1990

Information Systems and the Erosion of Personal Privacy

Scott D. Sterner

Report Number:
90-980

INFORMATION SYSTEMS AND THE EROSION OF PERSONAL PRIVACY

Scott D. Sterner

CSD-TR-980
May 1990

Information Systems and the Erosion of Personal Privacy

Scott D. Sterner

April 26, 1990

Purdue Technical Report CSD-TR-980

Abstract

Financial records, medical records, corporate personnel files, police records, and many other types of data are kept on most Americans and are stored in computerized systems. The potential of misuse of the information stored on these systems has caused concern in the minds of some. Unfortunately, the abuse of this information already occurs in very real and far-reaching ways. Improper employment practices, dissemination of personal information, and even surveillance of private citizens through the abuse of these systems have become all-too-common events in America today.

This paper studies both the potential for information abuse and cases where abuses of this sort already occur. Possible solutions to this problem, as suggested by various authorities, are also surveyed. The primary purpose of this report is to create a greater awareness of the current lack of personal information privacy.

This paper was derived from a class project for CS 590s, taught by Professor Eugene Spafford at Purdue University in the Spring of 1990.

Introduction

Financial records, medical records, corporate personnel files, police records, and many other types of data are kept on most Americans and are stored in computerized systems. The potential of misuse of the information stored on these systems has caused concern in the minds of some. Unfortunately, the abuse of this information already occurs in very real and far-reaching ways. Improper employment practices, dissemination of personal information, and even surveillance of private citizens through the abuse of these systems have become all-too-common events in America today.

There is a need for greater awareness of this problem and of how the government allows (and in some cases encourages) abuses of personal information to occur. Once one understands the problem, then one can attempt to find a solution, if indeed a solution exists.

Financial Privacy

A man and his wife went to an unfamiliar auto dealership to shop for a car. A salesman talked with them for 10 minutes and then went into his office for a brief period of time. When he returned, he offered to sell the car to the man with no further questions.

When the man asked how the salesman could trust a purchaser with a new car simply on his signature, the salesman escorted the man to his office. There he typed the man's name into a computer terminal on his

desk, and instantly the customer's full credit, financial, and earnings history appeared on the screen [Linowes, p. 126].

Stories like this are not uncommon. In fact, many companies use such systems, provided by consumer reporting bureaus, to learn of a customer's complete financial history. Many would find this relative ease shocking (as did the customer in this story), but it is fairly common today. Such reporting agencies have existed for many years, but it is only through the advent of the computer that they can produce results so quickly. "The five largest credit reporting companies in the United States maintain in their computers more than 150 million individual credit records." This information includes "full name, Social Security number, address, telephone number, name of spouse, place of work, salary, other sources of income, names of credit grantors, complete payment history, arrest and conviction records, bankruptcies, tax liens, and lawsuits" [Burnham, p. 42]. Anyone who uses a credit reporting agency can gain access to some or all of this information on anyone whose records are filed with this company. Since so many people have such access, it would not be difficult for an individual to ask a friend or co-worker to ask the credit reporting company for any desired information. In this way, any fact in the above list that is known about another person can be found out with little fear of detection or punishment.

This kind of information is not always correct, though, which is not surprising considering the number of people documented by these services. Consider the case of Lucky Kellener of Los Angeles. In 1978 he paid his brother's rent. When his brother was evicted several months later, Kellener's name was (inadvertently) included in the court papers. U. D.

Registry, a credit reporting agency, entered this incorrect listing in its records on Kellener, identifying him as an "undesirable tenant." Three years later, when trying to find a larger apartment, Kellener was coldly refused by three apartment houses before he learned of his "blacklisting" [Burnham, pp. 34-35].

In another Los Angeles case involving U. D. Registry, Barbara Ward was also unable to rent an apartment. When she found that her first apartment was infested with cockroaches and run by a landlord who refused to exterminate them, she tried to move. For revenge the landlord attempted to have her evicted. The landlord did not appear at the hearing, so the judge ordered the case off the calendar. However, because she once had received an eviction notice, she was unable to find another apartment several years later [Burnham, p. 35].

One of the largest credit record bureaus is TRW. It currently sells 35 million credit reports a year to 24,000 subscribers nationwide. Approximately 90 million customers have records stored in TRW's gigantic computer system (the largest single commercial concentration of computers in the world). Needless to say, a company of this size could not function efficiently if it bothered to double-check all of its information. As a result, about 350,000 individual subjects register formal complaints with TRW's consumer relations department about the inaccuracy of their reports [Burnham, pp. 44-45]. Considering the desire of most people to avoid unnecessary paperwork, one must wonder how often inconsistencies in records are not reported (not to mention how often errors in records are not even detected).

Several states have created laws to protect consumers from privacy

violations of their financial records. Forty-five states have "statutory recognition of financial privacy," and nine have "legislation regulating the disclosure of an individual's financial records." California has legislation requiring that a bank customer be given a 10-day notice before a state investigator can obtain records of the customer's financial transactions at that bank. Alabama statutes require that financial records be surrendered at the request of a government agency or under court order. Alabama law does note that these records should only be disclosed upon legal process. Other similar statutes exist, but most (like these) only protect the customer from disclosure of his bank transactions [Linowes, pp. 111-112]. Other financial records do not have such protections. In fact, even the statutes protecting bank records may not be adequate. In United States v. Miller (1976), the Supreme Court ruled that a customer's records are not owned by him but rather by the bank (Miller's bank records had been subpoenaed without his knowledge) [Burnham, p. 168].

