & Company, Inc.	Whitehouse Station, N.J.	857,997
Bristol-Myers Squibb Company	New York	844,392
Abbott Laboratories	Abbott Park, Ill.	839,998

Top Senate Recipients of Campaign Contributions 1987-96

INSURANCE INTERESTS

Senator	Party-State	Committee	Amount
Christopher Dodd	D-Conn.	Banking, Housing, and Urban Affairs	$180,882
Alfonse D'Amato	R-N.Y.	Banking, Housing, and Urban Affairs, chairman; Finance	153,500
John Chafee	R-R.I.	Joint Committee on Taxation	151,923
James Sasser	D-Tenn.	Banking, Housing, and Urban Affairs	138,550
Orrin Hatch	R-Utah	Judiciary, chairman; Finance	132,687
Dan Coats	R-Ind.	Labor and Human Resources	132,593
Larry Pressler	R-S.D.	Finance	124,499
Frank **Lautenberg**	D-N.J.		124,036
Kent Conrad	D-N.D.	Finance	122,508
Kay Bailey Hutchison	R-Texas		120,454
Lloyd **Bentsen**	D-Texas	Finance, chairman; Joint Committee on Taxation, chairman	119,550
Daniel Patrick **Moynihan**	D-N.Y.	Finance; Joint Committee on Taxation	119,500
Phil Gramm	R-Texas	Banking, Housing, and Urban Affairs; Finance	118,907
Richard Bryan	D-Nev.	Banking, Housing, and Urban Affairs; Finance	116,704
Christopher Bond	R-Mo.		115,700

Names in boldface are current members of the Senate.

Top Senate Recipients of Campaign Contributions 1987-96

MEDICAL INTERESTS

Senator	Party-State	Committee	Amount
Frank **Lautenberg**	D-N.J.		$244,858
Dan Coats	R-Ind.	Labor and Human Resources	222,812
Orrin Hatch	R-Utah	Judiciary, chairman; Finance	161,999
Max Baucus	D-Mont.	Finance; Joint Committee on Taxation	155,063
John **Chafee**	R-R.I.	Joint Committee on Taxation	142,075
John D. Rockefeller IV	D-W.V.	Finance	141,000
Robert **Packwood**	R-Ore.	Finance; Joint Committee on Taxation	135,927
Richard **Lugar**	R-Ind.		134,515
Daniel Patrick **Moynihan**	D-N.Y.	Finance; Joint Committee on Taxation	134,000
David Durenberger	R-Minn.	Finance; Labor and Human Resources	132,050
Tom **Harkin**	D-Iowa	Labor and Human Resources	130,282
Phil Gramm	R-Texas	Banking, Housing, and Urban Affairs; Finance; Small Business	127,550
Arlen Specter	R-Pa.	Judiciary	118,268
Christopher Dodd	D-Conn.	Banking, Housing, and Urban Affairs	118,150
Bill Bradley	D-NJ.	Finance	112,411

Names in boldface are current members of the Senate.

Top House Recipients of Campaign Contributions 1987-96

INSURANCE INTERESTS

Representative	Party-State	Committee	Amount
Barbara **Kennelly**	D-Conn.		$218,900
Earl Pomerby	D-N.D.		217,711
Richard Gephardt	D-Mo.	Minority Leader	207,077
Nancy Johnson	R-Conn.		198,376
Dan **Rostenkowski**	D-Ill.		145,250
Bill Paxon	R-N.Y.	Commerce	143,676
Newt Gingrich	R-Ga.	Speaker	142,212
Thomas **Bliley**	R-Va.	Commerce, chairman	140,191
Michael Andrews	D-Texas		126,603
Clay Shaw	R-Fla.		123,950
Charles **Rangel**	D-N.Y.		112,432
Steny Hoyer	D-Md.		112,047
Michael **Oxley**	R-Ohio	Commerce	109,200
John Dingell	D-Mich.	Commerce, ranking Democrat	108,700
Vic Fazio	D-Calif.		108,398

Names in boldface are current members of the House of Representatives.

Top House Recipients of Campaign Contributions 1987-96

MEDICAL INTERESTS

Representative	Party-State	Committee	Amount
Richard Gephardt	D-Mo.	Minority Leader	$232,743
Vic Fazio	D-Calif.		169,864
Charles **Rangel**	D-N.Y.		168,875
Robert **Matsui**	D-Calif.		158,110
Newt Gingrich	R-Ga.	Speaker	143,803
Dan **Rostenkowski**	D-I11.		141,175
Thomas **Bliley**	R-Va.	Commerce, chairman	131,507
Nancy Johnson	R-Conn.		125,606
John **Dingell**	D-Mich.	Commerce, ranking Democrat	118,250
Henry **Waxman**	D-Calif.	Commerce	113,400
Barbara **Kennelly**	D-Conn.		112,950
Michael **Bilirakis**	R-Fla.	Commerce	104,714
Dick Zimmer	R-N.J.		98,350
Peter Hoagland	D-Neb.		96,750
Martin Frost	D-Texas		94,100

Names in boldface are current members of the House of Representatives.

