Information Privacy: A Case Study and Commentary

By Michael McFarland, SJ

Computers and Information Privacy

Computers process information. They collect it, store it, aggregate it, search it, combine it in new ways, and draw inferences from it. When connected together in networks, they can communicate the information with one another, widely propagating the information from a single source, on the one hand, and concentrating and combining the information from many sources in a single repository, on the other.

Of course people have always collected and used information. Thorough, accurate information is essential for good decision making in a variety of contexts. A doctor, for example, needs information about a patient’s history and symptoms to make a reliable diagnosis and prescribe a program of treatment. A financial planner needs information about companies' past performance and strategies to formulate a sound investment strategy. Insurance companies need to know what risks a person is subject to, because of medical history, lifestyle and other factors. Banks and merchants who extend credit need to know what a person’s financial resources are and how reliable the person has been in paying off past debts. Employers need to be able to gauge the skills, competence dependability of prospective employees.

Businesses need information to understand the needs and desires of their markets, so that they can offer products and services that are attractive, price them accordingly, and identify potential customers and communicate effectively with them. They also want to track changes in the economy, society and culture that will affect consumer demand, prices, labor and raw material costs and many other factors.

Governments need vast amounts of information to administer benefit programs, collect taxes, maintain security and formulate policy. Law enforcement authorities want to know about suspects’ criminal histories and other factors that might indicate how dangerous they are and how likely it is that they might have committed a certain crime. Authorities also want to be able to identify potential threats to public security. The IRS wants to know if a taxpayer is hiding
income. Welfare authorities want to know the same thing about their clients. On the other hand, political and social movements require information to formulate and communicate their views, recruit adherents and organize protests and other activities, sometimes in direct opposition to government authorities.

Information is needed at the personal level as well. Parents want to know if their child-care worker can be trusted. They want to know if their children’s teachers or playmates pose any special threat to them. Homeowners want to know if a contractor they hired had a record of shoddy work or fraud. A person contemplating marriage would want to know if the prospective spouse was deep in debt, had a communicable disease, or was already married. People are always seeking news about family and friends, where they are, what they are doing, what their plans are, their health and well-being and their future prospects. Beyond that there is that boundless human curiosity that always seeks to know more about everything imaginable, whether it is physical or social systems, or the affairs of one’s neighbors and other “interesting” people.

Computers, however, provide new capabilities for handling information that were unimaginable just a generation or two ago. They can collect and store immense quantities of information, and search through it with lightning speed. They can combine that information in new ways, discovering patterns and relationships that were previously beyond reach. And through the wonders of computer networks, they can share that information across continents and even across department boundaries. Furthermore, the availability and attractiveness of computer-based services such as social networks, search engines and online shopping, encourage their users to reveal far more personal information than they otherwise would. This puts powerful new tools for acquiring and using information in the hands of decision makers and the curious alike.

Some of the information computers process comes from the measurement of physical processes, such as the weather patterns across the U.S. in January, or the trajectory of a comet. But much of the information is about individual human beings, their artifacts and their social
systems and processes. Some of that information is taken from public sources, such as encyclopedias, newspapers, blogs and other personal postings, government records and financial reports. But some of the information about human affairs is not yet public, and the originators and subjects have a personal interest in keeping it from becoming public. In some cases the information has proprietary value, such as the design of a new device, or an innovative business plan. In others its disclosure would leave the subject vulnerable to manipulation, prejudice, or discrimination, such as a history of mental health problems. Or the information might just be too intimate to share widely, such as a person's medical records or postings intended for a limited group of friends on a social network.

This is where conflicts arise over the collection and use, versus the protection, of personal information. These problems, which are usually discussed under the rubric of privacy, existed before the computer. But by opening access to immense new sources of information and offering powerful new capabilities for storing, analyzing and communicating it, the computer has significantly extended and aggravated the controversy.