Most people believe that such records, particularly bank records, cannot be disclosed to anyone without their express permission. Even those who are aware of disclosures seldom realize how many people have access to their records and how quickly these records can be obtained with current computer networking technology. Perhaps there will not be widespread complaint about these practices until many people have been approached by others with information about themselves that they believed was private.

Privacy of Medical Records

"A middle-aged woman, hospitalized for a tumor, learned that it was

malignant and began receiving chemotherapy treatments. Returning to work a few weeks later, she was edgy, anxious, and extremely sensitive regarding her condition. She did not want others to know about her illness fearing they would treat her as an object of pity. Yet on her very first day back at work following her confinement she was stopped on the way to her desk by a sympathetic co-worker. 'I'm so sorry to hear you have cancer,' the other employee remarked.

"The patient's medical record was on file in the personnel office because the employer administered a group health policy. Easily accessible, the entire staff learned of her condition" [Linowes, p. 120].

Cases like this are not rare. Medical information is often used in employment-related decisions. The idea that a person's medical records are private dates back many centuries. It is surprising that such an ancient notion could be so easily and inobtrusively cast aside for the sake of "effective decision making." Instances where employee medical records are known by co-workers are most common in companies that have group medical benefits.

These information releases are justified by insurers because "we are obligated to tell the employer because he pays the premiums." However, since the insurance is for a group medical plan, the premiums are paid by the workers, and the employer is only a middleman in the payment transaction. Thus there is no reason for an employer to see data on specific employees. Another consideration is that, in cases where psychiatric care is administered, patients may avoid further treatment because of fear that their problems will be revealed in detail to co-workers (a common occurrence) [Linowes, p. 120].

The most unfortunate aspect of improper medical information releases is that they could be easily avoided at no harm to the company. By bypassing a company's personnel office and sending claims directly to the carrier's office (where those who see the information are not co-workers of the patient and are instructed not to reveal medical information), only those who pay for the claims need know of their purpose [Linowes, p. 122].

The view held by many employers that every aspect of an employee's life should be examined when making hiring and career decisions about that employee encourages these kinds of privacy violations. If an employer wants to know why an employee went to see a psychiatrist, why doesn't he just ask him? If the employee refuses to answer, and there has been no negative change in his work performance, why question it? Many proponents of these measures consider their intrusion to be valid because they "head off future problems." In fact, they may cause more harm to their company than they prevent because of the loss of employer/employee trust. The desire of some employees to avoid necessary medical treatment in order to maintain their personal privacy can become a major problem.

Corporations and Employee Privacy

John, a 20-year employee and executive vice-president of a company, was first in line to replace the soon-retiring president. To his (and others') surprise, the second vice-president was chosen, despite his inferiority to John in experience and credentials. After attempts to learn the explanation of this decision failed, he hired a lawyer who subpoenaed the files of the selection committee. In those files was a copy of John's medical records. In a noted section, his personal doctor

wrote that the "patient seems to have trouble managing his finances." This was written at a time when John was having persistent headaches, and his doctor was examining the possibility of stress as a cause. When the selection committee read this remark, they concluded that if John was incapable of handling his own finances, he could not be trusted with the company's.

John was unable to get the president's job, but he was able to explain this remark to others in the future [Linowes, p. 27]. He had assumed that his records were private, and even then did not know their contents. This is one of many examples where seemingly the only person who does not possess a piece of information is the person who the information is about.

In Chicago, one woman was repeatedly refused government employment because of a note in her grammar school records. "Her third grade teacher carelessly wrote on a report that the woman's mother was crazy" [Linowes, p. 23]. This is a slightly different kind of computer record abuse. In this case, the potential employer put too much emphasis on third-hand, questionably reliable information that was not directly related to the employee. Perhaps this is similar to cases of people believing in their computers too much. The idea that "if the computer said it, then it must be right" is hardly new, but as computers are used to manage greater amounts of personal data, this blind faith in their "omniscience" becomes a much greater threat to personal privacy.

In the early 1970's, Richard Schwartz and Jerome Skolnick, both sociologists, performed a study on the effects of such information on hiring practices. They showed employment files on 100 men being considered for a menial job to a group of employers. Each of these hundred

men belonged to one of four groups. In one group, the men had no criminal records. A "second group had each been arrested for assault and acquitted of the charge with a letter from the judge explaining the presumption of innocence." The third group "had been arrested for assault and acquitted, but there was no letter from the judge. The fourth group had been convicted."

When "asked whether they would be willing to offer the individuals in each group a job," "36 percent said they would hire the men with no record, 24 percent said they would hire the men who had been acquitted and had a letter from the judge, 12 percent said they would hire the men who had been acquitted but had no letter, and four percent said they would hire the men who had been convicted" [Burnham, pp. 79-80].