Notes

Some of the following citations do not contain page numbers because they were obtained from electronic libraries.

SUMMARY

1. Interview with Louis Hafken, July 10, 1998; Nora Lockwood Tooher, "Physician Criticizes CVS Drug Advisory: The Psychiatrist Says a Letter Requesting That He Take a CVS Employee Off an Antianxiety Drug Is an Invasion of Privacy," *The Providence Journal-Bulletin,* February 27, 1998, p. 1F.
2. Interview with Louis Hafken.
3. Tooher, "Physician Criticizes CVS Drug Advisory: The Psychiatrist Says a Letter Requesting That He Take a CVS Employee Off an Antianxiety Drug Is an Invasion of Privacy."
4. Interview with Louis Hafken.
5. Vance Packard, *The Naked Society,* New York: David McKay Company, 1964, p. 12.
6. Packard, *The Naked Society,* pp. 3-13, 47-73, 169-187, 193-197; John Brooks, "There's Somebody Watching You," *The New YorkTimes Book Review,* March 15, 1964, p. 1.
7. Federal Trade Commission, "Staff Report: Public Workshop on Consumer Privacy on the Global Information Infrastructure," December 1996, downloaded from www.ftc.gov/reports/privacy/privacy3.htm.
8. Lawrence A. Ponemon, "Privacy Needs Protection," *Journal of Commerce,* March 23, 1998.
9. Ibid.
10. Andre Mouchard, "Under the Boss's Gaze: Does Big Brother Sign Your Paycheck? Workplace Privacy Is a Gray Area," *The Orange County Register,* April 22, 1996.
11. Maggie Scarf, "Keeping Secrets," *TheNew York Times Magazine,* June 16, 1996, p. 38.
12. Edmund Sanders, "Bankruptcy: They're Watching to See If You're on the Brink," *The Orange County Register,* December 28, 1997, p. K1; Edmund Sanders, "Seen a Counselor? Charged Milk and Bread? Your Worried Bank Is Watching," *The Orange County Register,* January 1, 1998, p. D1.
13. John Awerdick, "The Privacy Police," *Marketing Tools,* June 1995, p. 70.
14. House bill H.R. 184, summary and status downloaded from www.thomas.loc.gov.
15. Office of Technology Assessment, "Use of Integrity Tests for Pre-employment Screening," 1990.
16. Untitled abstract of article, *The New York Times,* October 4, 1973.

17. Paul S. Brown, "Protecting Employer Rights: RIMS Defends Legitimate Use of Surveillance," *Risk Management,* April 1997, p. 100.
18. Senate bill S. 600 and House bill H.R. 1813, summary and status downloaded from www.thomas.loc.gov.
19. "Privacy or Paranoia?" *The Indianapolis Star,* September 22, 1997.
20. Letter to the Center for Public Integrity from Jim Dempsey, senior staff counsel, Center for Democracy and Technology, July 1, 1998.
21. Michael G. Radigan, "Respecting Privacy Rights of Employees," *New York Law Journal,* February 18, 1997, p. S4.
22. Interview with Ed Mierzwinski, June 8, 1998.
23. Center for Responsive Politics, downloaded from www.crp.org/index/html.
24. CDB Infotek Web site, www.cdb.com/public/companyinfo/company.html.
25. Ronald Campbell, "Information Broker CDB Infotek Cuts Its Fee from $50, Raising Privacy Concerns: For Just $7, This Santa Ana Company Will Tell All—About You," *The Orange County Register,* February 17, 1998, p. A1; CDB Infotek Web site, www.cdb.com/public/products/pricing/.
26. Stan Soocher, "Prescription-Drug Papers Could Go to Journalist," *The National Law Journal,* September 5, 1983, p. 33; James H. Rubin, "Appeals Court Rules Agency May Not Keep Inventory Secret," Associated Press, July 22, 1983.
27. *The Congressional Record,* February 9, 1984, p. S1333.
28. "House Kills Medical-Records Privacy Measure," Associated Press, December 1, 1980.
29. Kerry Hall, "Lawmakers Join Call for Greater Privacy for Cellular-Phone Calls," *The Orange County Register,* February 6, 1997, p. A14.
30. "House Votes to Protect Cell-Phone Privacy," *Las Vegas Review-Journal,* March 6, 1998.
31. Stephen Green, "Feinstein to Seek Tougher Privacy Laws, Co-Authors Bill Aimed at Curbing Commercial Use of Personal Data," *The San Diego Union-Tribune,* June 6, 1997, p. A2.