In this essay we will consider the privacy issues raised by the use of computerized and networked information systems. We will first look at a case that illustrates several of the important issues involved. Then we will discuss the meaning and value of privacy and the threats to privacy posed by computers and computer networks. We will also look at the current legal protections for privacy. From this analysis, we will derive a set of norms for the proper protection of personal information.

Case: A National AIDS Registry

In the following case the characters and events are fictional, but the issues are real enough.

Dr. Jeremiah Foxx is a physician working for the National Institutes of Health (NIH). Over the past several years, he has been doing epidemiological studies on the AIDS epidemic, studying its spread through different geographic areas and different segments of the population. Through this work Dr. Foxx and his colleagues have been able to identify several important
trends, such as its disproportionate impact on certain minority groups, its spread to the heterosexual population, and its dramatic increase among women and children. This in itself has been valuable in identifying high-risk groups so that treatment and prevention can be targeted where they will do the most good and in providing better education on the risks involved, especially for those outside the supposed high-risk population. As the studies continue over time, Dr. Foxx hopes not only to learn more about the disease and its spread, and the influence of various environmental factors, but also to assess the impact of various initiatives to control the disease, such as drug treatment, clean needles programs, sexual education, the advocacy of sexual abstinence and condom distribution.

Even though drug treatments and better care have reduced the mortality rate from AIDS in the United States, it is still a very dangerous disease, especially in the African-American community, where it is still one of the leading killers. Moreover, in certain other countries, particularly in Africa and Asia, it has had a devastating impact. Good research is needed more than ever. However, Dr. Foxx and other AIDS researchers have been frustrated by the difficulty in obtaining good, reliable, timely data on AIDS cases nationwide. The data comes from surveys of thousands of doctors, hospitals and clinics throughout the country. It takes an enormous amount of effort to gather this information; and the results are fragmentary, inconsistent and incomplete. The response rate is far from 100 percent, and certain groups, typically the poorest and most isolated, are badly underrepresented, which distorts the results of the studies. Furthermore, even when cases are reported, there is often no good data on the personal and environmental characteristics of the persons afflicted, which makes it impossible to identify reliably some of the most important causal factors in the spread of the disease. And the lack of follow-up data makes it impossible to trace how the disease develops in different people and how they might transmit it to others. To further complicate matters, the privacy provisions of the Health Information Portability and Accountability Act (HIPAA) have made it even harder for researchers to obtain patient data for this and many other important diseases.

To address these problems, which are seriously impeding progress in AIDS research,
prevention and treatment, Dr. Foxx has proposed a National AIDS Registry, a centralized computer database holding information on all cases of AIDS, and its precursor HIV, in the United States. Whenever a health care provider diagnosed someone as HIV-positive, they would fill in a computerized form that would be transmitted directly to the database in Maryland. The form would contain not only medical information about the status of the disease and the overall health of the patient, but also personal information, including the patient’s name and address, economic and employment status, history of drug and alcohol use, racial and ethnic background, marital and family status and sexual history. On all future visits, the patient’s record would be updated with any further medical and personal developments.

The data in the database would be kept confidential, but would be available to AIDS researchers for studies of the kind Dr. Foxx has been doing. Through the use of this data, researchers could provide governments, the health care community, and others concerned with the disease, with invaluable information on how best the combat its spread. The information in the database would otherwise be kept confidential.

Dr. Foxx has been lobbying hard in Congress for his idea. He has found an ally in Senator Armand Goode. Sen. Goode has long been concerned about the AIDS epidemic, which, in spite of the progress made, continues to be a serious problem in this country, afflicting disproportionately the poor and the outcast, and a scourge devastating whole populations in some other parts of the world. Dr. Foxx’s proposal is a chance to use our science and technology to do something about it. The Senator has his staff draft a bill funding the database and reporting system and requiring participation by all health care providers that receive any federal funds, which is almost everyone because of Medicare. The bill also contains provisions to protect the confidentiality of the information and to restrict access to those who have a legitimate reason to use it, while adjusting HIPAA restrictions so as not to impede its use.