Many similar studies demonstrate the same principle: the appearance of criminality in any form, even without a conviction, is appropriate reason for refusing employment. Apparently the American legal notion that a person is innocent until proven guilty is not held in high regard by many employers.

Another study conducted at the University of Illinois examined many facets of personal information and its use by corporations. One hundred twenty-six Fortune 500 companies took part in the study. Responses of note include the following: 38 percent "do not have a policy concerning which records are routinely disclosed to inquiries from government agencies;" 80 percent "disclose personal information to credit grantors;" 43 percent "inform personnel of the types of records maintained;" 41 percent inform on how records are used; 42 percent consider it "necessary to collect information without informing the individual" [Linowes, pp. 40-41].

Although such policies are not always adhered to, they can be an effective means of curbing privacy violations in the workplace. Ford Motor Company's "Fair Information Practice Principles" [Linowes, p. 31] is an excellent example of what a corporate privacy standard should be like. (This standard is too long to be reprinted here, but interested readers are encouraged to use the Ford example as a model of what can be done.)

Privacy and Law Enforcement

Michael Ducross was stopped by police on 24 March 1980 for making an illegal left-hand turn near his home in Huntington Beach, California. The officer ran a check on Ducross using the FBI's National Crime Information Center, a computer-operated crime data system in Washington, D.C. The computer responded that Ducross was wanted for being AWOL from the Marine Corps since Christmas Eve of 1969. Ducross was taken to the brig at Camp Pendleton. He was held for five months before the Marine Corps dropped the charges. Ducross had never been AWOL. He left the Marines "under a special discharge program available to foreign citizens and Native Americans" (Ducross is a Canadian-born Indian) [Burnham, pp. 33-34].

Law enforcement examples of the effects of erroneous data are the most commonly used when discussing privacy issues. Most people are familiar with tales of mistaken identity, but cases like this one, where the information stored on a person is simply incorrect, are becoming more and more common. At the heart of virtually all of these stories is either the FBI itself, or the crime data systems the FBI operates. Not only is the FBI a culprit in many cases of "data botching," but their use of the

databases of other government agencies, each with many faults as well, multiplies the problem.

Coupled with this are the FBI's persistent efforts to create a national network of crime information, so that it would not have to go through other agencies to gain access to personal data. There is some indication that such a system could be constructed in the all-too-near future. Attorney General Edward Levi and Attorney General Griffin Bell found three major concerns that prompted them to stop the construction of this system. First, who should control the network? Second, will the variation in state laws and local policies and the often inaccurate nature of the records reduce a person's chances for a fair trial? And third, "could such a system be used to keep track of American citizens who are not criminals?" [Burnham, pp. 64-64]

Others have suggested that the data system would not even by very effective in fighting crime. As explained by the supervisor of a burglary section in a large California city, "The idea that a national rap sheet system would make an important contribution to our work here is just a bunch of baloney. Our problem is not to find out who the guy is. Our biggest problem is once we catch him coming out of a house with the goods, how do we keep him in jail and how do we make sure he stays in jail. If anything, we have over-information-oriented and over-computerized this department. The patrol officer learns to use the vast array of information resources at his command, which means you learn to sit in a car and punch in the numbers of people's license plates and the numbers of people's driver's licenses. What this does is inhibit the development of traditional police skills, of interviewing, interrogating, and investigating.

We need people to get out of their offices and get out of their cars and talk to people. Most of our leads come from citizens reporting a crime or having heard about a crime. Without these resources, which have nothing to do with computers and criminal histories, we would be dead" [Burnham, p. 72].

"Based on detailed interviews with criminal justice decision makers at local and state levels, a national [computerized criminal history] system as currently conceived would bring about little or no measurable change in the decision-making process of police, prosecutors, criminal court magistrates, and probation/parole personnel. The promised public benefit of a national criminal history system appears to be nonexistent. On the other hand, a national [computerized criminal history] system would have a great impact on organizational decision making in the public and private employment areas. There is considerable evidence that employers will take very seriously the fact that an employee has a criminal history record" [Laudon, p. 325].

"Contrary to popular belief and what the police sometimes contend, research indicates that very few arrests are the result of any kind of investigation at all" [Burnham, p. 70]. Some also suggest that the only changes in the abuse of personal privacy since the pre-computer days are that searches can be done more quickly and that people are more aware of what the government can find out about them and how the government does it.

What defense does the citizen have against inaccurate information in police records becoming public and damaging his reputation? Unfortunately, it does not appear that he has much of any. For example, there is the

Supreme Court case of Paul v. Davis.

Edward Charles Davis III was arrested for shoplifting on 14 June 1971 and pled not guilty. Seven months later, he found that the police had given a five-page flyer to 400 local merchants naming Davis and others as "known shoplifters." The case against Davis was dismissed shortly after this list was distributed.

"Davis sued the police in federal court for violating his right to due process by publicly branding him a criminal without a trial." The Supreme Court determined that "every defamation by a public official" of a private citizen is not a "depravation of liberty" in regard to due process [Burnham, p. 171].