CHAPTER 1—THE INVADERS

1. John Osmundsen, "Expert Fears Harmful Effects Amid Benefits from Computers," *The New York Times,* January 1, 1962, p. 33.
2. Nan Robertson, "Data Center Held to Peril Privacy," *The New York Times,* July 27, 1966, p. 41.
3. "Federal Data Banks and Constitutional Rights," staff report by Senate Judiciary Subcommittee on Constitutional Rights, 1974, vol. 1, p. xviii.
4. Ann Baker and John Finnegan, Jr., "Nineteen Eighty-Four Is Still Seven Years Away, but Big Brother Is Watching You Already," Associated Press, May 1, 1977.
5. Ibid.
6. Ibid.; "Federal Data Banks and Constitutional Rights," vol. 1, p. xxxvii.
7. Federal Data Banks and Constitutional Rights," vol. 1, p. xxv; Federal Trade Commission, "Staff Report: Public Workshop on Consumer Privacy on the Global Information Infrastructure," December 1996, downloaded from www.ftc.gov/reports/privacy/privacy3.htm.
8. Nancy L. Ross, "Panel to Urge Extending Privacy Law to Industry," *The Washington Post,* March 22, 1977, p. A2.
9. Policy Studies Associates, Inc., "Protecting the Privacy of Student Education Records," *Journal of School Health,* April 1997.
10. Federal Trade Commission, "Staff Report: Public Workshop on Consumer Privacy on the Global Information Infrastructure."
11. Vance Packard, *The Naked Society,* New York: David McKay Company, 1964, p. 9.

12. Ibid., pp. 179-181.
13. Interview with Kenneth McLean, July 10, 1998.
14. Ross, "Panel to Urge Extending Privacy Law to Industry; "Personal Privacy in an Information Society," Report of the Privacy Protection Study Commission, July 1977, pp. 336-337.
15. Packard, *The Naked Society, p.* 65.
16. "Personal Privacy in an Information Society," Report of the Privacy Protection Study Commission, p. 333.
17. Joan Cook, untitled abstract of article, *The New York Times,* January 3, 1974, p. 75.
18. Personal Privacy in an Information Society," Report of the Privacy Protection Study Commission, pp. 337-340.
19. Baker and Finnegan, "Nineteen Eighty-Four Is Still Seven Years Away, but Big Brother Is Watching You Already."
20. U.S. PIRG survey, downloaded from www.pirg.org/pirg/consumer/credit/mistakes/page2.htm.
21. Gerald Gold, "Flaws Are Found in Credit Bureau Law to Protect Consumers," *The New York Times,* September 30, 1973, p. 57.
22. Ibid.
23. Ibid.; testimony of Edmund Mierzwinski before the Senate Banking, Housing, and Urban Affairs Subcommittee on Consumer and Regulatory Affairs, October 22, 1991.
24. Interview with Kenneth McLean.
25. Ibid.
26. Report of the Privacy Protection Study Commission, July 1977, various pages and sections; Nancy L. Ross, "Panel Urges Personal Privacy Safeguards in Computer Age," *The Washington Post,* July 13, 1977, p. A2.
27. Ibid.
28. Robert M. Gellman, "Can Privacy Be Regulated Effectively on a National Level?" downloaded from http://153.104.15.245/students/orgs/law-revi/vol_41/Issue_1/gellman.htm.
29. Teresa Carson, "Public Finds Banks Are Not Too Curious," *American Banker,* May 4, 1979.
30. Federal Trade Commission, "Staff Report: Public Workshop on Consumer Privacy on the Global Information Infrastructure."
31. Interview with Evan Hendricks, publisher, *Privacy Times,* June 8, 1998.

CHAPTER 2—No LIMIT

1. Sari Horwitz, "FTC Launches Credit-Rights Campaign: Miller Calls Problems No. 1 Source of Consumer Complaints to Agency," *The Washington Post,* May 28, 1985, p. El.
2. Michael Precker, "Credit Conscious: Bureaus' Handling of Sensitive Data Remains Controversial," *The Dallas Morning News,* October 1, 1994, p. 1C.
3. Joe Cannariato, "Equifax Provides Insurance Firms with Clear View of Clients," *The Business Journal-Milwaukee,* June 9, 1986, section 2, p. 5.
4. Ann Mariano, "Backlog at the Bureau: Stiff Lending Rules Slow Credit Checks," *The Washington Post,* August 2, 1986, p. E1.
5. Doug Hitchcock, "Computer Model Predicts Customers' Odds of Bankruptcy," *Kansas City Business Journal,* February 1, 1988, section 1, p. 8.
6. Prepared statement of Federal Trade Commission before the Senate Banking, Housing, and Urban Affairs Subcommittee on Consumer and Regulatory Affairs, October 22, 1991; Simson L. Garfinkel, "How Computers Help Target Buyers," *The Christian Science Monitor,* July 25, 1990, p. 13.
7. "The Privacy Issue Is Bigger Than You Think," *DM News,* December 1, 1988.