Dr. Foxx and Senator Goode prepare a press release and hold a press conference to announce the bill and invite comments from interested parties. The reaction is swift and fierce, not at all what they expected. Privacy advocates such as the EPPO, the Electronic Privacy Protection
Organization, express strong opposition. Who will have access to this information, they want to know? Will employers get to see it? What about health insurers, or banks and others checking for credit worthiness? Even if they are denied access by law, what is to stop them from using inside contacts to get the information anyway? And how will that information be protected from the prying eyes of the press, who always prove to be most resourceful in their quest for interesting information? The mere revelation that someone has HIV or AIDS, let alone some of the other personal information, can be economically and personally devastating, particularly in a society where AIDS sufferers are constantly victimized by prejudice and discrimination. With so many people from different organizations having access to the information under the umbrella of “research,” how can its security be guaranteed? And even if the information can be kept secure from these illegitimate inquiries, what about law enforcement agencies? What is to stop them from obtaining a warrant to access identifying information about a suspect they are seeking or gathering personal information as part of an investigation? Worse yet they could use the database for “fishing expeditions,” looking for illegal or suspicious patterns of behavior among the subjects, or comparing the names in the database against a list of wanted persons. In spite of the supposed safeguards called for by the bill, the existence of a large, centralized, easily accessed database containing so much sensitive personal data is an unacceptable threat to the privacy of the subjects.

It is bad enough that someone with HIV or AIDS is exposed by this database. But what about someone who is falsely identified as having the disease? Bad data is a problem in any large database. It would be even worse in this case, where the data entry is so decentralized, with little opportunity for checking or control. There will be simple data entry errors, misidentifications, misinterpretations and intentional misrepresentations. Furthermore there are many false positives in tests for HIV. Once bad data gets into a large database like this, it tends to take on a life of its own, even if it is later discovered and repudiated. It will be impossible to detect and root out all bad data. And the damage done by that data, especially to the subjects, will be enormous.
Even beyond the specific harm that will be done by the AIDS Registry, there are deeper issues of human rights. To take, store and use personal information without the subjects’ permission, and to make it available to unspecified parties is not only an invasion of their privacy, but an attack on their freedom. The subjects lose control of a very important aspect of their personal life, namely what others know about them.

This critique is disappointing, but not totally unexpected. “Troublemakers,” says Dr. Foxx. “They are always on their high horse about something, standing in the way of progress.” But the response of the medical community, which he would have expected to be sympathetic, is not much better. In general they are sympathetic with the goals of the proposal. They understand that easier access to more accurate and complete data on the demographics of AIDS and the environmental factors affecting it could be a great help in their efforts to control the disease and could lead to a more enlightened public policy. But for most of them the cost is clearly unacceptable. Under the system as proposed, doctors would be forced to violate doctor-patient confidentiality, an essential element in building mutual trust and respect between physician and patient. Moreover, those in the health care industry who deal with AIDS patients are convinced that many who badly need medical care will avoid it unless they have complete confidence that their condition and other personal information will be kept in strictest confidence.

The most devastating opposition of all, however, comes from AIDS activists themselves. One leader of the movement, Phil Brothers, speaks for many when he says, “People with HIV not only have to live with the burden of this disease, but are constantly being victimized by prejudice and discrimination. We have lost our jobs and our health insurance, been thrown out of schools and been shunned by family, friends and neighbors. This project will leave us even more exposed to mistreatment from ignorance, fear and prejudice. That is not the kind of 'help' we want. We are tired of being used by these outsiders. The bureaucrats, the hospitals, the academics just want to poke and prod us and tell us what to do. They don’t care about what we want. We are just statistics to them. Well, we still have lives to live. They should just leave us alone instead of treating us like laboratory rats.”
By this time the Senator is looking for cover. Even Dr. Foxx is a little shaken; but he is not ready to give up. “Why can't they understand?” he pleads. “We just want to help them. This is for their own good. We can't do anything unless we get better data.” He persuades the Senator that they should not give up the project, but should look for ways to make it less threatening. They can write in better guarantees of confidentiality and perhaps forego some of the more sensitive personal data. They can also have the subject sign a generic consent form releasing the data to the registry. The Senator reluctantly agrees to go ahead with a revised draft.