This case sets the precedent that, essentially, law enforcement officials, even at the local level, do not need proof of a crime to attach a warning label of "potential criminal" to a person's record. The implications of this are staggering. Potentially, such a precedent could be used to allow abuses ranging from local embarrassment of a personal enemy to nationwide persecution of a particular group of people within society. Such actions would certainly not be new, as will be discussed later. However, one would have thought that a nation built on the principle of personal liberty would advance in the protection of its individuals from a potential police state rather than encourage such a state to develop.

Government and Personal Privacy

Irwin Blye, the head of a New York City investigative firm, was given the challenge of learning all he could about an individual without ever even speaking to him. For his usual fee, Blye produced a standard five-

page (single-spaced) report on the man (a New Jersey newspaperman) and his background, including his father's income before his retirement. All of this information was found legally, although not all of it was correct.

Blye also has called banks and by "sounding knowledgeable" was able to discover a customer's complete bank record. This, too, is perfectly legal [Linowes, p. 159].

Why can an ordinary citizen gain access to so much information about others? This question is often asked in cases such as this. Unfortunately, most people overlook a greater question. If a private citizen can legally learn a person's address, occupation, and financial information, what does the government know about this person?

Anyone who does not believe that the government can easily track them down is either uninformed or naively patriotic. The IRS has a program that tracks down parents who do not pay their court-ordered child support using various federal data systems. "For 1981 returns filed in 1982, the IRS used its computers to prevent the distribution of $168 million in refunds scheduled to go to 275,479 delinquent parents" [Burnham, p. 32]. The program, which began in California, works by giving refunds due to delinquent parents to their children instead.

The Federal Child Support Enforcement Office works along a similar line. According to Louis Hays, the director of the Office, in about one year "the states asked us for address information on 200,000 individuals. We put those names on magnetic tapes and periodically submitted them to the Internal Revenue Service, the Social Security Administration, the Defense Department, the Veterans Administration, and the National Personnel Record Center." The Office then sends the information back to the states.

Hays also has said that it is easy to find the delinquent parents. Getting them to pay is the difficult part of the process [Burnham, p. 31].

The government has many other beneficial programs that use the power of computers to save money and increase effectiveness. "Computer matching covers many processes used to detect payment errors, increase debt collection, and identify abusive grant or procurement practices. The Department of Education, for instance, uses computer matches to identify federal workers who default on student loans. The National Science Foundation screens research fund applicants against its employee and consultant lists to prevent any conflict of interest in grant awards" [Kusserow, p. 542].

"The federal Department of Health and Human Services uses matches to unearth doctors who are double-billing Medicare and Medicaid for the same service. Over 230 problem health providers were removed from participation in the Medicare program in [1984]--a 253 percent increase over the previous year. [They] have also matched the Social Security benefit rolls against Medicare's record of deceased patients and discovered thousands of cases of administrative error and fraud. This project alone resulted in savings of over $25 million" [Kusserow, p. 542]. "Computer matching and other innovative techniques helped [the federal Department of Health and Human Services] identify $1.4 billion in savings--about a 300 percent increase over the previous year" [Kusserow, p. 542].

Indeed, computer systems do serve many good purposes. In just the case of computer matching, these systems can be used for: "assuring that ineligible applicants are not given costly program benefits; reducing or terminating benefits for recipients who are being paid erroneously; detecting fraudulent claims and deterring others from defrauding the pro-

gram; collecting overpayments or defaulted loans more effectively; monitoring grant and contract award processes; improving program policy, procedures, and controls" [Kusserow, p. 543].

Louis Hays, like most government officials, does not believe that these systems could be used for mass tracking of people or civil rights abuses by the government. Unfortunately, such violations of proper information use have already occurred several times in U. S. history.

In 1942, when the internment of Japanese Americans began, the government asked the Census Bureau to provide information on the names and addresses of all Japanese Americans living on the West Coast. Most Americans are led to believe that such information is confidential. In fact, the Bureau's own legal charter states that "in no case shall information furnished under the authority of this act be used to the detriment of the person or persons to whom such information relates." Indeed, the Census Bureau has since denied that it has ever given out specific names and addresses. For the most part, this has been true, although during World War I they did help the government track down draft dodgers with such data. In the case of the Japanese Americans, however, the Census Bureau only provided aggregate information (except in one instance, when under pressure from the military the Bureau did give out specific names and addresses). At that time, Bureau officials would "lay out on a table various city blocks where Japanese lived and then would tell...how many were living in each block" [Burnham, pp. 23-24]. The rest was up to the military, and history shows how effective they were at their work.

Under President Johnson, army intelligence agents "monitored the membership and policies of peaceful organizations who were concerned with

the war in Southeast Asia, the draft, racial and labor problems, and community welfare" [Burnham, p. 36]. "Christopher H. Pyle, a former Army intelligence officer has revealed: 'The Army maintains files on the membership, ideology, program, and practices of virtually every activist political group in the country. These include not only such violence-prone organizations as the Minutemen and the Revolutionary Action Movement (RAM), but such non-violent groups as the Southern Christian Leadership Conference, Clergy and Laymen United Against the War in Vietnam, the American Civil Liberties Union, Women Strike for Peace, and the National Association for the Advancement of Colored People'" [Miller, p. 40].