8. Cheryl Wetzstein, "Bureaus, Consumer Advocates Argue Over Rate of Goofs," *The Washington Times*, September 27, 1990, p. C11.
9. "When the Credit Bureau Fouls Up," Associated Press, September 14, 1990.
10. Simson L. Garfinkel, "Privacy Issue Caught in Credit Network," *The Christian Science Monitor*, July 18, 1990, p. 1.
11. David Berreby, "The Ordeal of the Credit Fraud Victim," *The New York Times*, September 4, 1988, section 3, p. 7.
12. Albert B. Crenshaw, "Giving Credit Where Credit's Due: Congress Looks into Consumer Anger over Credit Bureau Databases," *The Washington Post*, June 17, 1990, p. H11.
13. Simson L. Garfinkel, "Putting More Teeth in Consumer Rights," *The Christian Science Monitor*, August 8, 1990, p. 13; James Kilpatrick, "Credit Reporting Act Needs to Be Updated," *St. Louis Post-Dispatch*, July 17, 1990, p. 3B; Stephen Barlas, "Prescreen Notification Measure Seems Dead for Now, May Be Reintroduced," *DM News*, October 29, 1990, p. 3.
14. Barlas, "Prescreen Notification Measure Seems Dead for Now, May Be Reintroduced."
15. Testimony of Kenneth Hoerr before the House Banking Subcommittee on Consumer Affairs and Coinage, June 12, 1990.
16. Horwitz, "FTC Launches Credit-Rights Campaign: Miller Calls Problems No. 1 Source of Consumer Complaints to Agency."
17. Barlas, "Prescreen Notification Measure Seems Dead for Now, May Be Reintroduced."
18. Jeanne Iida, "Congress Eyeing Banks as Culprits in Credit Reports," *American Banker*, September 11, 1991, p. 1.
19. Albert B. Crenshaw, "Checking the Credit Bureau Industry: Complaints About Errors Spark Call for Stronger Regulation," *The Washington Post*, June 9, 1991, p. H3.
20. Robert Naylor, Jr., "Consumer Group Urges Federal Crackdown on Credit Reporting Companies," Associated Press, April 30, 1991.
21. Dave Skidmore, "Study Finds Erroneous Credit Reports Hard to Fix," Associated Press, June 6, 1991.
22. Letter from Karen E. Porter, town clerk and treasurer, Norwich, Connecticut, to Senator Alan Dixon, October 4, 1991. Cited in hearing before the Senate Banking, Housing, and Urban Affairs Subcommittee on Consumer and Regulatory Affairs, October 22, 1991.
23. "California Finance Executive Testifies Before Congress on Credit Reporting Measures," PR Newswire, June 6, 1991.
24. Robert Naylor, Jr., "Congress Considering Tighter Controls on Credit Reporting Industry," Associated Press, September 22, 1991
25. Ibid.
26. Michael Max Phillips, "Senate Panel Gives Boost to New Credit Reporting Law," States News Service, October 22, 1991.
27. Robert A. Rosenblatt, "TRW Agrees to Improve Credit Reports," *Los Angeles Times*, December 11, 1991, p. A1; Rich Harris, "Consumer Credit Giant Plans Major Restructuring," Associated Press, December 12, 1991.
28. "Credit Bill Gets Support," Reuters, October 28, 1991; "Credit Bureaus Back Reporting Act Revision," *The Chicago Tribune*, October 25, 1991, p. C3; "Equifax Testifies at Congressional Hearing on FCRA Reform," PR Newswire, October 24, 1991.
28. Hearing before the Senate Banking, Housing, and Urban Affairs Subcommittee on Consumer and Regulatory Affairs, October 22, 1991; Kathy M. Kristof, "Equifax Agrees to Reforms in Credit Reports: The Firm Will Also Pay $150,000 in the Agreement That Brings It in Line with Actions Forced on TRW," *Los Angeles Times*, July 1, 1992, p. D1.