A few days later, a plain brown envelope arrives at the Senator's office. In it is a large sheaf of papers, including records of all the Senator's credit card purchases for the past three months, medical records of his wife's treatment for depression, including her prescriptions, and his daughter's grades from college. On top is a note that reads, “We know where you live. We are sick of Big Brother snooping on the lives of innocent citizens. If you do not drop your support of the National AIDS Registry, we will publish all these records on the Internet and make sure everyone knows where to find it. You have twenty-four hours to decide.” It is signed “The Cyberspace Freedom Fighters.” The Senator considers calling in the FBI. “They must have done something illegal to get this,” he thinks, “didn't they?” But then he reconsiders. “If I do go to the FBI, one way or the other all that stuff will come out.” The next day Senator Goode announces that the public debate has made him more sensitive to the privacy concerns of many segments of the population, so he is withdrawing his support of the National AIDS Registry bill.

****

There is as yet no National AIDS Registry of the kind discussed here. But there are now several extensive nationwide and statewide databases of medical records in the United States. For example IMS America in Towntowa, New Jersey, has software installed in the offices of thousands of doctors around the world, which allows it to collect patient information directly from their computers. The data, from which patient names have been stripped, is purchased by drug companies and other private concerns to compare the effectiveness of different treatment
regimes or to track the use of their products. In Boston the Medical Information Bureau has records on tens of millions of people who have illnesses that could shorten their life expectancy, including HIV. The data is collected and used by insurance companies to assess applicants for health and life insurance. Individuals are required to consent to the release of the information when they apply for insurance. The state of Maryland, under the authority of a 1993 state law, is collecting hundreds of thousands of patient records to build a vast computer database of medical records. The information is needed, the state claims, to provide better health care programs and to control health and insurance costs. At the federal level, auditors for the Department of Health and Human Services have insisted on obtaining the names of AIDS patients from organizations that care for them, in order to check on the validity of their claims to benefits. The care-giving organizations sued the federal government to stop the practice, claiming that it violated patient confidentiality. More generally, beginning with HIPAA, the federal government has been pushing for a widespread conversion to Electronic Health Records (EHRs) throughout the health care system in the U.S., in order to reduce costs, to enable the efficient sharing of information among health care providers, payers, such as insurance companies and governments, pharmacies, researchers and other parts of the health care system, and to promote greater accuracy, consistency and security of patient information. In 2009 the American Recovery and Reinvestment Act (ARRA, otherwise knows as the stimulus bill) contained a mandate that health care providers show “meaningful use” of EHRs by 2014, while also promising subsidies to help pay for the conversion. In spite of the great promise claimed for EHRs, however, there is still a good deal of skepticism about their effectiveness and especially about the dangers and risks they introduce into the system. Privacy is a particular concern. In

2 ibid.
4 See for example Diana Manos, “Electronic health records not a panacea, researchers say,” Healthcare IT News,
spite of the strict standards imposed by HIPAA, the Department of Health and Human Services reports hundreds of major breaches of patient confidentiality each year. For example, in 2011 the UCLA Health System agreed to pay $865,500 in penalties for leaking confidential patient data. All personal medical data is highly sensitive; but it is even more so for a disease like AIDS, where, in spite of progress in treatment, prevention, education and understanding, there is still a strong stigma attached.

This case illustrates some of the problems involved in the collection, storage, analysis and communication of personal information. The next section provides a framework for thinking about such issues.

What is Privacy?

Definitions of Privacy

Privacy has many meanings. The most general is freedom from interference or intrusion, the right “to be let alone,” a formulation cited by Louis Brandeis and Samuel Warren in their groundbreaking 1890 paper on privacy. This recognizes that each person has a sphere of existence and activity that properly belongs to that individual alone, where he or she should be free of constraint, coercion, and even uninvited observation. As we would say today, each of us needs our own “space.” Most would recognize the protected sphere to include personal opinions, personal communications, and how one behaves behind closed doors, at least as long as these do


5 http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/breachtool.html


not lead to any significant threats to society. Many would also include behavior within the family and other intimate relationships in that sphere.