"Out of this surveillance, the army created blacklists of organizations and personalities which were circulated to many federal, state, and local agencies that were asked to supplement the data provided. Not only descriptions of the contents of speeches and political comments were included, but irrelevant entries about personal finanaces, such as the fact that a militant leader's credit card was withdrawn. In some cases, a psychiatric analysis taked from the army or other medical records was included" [Burnham, p. 36].

Our future may be seen in the actions other nations have already taken to abuse information systems for purposes of "improving their country." In 1982, a Norwegian research project studied "police files, school records, and health data to identify small children with potential psychological problems that might lead to later antisocial activities" [Gray, p. 251].

In the time it takes to get a cup of coffee, the government can learn a wealth of information about many members of our society. Most people

realize that they are on file with agencies such as the Social Security Administration, but the existence of many other government records on them is not as well known. "For example: if you are an executive in a company that has military contracts, you are probably on file with the Defense Intelligence Agency; if your child ever applied for a student loan, you are probably on file with the Department of Education; if you were involved in a banking transaction exceeding $10,000, the Treasury Department has you on file; if you are a corporate officer, the Securities and Exchange Commission has a business profile on you; if a teenager in your family ever faced a drug or similar charge, the details are probably on file with the Justice Department; if you made a political contribution of $100 or more, a record on you is kept with the Clerk of Congress or Federal Election Commission" [Linowes, p. 82].

The fact that the government has all of this information and uses it is more disturbing when one remembers the inaccuracy of their data. One study of the National Crime Information Network Computerized Criminal History system found that 54.1 percent of the records had some "significant quality problem." FBI Ident records had quality problems in an almost unbelievable 74.1 percent of all records [Gray, p. 249]. Couple this with the fact that 95 percent of all working Americans work for corporations, 66 percent have life insurance, and 90 percent are covered by health plans [Burnham, p. 49], the wealth of information on the life and livelihood of most Americans is astounding. Even more worrisome is the fact that most maintainers of these systems are more than happy to comply with requests for information made by government agencies, particularly the FBI.

A new term was even coined to describe this kind of surveillance:

dataveillance. It is described as "the systematic use of personal data systems in the investigation or monitoring of the actions or communications of one or more persons" [Clarke, p. 499]. It should be clear that dataveillance and other forms of privacy violations will eventually begin to affect the way society operates (if it has not already). In his paper on dataveillance, Roger Clarke suggests several possible effects of these policies and procedures that are well worth examining. In his list of threats to society he offers: establishment of a "prevailing climate of suspicion;" development of "adversarial relationships;" shifting the "focus of law enforcement" to "easily detectable and provable offenses" (which arguably is already happening); "inequitable application of the law; decreased respect for the law; reduction in the meaningfulness of individual actions; reduction in self-reliance and self-determination; stultification of originality; increased tendency to opt out of the official level of society; weakening of society's moral fiber and cohesion; destabilization of the strategic balance of power;" and "repressive potential for a totalitarian government" [Clarke, p. 505]. If these potential effects seem extreme and unlikely, perhaps our understanding of the extent of current dataveillance is insufficient. As David Burnham writes, "Does not surveillance, even the innocent sort, gradually poison the soul of a nation? Does not surveillance limit personal options for many individual citizens? Does not surveillance increase the powers of those who are in a position to enjoy the fruits of this activity?" [Burnham, p. 47]

What about the Privacy Act of 1974? Does it offer any real protection from dataveillance? Not necessarily. Although it attempts to "define individual rights in relation to stored data," it is generally not enforced

[Gray, p. 244]. "The political milieu which favored passage of the Privacy Act of 1974 has changed and is not supportive of (these) proposals" [Laudon, p. 400]. It has become a sort of privacy "jaywalking" law. It will only be used either in extreme cases, or to exact revenge on someone for harboring disrespect for authority.

The main shortcomings of the Privacy Act are well known.

"1. It fails to provide for an independent enforcement mechanism, a Privacy Protection Commission.

2. It vests enforcement of the act with individuals who may recover actual damages by bringing civil suits if a government agency willfully and intentionally violates the act.

3. The act provides no recourse to individuals whose records have been abused by virtue of incompetence, error, and mistake.

4. It fails to provide concrete guidelines or general performance criteria for the development of new systems and the enhancement of existing systems.

5. It fails to prevent because of ambiguous language the development of general purpose, national information systems capable of widespread social surveillance"

[Laudon, pp. 374-375].

In the case of IRS information, the courts have ruled that "Fifth Amendment protections do not prevent prosecution if an individual violates IRS filing requirements" [Gray, p. 247]. Although the IRS occasionally denies requests for information that are made by other government agencies, in most situations it honors these requests.

Many people argue that such information only affects "wrongdoers" and is needed by the government to do its job, particularly in the area of law enforcement. But the potential for widespread abuse cannot be denied.

"Effective merging of data files can tell [the government] with great accuracy what people do and where (previously requiring physical surveillance) and what they think, read, and express (previously requiring electronic surveillance)" [Laudon, p. 380].