30. Henry Gilgoff, "Credit Reporters Under Siege: Facing a Barrage of Criticism from Consumers, Information Companies Try to Stave Off Tighter Regulation," *Newsday,* January 26, 1992, p. 68.
31. Hearing before the Senate Banking, Housing, and Urban Affairs Subcommittee on Consumer and Regulatory Affairs, October 22, 1991; Kristof, "Equifax Agrees to Reforms in Credit Reports: The Firm Will Also Pay $150,000 in the Agreement That Brings It in Line with Actions Forced on TRW."
32. Albert B. Crenshaw, "Critics of Credit Reports Say House Bill Is Flawed: Backers Fighting Inclusion of Preemption Clause," *The Washington Post,* August 2, 1992, p. H3.
33. Anne Saker, "House Ready to Vote on Credit-Report Bill," Gannett News Service, August 4, 1992.
34. "American Financial Services Association Responds to Naag's Statements Regarding Preemption Provision in Credit Reporting Bill," PR Newswire, July 31, 1992.
35. "Consumer Groups Lobby to Preserve States' Rights to Regulate Credit Industry," States News Service, March 27, 1992
36. Sharyn Wizda, "Consumer Groups Criticize Barnard for Amendment to Credit-Reporting Bill," States News Service, March 27, 1992.
37. Crenshaw, "Critics of Credit Reports Say House Bill Is Flawed: Backers Fighting Inclusion of Preemption Clause."
38. Paul Kirby, "House Panel Amends Credit Reporting Bill," States News Service, March 25, 1992; Sharyn Wizda, "Consumer Groups Criticize Barnard for Amendment to Credit-Reporting Bill," States News Service, March 25, 1992.
39. Saker, "House Ready to Vote on Credit Report Bill."
40. Leonard Sloane, "Unraveling of Measure to Revamp Consumer-Credit Reporting," *The New York Times,* October 17, 1992, section 1, p. 34.
41. Tony Munroe, "Credit-Reporting Bill Introduced: Almost Mirrors Failed '92 Effort," *The Washington Times,* February 20, 1993, p. C5.
42. Robert M. Garsson, "Lenders Protest Credit Reporting Proposals," *American Banker,* October 27, 1993, p. 3.
43. Robert M. Garsson, "Fair Credit Reporting Bill Advances in House," *American Banker,* February 10, 1994, p. 3; "Feb. 9 Vote Sought on Fair Credit Act," *American Banker,* February 3, 1994, p. 3.
44. "Fair Credit Reporting Bill Passes, but Chances Are in Doubt," *American Banker,* March 4, 1994, p. 2.
45. Carrie Teegardin, "House OKs Bill Aimed at Making Credit Bureaus More Responsive," *The Atlanta Journal-Constitution,* June 14, 1994, p. F3.
46. Henry Gilgoff, Credit Report Bill Dies: Supporters Blame Gramm, *Newsday,* October 12, 1994, p. A41.
47. John Harwood, "Cash Machine: Candidate Phil Gramm Rarely Skips a Chance to Raise More Money; Dogged Fund Raising Boosts Texan's Hope of Winning Presidential Nomination; Always Time for Another Call," *Wall Street Journal,* February 17, 1995, p. A1.
48. The Center for Public Integrity, analysis of 1995-96 campaign finance records.
49. Interview with Evan Hendricks, June 8, 1998.
50. John McCormick, "New Laws on Credit Records Mean Big Changes," *The Des Moines Register,* October 1, 1997.
51. Letter from Robert Pitofsky to Senator Richard Bryan, September 20, 1996. Downloaded from www.ftc.gov.
52. Interview with Ed Mierzwinski, June 8, 1998.

53. Interview with Ed Mierzwinski.
54. Stephen Green, "Feinstein to Seek Tougher Privacy Laws: Co-Authors Bill Aimed at Curbing Commercial Use of Personal Data," *The San Diego Union-Tribune,* June 6, 1997, p. A2.
55. Interview with Ed Mierzwinski.
56. Ibid.

CHAPTER 3—AN UNLOCKED DOOR

1. Dana Hawkins, "A Bloody Mess at One Federal Lab: Officials May Have Secretly Checked Staff for Syphilis, Pregnancy, and Sickle Cell," *U.S. News & World Report,* June 23, 1997, p. 26.
2. Ibid.
3. Ibid.
4. Interview with Vicki Laden, July 9, 1998.
5. Dana Hawkins, "A Bloody Mess at One Federal Lab: Officials May Have Secretly Checked Staff for Syphilis, Pregnancy, and Sickle Cell."
6. Interview with Vicki Laden.
7. Dana Hawkins, "Court Declares Right to Genetic Privacy," *U.S. News & World Report,* February 16, 1998, p. 4.
8. Interview with Lynn Yarns, July 17, 1998.
9. Dana Hawkins, "Court Declares Right to Genetic Privacy."
10. Testimony and prepared statements of Bonnie Rogers, M.D., and Janlori Goldman before the Senate Committee on Labor and Human Resources, February 26, 1998.
11. Christine Gorman, "Who's Looking at Your Files? Prying Eyes Find Computerized Health Records an Increasingly Tempting Target," *Time,* May 6, 1996, p. 60.
12. "Congress Must Look at Protecting Privacy of All Medical Records," *Sun-Sentinel* (Fort Lauderdale), December 2, 1997, p. 16A; testimony of Senator Patrick Leahy before Senate Committee on Labor and Human Resources, October 28, 1997.
13. Gorman, "Who's Looking at Your Files?"
14. Andre Mouchard, "Under the Boss's Gaze: Does Big Brother Sign Your Paycheck? Workplace Privacy Is a Gray Area," *The Orange County Register,* April 22, 1996, p. D6.
15. Jay Greene, "Your Secret's Out: Your Medical Records—Perhaps Your Most Personal Information—Also Are the Most Vulnerable to Public Scrutiny," *The Orange County Register,* April 24, 1996, p. C1.
16. Nat Hentoff, "Privacy Law Exempts Police," *The Chattanooga Times,* November 3, 1997, p. A8.
17. Meredith Goad, "Losing Hold of Patient Confidentiality," *Portland Press Herald,* May 18, 1998, p. A1.
18. David Ress, "Leak Raises Privacy Issue: Insurance Worker's Release of Medical Records Points to Dangers in System," *The Richmond Times Dispatch,* March 3, 1996, p. E1.
19. Maggie Scarf, "Keeping Secrets," *The New York Times Magazine,* June 16, 1996, p. 38.
20. John Riley, "Open Secrets: Changes in Technology, Health Insurance Making Privacy a Thing of the Past," *Newsday,* March 31, 1996, p. A5.
21. Richard D. Lyons, "Insurance Data Called Faulty," *The New York Times,* October 4, 1973, p. 22.
22. Terence Hunt, no headline, Associated Press, June 28, 1979.
23. Louise Cook, no headline, Associated Press, May 30, 1978.
24. Richard D. Lyons, "Insurance Data Called Faulty."
25. Louise Cook, no headline, Associated Press, May 30, 1978.
26. Interview with James Corbett, vice president, medical Information Bureau, July 17, 1998.
27. Ibid.
28. Public Opinion Online, "Dimensions of Privacy," poll released January 1979.