This broad concept of privacy has been given a more precise definition in the law. Since the Warren-Brandeis article, according to William Prosser, American common law has recognized four types of actions for which one can be sued in civil court for invasion of privacy. They are, to quote Prosser:

1. Intrusion upon the plaintiff’s seclusion or solitude, or into his private affairs.
2. Public disclosure of embarrassing private facts about the plaintiff.
3. Publicity which places the plaintiff in a false light in the public eye.
4. Appropriation, for the defendant’s advantage, of the plaintiff’s name or likeness.  

The first category is the broadest and the hardest to interpret. “Intrusion” can mean physical presence, excessive telephone calls, and unauthorized observation, such as peering through windows of someone's home. It also covers cases where an authority forces someone to reveal personal information against that person’s will, such as a court's unjustified demand that someone produce a broad array of personal records or an unnecessary requirement that someone take a blood test.  

Another problem is defining what constitutes “private affairs.” It is not an invasion of privacy, according to the courts at least, to follow someone on the street or to take a person’s photograph in a public place. It would be, however, to do so unbidden in their home or a hospital room.  

This category of privacy applies only to that part of a person’s affairs that are not public and which the person does not wish to make public.  

While the first of Prosser’s categories can include attempts to influence, control or coerce someone’s private affairs, most of the cases covered by this category and all of those covered by the other three involve the collection and/or use of personal information about someone. That is

---

10 ibid.
11 ibid.
the core meaning of privacy. While some use the term more broadly to refer to any kind of 
uninvited interference with someone's personal life, privacy in the strict sense means shielding 
one's personal life from unwanted scrutiny.

*Informational Privacy*

It is this narrower meaning of privacy, which James H. Moor calls “informational privacy,”¹² 
that concerns us here, because that is what is threatened by the information-processing 
capabilities of computers. Moor defines the right to informational privacy as “the right to control 
of access to personal information.” This is a common definition in the literature, and one that we 
shall adopt here as well. The definition contains four important elements. First, it is about 
*information*. It focuses on the quest for knowledge about someone, rather than, say, physical 
proximity or constraint, or any other type of interference. Second, it refers to *personal* 
information. The knowledge intended gives some access to the subject's person, whether it is his 
or her identity, thoughts, aspirations, passions, habits, foibles or transgressions. Third, the issue 
is one of *control*. It is not how much or how little is known about the subject, but whether the 
subject can choose how much of the information is revealed and to whom. Finally, privacy is 
declared as a *right*. Within certain “domains,” as More puts it, the person's control of personal 
information ought to be respected and protected.

This concept of informational privacy certainly applies to the AIDS Registry case discussed 
earlier. Dr. Foxx's proposal was about gathering information of a very personal nature. Just the 
fact that someone has HIV is very personal. Medical conditions always are, but this one even 
more so, because of its tragic implications for one's life and one's future. Moreover the plan 
proposed to gather much more highly sensitive personal information, such as family history and 
patterns of behavior. The reporting of the information was to be automatic and mandatory, 
giving the patient no say in whether it was revealed and to whom. Finally the information sought

¹²James H. Moor, "How to Invade and Protect Privacy with Computers," in Carol C. Gould (ed.), *The Information 
is part of the doctor-patient relationship, a domain that we generally regard as especially
privileged and in need of protection. If there is a right to privacy, it should apply in this case.
The validity of that right is what we must now examine.

Why We Care about Privacy

Privacy is important for a number of reasons. Some have to do with the consequences of not
having privacy. People can be harmed or debilitated if there is no restriction on the public's
access to and use of personal information. Other reasons are more fundamental, touching the
 essence of human personhood. Reverence for the human person as an end in itself and as an
 autonomous being requires respect for personal privacy. To lose control of one's personal
 information is in some measure to lose control of one's life and one's dignity. Therefore, even if
 privacy is not in itself a fundamental right, it is necessary to protect other fundamental rights.