Edgar Dunn suggests that there are several conflicts within government that affect how information is handled with respect to personal privacy. These conflicts include: "personal privacy versus effective government, personal privacy versus behavioral research, personal privacy versus law enforcement, and personal privacy versus free dissemination of the news" [Gray, p. 246].

The Shortcomings of Privacy Legislation

The picture of privacy in our society seems to be somewhat grim. Is there existing legislation that can be used to protect the privacy of American citizens? Some laws do exist, but their usefulness has been questioned by many.

"The regulatory and legal framework devised in the early 1970's to ensure the social control of [computerized criminal history] systems and their compliance with constitutional and statutory requirements is inadequate. Management responsibilities ot maintain accurate, unambiguous, and complete information, and the ability to account for the flow of information, cannot be enforced for a variety of financial, political, and institutional reasons. The protection of individual rights as defined in regulation cannot be assured given the inability of systems to control the dissemination of criminal history records and to purge or seal these records when required to do so by the courts" [Laudon, p. 323].

"There are no comprehensive federal or state statutes that specifically address criminal history information or related 'hot files' such as wanted warrant systems" [Laudon, p. 146]. "Unlike systems operated by the Internal Revenue Service or the Social Security Administration, there is no single federal jurisdictional authority to control the ebb and flow of criminal information. Neither are there federal enforcement mechanisms for violation of federal or state statutes" [Laudon, p. 146].

"Under current federal law and regulations, there are no civil or criminal penalties for violation of [National Crime Information Center (NCIC) Computerized Criminal History] system standards. Although agencies failing to comply with regulations on federal systems, or with NCIC system standards (i.e., management-imposed standards) are subject to cancellation of NCIC and Ident services. As a practical matter, however, this has never been invoked" [Laudon, p. 315].

"Existing regulations provide only a weak basis for authorizing the FBI to operate a national criminal history system: they fail to identify the type and nature of criminal history system that the FBI will be permitted to operate; fail to identify the specific management responsibilities of the FBI vis-a-vis state contributors; fail to identify the precise role which the states and the federal government are to play in a cooperative venture to create a national system; fail to provide for external audit; and provide only for a weak form of management oversight, leaving most important matters such as auditing, data quality, file content, and file size to FBI management and state authorities" [Laudon, p. 313].

"The existing common-law structure does nothing to give the data subject a right to participate in decisions relating to personal information

about him, a right that is essential if he is to learn whether he has been victimized by a privacy invasion" [Miller, p. 189]. "It makes no sense to rely on the victim's right to bring suit against those who have injured him when he is not informed of the source of his injury--or, in some cases, he remains unaware of the fact that he has been damaged. Even if he later discovers that his informational profile has been disfigured, an individual may find it impossible to sue if his grievance has become too ancient to command the law's attention" [Miller, p. 189].

Occasionally, though, someone actually does attempt to sue because of damage to his reputation. In general, such suits do not succeed. The reason for this is a matter of basic, simple law. "The Supreme Court has never held that the integrity of a person's reputation is constitutionally protected. Furthermore, it is sometimes stated that the best corrective for the injuries caused by a defamation is more rather than less speech, on the theory that the truth eventually will win out if open debate is encouraged. This point has no validity in the privacy context, however, because further discussion of the sensitive information will only increase the injury to the individual's privacy" [Miller, p. 193].

Not only does the Supreme Court have this view, but "the Supreme Court has held that falsehoods published by a government official acting within the scope of his discretionary authority are absolutely privileged" [Miller, p. 196]. "The notion that the courts will recognize a general principle requiring data handlers to treat personal information as confidential or will declare that file keepers owe a fiduciary duty to file subjects seems to be wishful thinking. Nor is it realistic to think that a pledge of confidentiality can be secured on a contractual basis" [Miller,

p. 200].

This is not to say that legislation could not be created to counter privacy problems. But such legislation does not yet exist, and some are not sure that it ever will. Public policy has failed to regulate these systems for several reasons: there is a lack of basic research on the organization and use of information; poor system development practices have been used in the creation of these systems; the systems are supported by legislators in order to win voters; the interests of bureaucratic organizations in the government have prevailed; congressional red tape has hampered efforts to enact privacy legislation [Laudon, pp. 342-366].

Possible Solutions

Clearly, a new approach is needed to solve these problems. Current legislation is inadequate to protect privacy, so changes are in order. "First, there is the obvious need...to redefine what [is meant] by privacy. Societal notions, or senses, of privacy have always undergone change. Second, there may have to be new laws, regulations, and rules that apply to computer-driven devices that have the capacity to invade data privacy. The more information pools are centralized, the more serious the unrestricted flow of information becomes. American society wants more and better information and personal privacy; as usual, we want it both ways" [Hixson, p. 216].

Many people have offered potential solutions to these problems. Diane L. Zimmerman has said, "Privacy law might be more just and effective if it were to focus on identifying (preferably by statute) those exchanges

of information that warrant protection at their point of origin, rather than continuing its current, capricious course of imposing liability only if the material is ultimately disseminated to the public at large" [Hixson, p. 182].