29. Terence Hunt, no headline, Associated Press, May 30, 1978..
30. Janet Staihar, "Bill to Protect Patients' Privacy Approved," Associated Press, January 29, 1980; "House Kills Medical-Records Privacy Measure," Associated Press, December 1, 1980.
30. House bill H.R. 5831.
32. Judi Hasson, "Access to Medical Files Reform Issue," *USA Today*, July 27, 1993, p. A1.
33. Robert S. Boyd, "Medical Record Storage Brings Up Privacy Issues: Computers Files Are Easy Prey," *The Times-Picayune*(New Orleans), November 13, 1993, p. A6.
34. Hasson, "Access to Medical Files Reform Issue"; Boyd, "Medical Record Storage Brings Up Privacy Issues: Computers Files Are Easy Prey."
35. Bob Dart, "Workers Fret About Privacy in a New Health Care System," *The Atlanta Journal-Constitution*, August 19, 1994, p. C2.
36. Office of Technology Assessment, "Protecting Privacy in Computerized Medical Information," September 1993, p. 15.
37. Mitch Betts, "Health Reform Raises Privacy Issues," *Computerworld*, April 11, 1994, p. 55.
38. Robert M. Gellman, "Can Privacy Be Regulated Effectively on a National Level?," October 20, 1997, p. 5. Paper delivered at Georgetown University Law Center symposium "Privacy at the Crossroads: Law, Technology, and Public Policy." Downloaded from www.epic.org/events/privacy-gulc.
39. Senate bill S. 1360.
40. "Bill Sets Privacy Standards Similar to Industry Programs," *Strategies for Healthcare Executives*, November 2, 1995; "AHIMA Patient Privacy Rights Protected in Medical Records Confidentiality Act of 1995," PR Newswire, October 24, 1995.
41. "Medical Privacy Bill Awaits Action in Early 1996," *Washington Health Week*, January 1, 1996; Gina Kolata, "Firms Trading in Private Medical Records: Senators Call for Rules on Data's Use and Disclosure," *The New York Times*, November 15, 1995, p. A1; Mitchel E. Ostrer, "An Inexpensive Reform: The Medical Records Confidentiality Act," *New Jersey Law Journal*, July 8, 1996, p. 11.
42. "House Kills Medical-Records Privacy Measure," Associated Press, December 1, 1980.
43. Senate bill S. 1360; Ostrer, "An Inexpensive Reform: The Medical Records Confidentiality Act."
44. John Riley, "Open Secrets: Your Medical Records: Will Bill Cure Ills? Legislation on Access to Medical Data Sparks Debate," *Newsday*, April 3, 1996, p. A8.
45. Gorman, "Who's Looking at Your Files?"
46. Ostrer, "An Inexpensive Reform: The Medical Records Confidentiality Act."
47. Alison Bass, "Privacy of Medical Records Is an Issue for Lawmakers in the Information Age," *The Boston Globe*, November 4, 1995, p. 1.
48. The Center for Public Integrity, analysis of 1996 lobbying disclosure records.
49. "Revised Confidentiality Act Due Soon," *Medicine & Health*, May 27, 1996.
50. Ibid.
51. Brenda Paik Sunoo, "Business-Friendly Bills—At Last!," *Personnel Journal*, October, 1996, p. 76; "Privacy Rites," *The Courier-Journal* (Louisville), March 8, 1997, p. A6.
52. John Schwartz, "Health Insurance Reform Bill May Undermine Privacy of Patients' Records," *The Washington Post*, August 4, 1996, p. A23.
53. Richard L. Clarke, "Medical Records: Privacy Ensured" (Letter to the Editor), *The Washington Post*, August 27, 1996, p. A10.
54. Schwartz, "Health Insurance Reform Bill May Undermine Privacy of Patients' Records."
55. Jonathan Riskind, "Lawmaking Follows a Long and Winding Road: A Bill's Journey Is Rarely Simple, Direct in Congress," *The Columbia Dispatch*, August 5, 1996, p. 1A.
56. Interview with Dean Rosen, September 25, 1997.