In what follows we will consider the most important arguments in favor of privacy.

Protection from the Misuse of Personal Information

There are many ways a person can be harmed by the revelation of sensitive personal
information. For example, if there were an AIDS Registry like the one discussed earlier, and the
fact that certain persons were infected by HIV leaked out, it could have a terrible impact on
them. They could lose their health insurance. They could be isolated at work and even lose their
jobs. They could be denied participation in many social activities and be shunned by neighbors,
associates, friends and, for those in school, classmates. They could be subject to all manner of
innuendo, prejudice and even blackmail. In these and many other ways, people who are already
facing a painful, life-draining and tragic illness would be denied human contact, understanding
and support when it is most desperately needed, because of inadequate respect for and protection
of their privacy.

The AIDS case is particularly poignant and compelling, but there are many other situations
where persons can be hurt by inadequate regard for their privacy. Medical records,
psychological tests and interviews, court records, financial records—whether from banks, credit
bureaus or the IRS—welfare records, sites visited on the Internet and a variety of other sources
hold many intimate details of a person’s life. The revelation of such information can leave the
subjects vulnerable to many abuses.

Good information is needed for good decisions. It might seem like the more information the
better. But sometimes that information is misused, or even used for malicious purposes. For
example, there is a great deal of misunderstanding in our society about mental illness and those
who suffer from it.13 If it becomes known that a person has a history of mental illness, that
person could be harassed and shunned by neighbors. The insensitive remarks and behavior of
others can cause the person serious distress and embarrassment. Because of prejudice and
discrimination, a mentally ill person who is quite capable of living a normal, productive life can
be denied housing, employment and other basic needs.

Similarly someone with an arrest record, even where there is no conviction and the person is
in fact innocent, can suffer severe harassment and discrimination. A number of studies have
shown that employers are far less likely to hire someone with an arrest record, even when the
charges have been dropped or the person has been acquitted.14

In addition, because subjects can be damaged so seriously by the release of sensitive personal
information, they are also vulnerable to blackmail and extortion by those who have access to that
information.

Privacy protection is necessary to safeguard against such abuses.

Privacy and Relationship

Privacy is also needed in the ordinary conduct of human affairs, to facilitate social
interchange. James Rachels, for example, argues that privacy is an essential prerequisite for

forming relationships. The degree of intimacy in a relationship is determined in part by how much personal information is revealed. One reveals things to a friend that one would not disclose to a casual acquaintance. What one tells one’s spouse is quite different from what one would discuss with one’s employer. This is true of more functional relationships as well. People tell things to their doctors or therapists that they do not want anyone else to know, for example. These privileged relationships, whether personal or functional, require a special level of openness and trust that is only possible if there is an assurance that what is revealed will be kept private. As Rachels points out, a husband and wife will behave differently in the presence of a third party than when they are alone. If they were always under observation, they could not enjoy the degree of intimacy that a marriage should have. Charles Fried puts it more broadly. Privacy, he writes, is “necessarily related to ends and relations of the most fundamental sort: respect, love, friendship and trust... without privacy they are simply inconceivable.”

Autonomy

The analysis of Rachels and Fried suggests a deeper and more fundamental issue: personal freedom. As Deborah Johnson has observed, “To recognize an individual as an autonomous being, an end in himself, entails letting that individual live his life as he chooses. Of course, there are limits to this, but one of the critical ways that an individual controls his life is by choosing with whom he will have relationships and what kind of relationships these will be. Information mediates relationships. Thus when one cannot control who has information about one, one loses considerable autonomy.”

To lose control of personal information is to lose control of who we are and who we can be in relation to the rest of society. A normal person’s social life is rich and varied, encompassing

many different roles and relationships. Each requires a different persona, a different face. This does not necessarily entail deception, only that different aspects of the person are revealed in different roles. Control over personal information and how and to whom it is revealed, therefore, plays an important part in one's ability to choose and realize one's place in society. This operates on many different levels. On a personal level, for example, one ought to be able to choose one's friends. That means that one should be able to choose to whom to reveal some of the personal revelations that are only shared among friends. This choice is only meaningful if one can also choose to exclude some from friendship and the privileged revelations that come with it.