Changes in legislation are necessary to insure privacy. There is dispute, however, on what changes should be made. One thing that is agreed upon is that these changes will not be simple. As Arthur Miller has written, "Extremely complex legislation...is necessary if specific privacy safeguards are to be prescribed." "To insure adequate proctection, legislation would have to prescribe how these techniques should be used, deal with virtually every aspect of information integrity, and draw difficult distinctions in terms of levels of information sensitivity" [Miller, p. 224].

Unfortunately, it may be very difficult to motivate Congress to create any new privacy legislation. "Congressional inertia, a lack of technical expertise on Capitol Hill, and the labyrinthine character of the computer-privacy problem all combine to make it extremely unlikely that a refined statutory scheme will emerge in the foreseeable future" [Miller, p. 224].

The idea of an overseeeing government agency has been proposed by some. One early supporter of this idea was the late Senator Sam Ervin. In a speech delivered in November 1969 at the Wharton School of Finance and Commerce, Ervin stated his case.

> "I see no existing agency which could assume these complicated and delicate problems. Those charged with regulating communications have built-in biases in their operating methods and their approaches to these problems, particularly the preservation of individual privacy.

> While I dislike adding to an already weighty bureaucracy, the problem is serious enough to warrant a separate agency. For this reason, therefore, I would support the creation of some separate agency to deal specifically with computer systems.
>
> I believe we have learned enough over the past 50 years about the design and operations and problems of regulatory agencies to enable us to create one which has built-in protections to assure that it serves the interests of the individual citizen and not solely those of the industry it is supposed to regulate" [Miller, p. 233].

As David Flaherty has written, "Without a privacy protection commission, it will be of dubious utility to continue to rely on individuals protecting their privacy through their own initiative in the courts and on shaping data protection legislation on a sector-by-sector basis. The processes are simply too expensive and complicated to be accomplished without continuing input by the specialists working for a data protection agency. A privacy protection commission would facilitate the design, justification, and implementation of sector-by-sector legislation for data protection" [Flaherty, p. 365].

Flaherty also provides guidelines for the responsibilities that such a commission should have.

> "1. Articulating privacy concerns in every relevant situation, functioning essentially as an alarm system for the protection of personal privacy.
>
> 2. Carrying out oversight to protect the privacy interests of individuals in all federal information-handling activities.
>
> 3. Implementing statutory duties under a revised Privacy Act.

4. Conducting investigations and audits of information systems to monitor compliance with the provisions of a revised Privacy Act.

5. Developing and monitoring the implementation of appropriate security guidelines and practices for the protection of personal information in federal hands.

6. Advising and developing regulations appropriate for specific types of personal information systems. Staff members of the proposed privacy protection commission could thus become specialists in different types of information systems and information flows.

7. Monitoring and evaluating developments in information technology with respect to their implications for personal privacy.

8. Conducting research and reporting on all types of privacy issues in the United States" [Flaherty, pp. 365-366].

"Some have argued that such a federal privacy protection commission lacks a constituency, such as a consumer movement, to support it. One response is that it has been the legislatures in other countries, such as France and West Germany, that have recognized the need for strong, independent data protection agencies; there has never been a mass popular uprising in favor of such innovative legislation. In the right political climate, a single congressional subcommittee should be able to persuade senators and representatives of the need to act, as has happened so often with sectoral privacy legislation" [Flaherty, p. 367].

One should not put too much faith in the government to act, though. "In evaluating the need for a protective agency, it cannot be emphasized too strongly that the incentives for the government and the bureaucracy are in the direction of invading, or at least ignoring or neglecting, privacy interests rather than protecting them" [Flaherty, p. 382].

"A somewhat different, and in may ways more drastic, legislative approach involves requiring computer manufacturers, users, and data networks to employ prescribed safeguards for maintaining the integrity of personal information. This can take the form of imposing a statutory duty of care on everyone connected with the data-handling process, which would have the effect of encouraging privacy consciousness, or of enacting detailed privacy-oriented technical and procedural requirements that would have to be followed by computer manufacturers and handlers of personal information" [Miller, p. 223].

Along this line Miller has written, "The managers of a computer system and anyone else who is responsible for a release of private information should be held liable for the privacy invasion, even if the actual dissemination to the public is the work of the press and is protected by the First Amendment" [Miller, p. 199].

John Shattuck has proposed the following "general framework for safeguarding individual rights" from privacy invasions by government computer matching programs.

"1. The Privacy Act should be amended to clarify that computer matches are not ipso facto 'routine uses' of personal record systems.

2. No further federal computer matches should be permitted without express congressional authorization.

3. Congress should not authorize computer matches of sensitive personal records systems (the confidentiality of which is otherwise protected by statute) such as taxpayer records maintained by the IRS, census records maintained by the Census Bureau, or bank records maintained by federally insured banking institutions.

4. No computer match should be authorized unless and until an

analysis has been made of its projected costs and projected savings in the recoupment of funds owed to the government. The match should not be authorized unless the public benefit will far outweigh the cost--and unless individual rights will be protected. The results and full costs of any match should be published.