57. Beverly Woodward, "Intrusion in the Name of 'Simplification,'" *The Washington Post*, August 15, 1996, p. A19.
58. Interview with Greg Moody, September 27, 1997.
59. The Center for Public Integrity, analysis of 1995-96 campaign finance records.
60. "The Race Is On to Influence the Rules Needed to Make Kassebaum-Kennedy Work," Financial Service Online, September/October 1996.
61. Mary Agnes Carey, "Health Care Industry Opposes Privacy Bill," *The Plain Dealer* (Cleveland), August 27, 1997 p. A19.
62. Written testimony of Dr. Sherine Gabriel, on behalf of the Healthcare Leadership Council, hearing before the House Government Reform and Oversight Subcommittee on Government Management, Information, and Technology, June 5, 1997.
63. Hearing before the Senate Committee on Labor and Human Resources, February 26, 1998.
64. "Congress Must Look at Protecting Privacy of All Medical Records," *Sun-Sentinel* (Fort Lauderdale), December 2, 1997, p. A16.
65. Margo D. Beller, "Groups Applaud Recommendations Protecting Medical Record Privacy," *Journal of Commerce*, October 30, 1997, p. A11.
66. Jerry Geisel, "Administration Leaves Rules on Record Privacy to Congress," *Business Insurance*, September 22, 1997, p. 2.
67. "Feds Pulled a Fast One on Public in Issuing Medical Privacy Rules," *The Daily Record* (Baltimore), October 8, 1997, p. 13.
68. Statement of Senator Patrick Leahy, hearing before the Senate Labor and Human Resources Committee, February 26, 1998.
69. "Privacy Protection Bill Needs Some Modifications," *National Underwriter*, April 27, 1998, p. 52.
70. "Privacy Bill Key Issue for Alliance in 1998," *BestWire*, April 29, 1998.
71. "Privacy Protection Bill Needs Some Modifications."
72. Marilyn Werber Serafini, "Medical Privacy in the Information Age," *National Journal*, April 18, 1998.
73. Lizette Alvarez, "Congressman Sues a Colleague Over Disclosing GOP Talks," *The New York Times*, March 9, 1998, p. A16.
74. "Senator James Jeffords (R-VT) and Senator Christopher Dodd (D-CT) News Conference Re: Medical Records Confidentiality," Federal News Service, April 3, 1998.
75. Statement of Senator Patrick Leahy, hearing before the Senate Labor and Human Resources Committee, February 26, 1998.

CHAPTER 4—THE WATCHFUL EYE

1. Interview with Gail Nelson, July 9, 1998.
2. Interview with Jeffrey Feuer, July 9, 1998.
3. Office of Technology Assessment, "The Electronic Supervisor: New Technology, New Tensions," 1987, p. 15.
4. Sara Eckel, "Orwell Didn't Anticipate Big Business New Technologies Make Watching," *Sacramento Bee*, December 1, 1997, p. B7.
5. Lewis L. Maltby, testimony to House Education and Labor Subcommittee on Labor-Management Relations, June 30, 1993.
6. Office of Technology Assessment, "The Electronic Supervisor: New Technology, New Tensions," p. 19.
7. Ibid., p. 98.
8. Ibid., pp. 17-19.

9. Privacy Protection Study Commission Report, p. 223. Quoted in testimony by Marc Rotenberg, Computer Professionals for Social Responsibility, to Senate Labor and Human Resources Subcommittee on Employment and Productivity," September 24, 1991.
10. John Yoch, "Employee Privacy: Is Law Needed?," *American Banker*, February 25, 1980.
11. Ibid.
12. Nancy L. Ross, "Poll Finds Little Progress on Privacy," *The Washington Post*, July 28, 1979, p. C11.
13. "Privacy in the Computer Age," *The Washington Post*, April 21, 1989, p. A26.
14. Ann Crittenden, "Experts Find Abuse of Employee Rights," *The New York Times*, June 20, 1980, p. 10.
15. Office of Technology Assessment, "The Electronic Supervisor: New Technology, New Tensions," p. 85.
16. Ibid., p. 93.
17. Ibid.
18. Ibid., pp. 134-135.
19. Ibid., p. 104.
20. Ibid., p. 14
21. Rorie Sherman, "Polygraph Suits? That's No Lie: New Act Sure to Spur Litigation," *The National Law Journal*, September 5, 1988, p. 3.
22. J.R. Anderson, "No One Cares If It's True: Background Checks Have Little Limit," *Newsday*, December 9, 1991.
23. Charles Piller, "Bosses with X-Ray Eyes," *Macworld*, July 1993. Appended to testimony before the Senate Labor and Human Resources Subcommittee on Employment and Productivity, June 22, 1993.
24. Michael J. Smith et al., "Electronic Performance Monitoring and Job Stress in Telecommunications Jobs," unpublished paper, Department of Industrial Engineering, University of Wisconsin at Madison, 1990.
25. Prepared statement of Cindia Cameron before the Senate Labor and Human Resources Committee, September 24, 1991.
26. Testimony of Renee Maurel before the Senate Labor and Human Resources Subcommittee on Employment and Productivity, September 24, 1991.
27. Office of Technology Assessment, "The Electronic Supervisor: New Technology, New Tensions," p. 46.
28. Ibid., p. 47.
29. Ibid., p. 47.
30. Ibid., p. 109.
31. Letter to the Center for Public Integrity from Jim Dempsey, senior staff counsel, Center for Democracy and Technology, July 1, 1998.
32. OTA, p. 109.
33. Ibid.; Michael G. Radigan, "Respecting Privacy Rights of Employees," *New York Law Journal*, February 18, 1997, p. S4.
34. R.J. Ignelzi, "Under Scrutiny: E-Mail, Phone Calls, Voice Mail Legally Can Be Monitored by Boss," *The San Diego Union-Tribune*, July 3, 1995, p. D1.
35. Senate bill S. 516.
36. Senator Paul Simon, statement to Senate Labor and Human Resources Subcommittee on Employment and Productivity; statements by other witnesses (Cindia Cameron, Vincent Roffolo, Lawrence Fineran, etc.) analyzing the legislation.
37. House bill H.R. 1218.

38. Lawrence Fineran, testimony to Senate Labor and Human Resources Subcommittee on Employment and Productivity, September 24, 1991.
39. Paul S. Brown, "Protecting Employer Rights: RIMS Defends Legitimate Use of Surveillance," *Risk Management,* April, 1997, p. 100.
40. Representative Pat Williams, statement before the House Education and Labor Subcommittee on Labor-Management Relations, June 30, 1993.
41. Statement of Household Finance Corporation before the House Education and Labor Subcommittee on Labor-Management Relations, June 30, 1993.
42. Letter from Marc E. Lackritz, Securities Industry Association, to Representative Marge Roukema, June 21, 1993.
43. Statement of Associated Builders and Contractors before the House Education and Labor Subcommittee on Labor-Management Relations, June 30, 1993.
44. Written testimony by James Royer before the House Education and Labor Subcommittee on Labor-Management Relations, June 30, 1993.
45. Representative Marge Roukema, testimony before the House Education and Labor Subcommittee on Labor-Management Relations, June 30, 1993.
46. The Center for Public Integrity, analysis of 1988-96 financial disclosure records.
47. Representative Peter Hoekstra, statement before the House Education and Labor Subcommittee on Labor-Management Relations, June 30, 1993.
48. Senator Strom Thurmond, opening statement, hearing before the Senate Labor and Human Resources Subcommittee on Employment and Productivity, June 22, 1993.
49. Stephanie Armour, "Watch Out—'Big Brother' Might Just Be Watching You," Gannett News Service, February 1, 1998
50. L.A. Lorek, "Software Programs Give Big Boss Chance to Be Big Brother, *Sun-Sentinel* (Fort Lauderdale), February 1, 1998, p. 4F
51. Dan Balaban, "Personality Testing Is Catching On Among U.S. Businesses: Some Experts Worry That Employers Place Too Much Importance on Results," *Kansas City Business Journal,* May 2, 1997, p. 6; Peggy Schmidt, "Lie-Detector Tests in a New Guise," *The New York Times,* October 1, 1989, section 3, p. 29.
52. Office of Technology Assessment, "The Use of Integrity Tests for Pre-Employment Screening," September 1990, p. 10.
53. "Assembly Will Vote on Anti-Peeping Bill," Capitol Alert News Service, May 19, 1998.

CHAPTER 5—THE DATA OCTOPUS

1. Senator Dianne Feinstein, introductory remarks on the Personal Information Privacy Act of 1997, *The Congressional Record,* June 10, 1997.
2. Elizabeth Corcoran, "FTC Seeks Credit Agency Access Limits: On-Line Privacy Fears Behind Agency's Move," *The Washington Post,* September 24, 1996, p. A5; "FTC Backs Consumers in Privacy Flap," Bloomberg Business News, September 24, 1996; "FTC Recommends That Congress Change the Law to Provide Additional Confidentiality Protections for Consumers," Federal Trade Commission press release, September 24, 1996.
3. Letter from Lance Clem to Senator Alan Dixon, October 3, 1991, included in hearing before the Senate Banking, Housing and Urban Affairs Subcommittee on Consumer and Regulatory Affairs, October 22, 1991.
4. General Accounting Office, "Identity Fraud: Information on Prevalence, Impact, and Internet Role Is Limited," p. 39.
5. Ibid., pp. 3-4.

6. Representative Jerry Kleczka, introductory remarks on the Personal Information Privacy Act, *The Congressional Record*, June 10, 1997.
7. Robert O'Harrow, Jr., and John Schwartz, "A Case of Taken Identity: Thieves with a Penchant for Spending Are Stealing Consumers' Good Names," *The Washington Post*, May 26, 1998, p. A1.
8. General Accounting Office, "Identity Fraud: Information on Prevalence, Impact, and Internet Role Is Limited," May 1998, p. 49.
9. Ibid., pp. 3-4.
10. Ibid., p. 5.
11. Ibid., p. 57.
12. Interview with Evan Hendricks, June 8, 1998.
13. Marcy Gordon, "Bonanza for Big Brother: Privacy in Peril, House Panel Told," *The Record* (Bergen County, New Jersey), September 19, 1997, p. B1.