5. Procedural due process protections for the persons whose records are to be matched should be specified by statute, including the right to counsel, the right to a full hearing, and the right to confidentiality of the results of a match" [Shattuck, p. 541].

Richard Kusserow has raised objections to these guidelines. In his words, "requiring congressional authorization for each match and affording persons whose records are being matched rights far in excess of those available to the actual subjects of a law enforcement inquiry would not improve--but end--the use of matching" [Kusserow, p. 545]. Some would offer the counter-argument that ending government computer matching would not necessarily be a bad thing.

Kenneth Laudon also offers some proposals for decreasing the abuse of information.

1. A privacy protection commission should be created "to advise the President and Congress on the privacy merits of new systems and to oversee existing systems."

2. Criteria for evaluating systems should be developed. Questions to be asked about any system should included:

   a. Is the system needed?
   b. "Will it work and how well?"
   c. What alternatives are there to the system?
   d. How is the system accountable and how does the public participate?

Also, "congressional committees on privacy" should be established.

3. "Amend the 'routine use' clause of the Privacy Act."

4. "Examine the issue of consent."

5. "Attach a cost to information," as an aid in determining compensation for damages.

6. "A Constitutional amendment to protect electronic communication" should be created and enacted.

7. "A Constitutional amendment to protect certain files" should be created and enacted.

8. "A National Defense Information Systems Education and Research Act" should be created and enacted [Laudon, pp. 382-400].

Although these proposals are directed toward government systems, such legislation could be made to encompass private information systems as well.

What can be done to control the rampant abuse of information systems in the private sector? Susan Gray offers five potential methods of solving this problem. These were generated from theories formulated by other authors. Basically, the proposed solutions are: (1) "it is the responsibility of the individual to be well-informed about security systems;" (2) some form of liability should be created for maintainers of inaccurate information; (3) limits should be set on "what personal information may be collected" and enforced by "an oversight organization;" (4) a national computerized fingerprint system should be used to diminish confusion when records of two people with similar backgrounds and identifiers (name, Social Security numbers, et cetera) are encountered; and (5) "stricter data-dissemination restrictions" should be created and enforced so that access to information is more tightly controlled [Gray, pp. 254-255].

David Linowes, whose work is frequently referenced in this paper, offers nine recommendations for creating a corporate privacy behavior

standard that encompass all conceivable aspects of privacy, including several not discussed in this paper. They are valid even when examining government systems, and they make a fine closing piece for a discussion of potential solutions. These recommendations are:

"1. Acquire only relevant information.

2. Consider pretext interviews unacceptable methods of gathering information.

3. Use no polygraph or other lie detector tests in employment.

4. Allow and encourage employees and consumers to see and copy records pertaining to them.

5. Keep no secret records.

6. Establish a procedure for challenging and correcting erroneous reports.

7. Use information only for the purpose for which it was originally acquired.

8. Transfer no information without the subjects' authorization or knowledge.

9. Destroy data after its purpose has been served"

[Linowes, pp. 175-176].

If most companies used standards based on these guidelines, a large percentage of corporate privacy problems would be eliminated, since so many stem from employers' own abuse of information. Likewise, the primary abuser of government systems is the government itself, so legislators may do well to enact laws that also are based on these guidelines.

Conclusion

"Computerization facilitates bureaucratic trends without originating

or altering them" [Gray, p. 248]. In other words, there is nothing new under the sun when it comes to the lack of personal privacy. The only changes over time are in the volume of data known and the speed with which it can be used to the advantage of the few and the disadvantage of the many.

Clearly, there is a need for measures to be taken to ensure greater information privacy. Unfortunately, the government cannot be relied upon to act. Considering the legislators, agencies, and corporations that support these information systems, it is doubtful that any existing organization will move for greater privacy protection. Until the American people become aware of this problem and act, the trend away from privacy will no doubt continue. By that point, however, it will probably be too late to stop privacy violators with any degree of effectiveness.

Bibliography

David Burnham, The Rise of the Computer State, Random House, New York (1983).

Roger A. Clarke, "Information Technology and Dataveillance," Communications of the ACM, Volume 31, Number 5 (May 1988), pp. 498-512.

David H. Flaherty, Protecting Privacy in Surveillance Societies, The University of North Carolina Press, Chapel Hill (1989).

Susan H. Gray, "Electronic Data Bases and Privacy: Policy for the 1990's," Science, Technology, and Human Values, Volume 14, Number 3 (Summer 1989), pp. 242-257.

Richard F. Hixson, Privacy in a Public Society, Oxford University Press, New York (1987).

Richard P. Kusserow, "The Government Needs Computer Matching to Root Out Waste and Fraud," Communications of the ACM, Volume 27, Number 6 (June 1984), pp. 542-545.

Kenneth C. Laudon, Dossier Society, Columbia University Press, New York (1986).

David F. Linowes, Privacy in America, University of Illinois Press, Chicago (1989).

Arthur D. Miller, The Assault on Privacy: Computers, Data Banks, and Dossiers, The University of Michigan Press, Ann Arbor (1971).

John Shattuck, "Computer Matching is a Serious Threat to Invdividual Rights," Communications of the ACM, Volume 27, Number 6 (June 1984), pp. 538-541.