Consider the case of Carrie and Jim. Jim met Carrie at a party and was immediately smitten by her grace and beauty. Unfortunately for Jim it was not mutual. Carrie made it quite clear she had no interest in any kind of relationship. But this brush-off just fueled Jim’s obsession with her. He began to stalk her, following her wherever she went and looking her up online, until he knew her daily schedule, her friends, and her favorite shops and restaurants. He did careful research on her trash, reading her letters and inspecting her receipts, learning what kind of cosmetics she used and what her favorite ice cream was. He even peeked through her window at night to see what she wore and how she behaved when she was alone. Even if Jim never did anything to attack or harass Carrie, even if she never found out about his prying, she has lost some of her freedom. She did not want him to have access to her personal life, but he seized it anyway.

Privacy is an issue in other, more professional, relationships as well, as the following case illustrates. Fred Draper19 grew up in Brooklyn, where as a youth he ran with a very tough crowd. By the time he was 16 he had been convicted of armed robbery and malicious destruction of property, and was on probation until he was eighteen. But Fred was also a very talented student, and he was fortunate enough to have a teacher in high school recognize his potential and take him under his wing. Through a combination of encouragement, guidance and discipline, the

19Not a real person. This case, like the one before it, is a composite.
teacher was able to get Fred to focus on school and stay out of trouble, so that he graduated with an outstanding record and won a scholarship to NYU. He was successful there also, going on to law school. Upon finishing law school, Fred was hired by a top Wall Street law firm, where he was well on his way to establishing himself as one of their top young lawyers. Then a newspaper reporter took notice of Fred and his growing prominence and decided to see if there was a story there. There was. The reporter traced Fred back to his old neighborhood and learned about his past history. He wrote a story about it, praising Fred for the way he had overcome his past and made a respectable life for himself. But some of Fred clients had a different reaction. They were not comfortable dealing with a former hood from Brooklyn, so they asked that he be taken off their accounts. The firm complied with their wishes and ultimately let Fred go, deciding that he was too much of a liability to keep. This again illustrates the importance of privacy in allowing people the freedom to realize their potentialities. Once the information about his past had leaked out, Fred was no longer able to maintain his professional persona in relation to his clients, a persona that he had proved he was capable of fulfilling.

**Human Dignity**

Autonomy is part of the broader issue of human dignity, that is, the obligation to treat people not merely as means, to be bought and sold and used, but as valuable and worthy of respect in themselves. As the foregoing has made clear, personal information is an extension of the person. To have access to that information is to have access to the person in a particularly intimate way. When some personal information is taken and sold or distributed, especially against the person's will, whether it is a diary or personal letters, a record of buying habits, grades in school, a list of friends and associates or a psychological history, it is as if some part of the person has been alienated and turned into a commodity. In that way the person is treated merely as a thing, a means to be used for some other end.

This is at the core of the AIDS sufferers’ argument against an AIDS Registry in the case described earlier. When they complained, "We are just statistics to them," they were objecting to
the dehumanization that occurred when their very personal stories were taken from them and used without any consent on their part and without any personal involvement or care on the part of the researchers. Because of the patients' loss of control and the lack of respect for them as persons, they felt like "laboratory rats." Similarly those who stole Sen. Goode's personal information and used it to blackmail him into changing his position were guilty of the same disrespect and dehumanization. The Senator and his family were simply a means to an end for them, to be used to achieve a particular goal. Even if the goal were considered worthy, it would not justify the abuses committed in its name.

Privacy and Power

Privacy is even more necessary as a safeguard of freedom in the relationships between individuals and groups. As Alan Westin has pointed out, surveillance and publicity are powerful instruments of social control.\textsuperscript{20} If individuals know that their actions and dispositions are constantly being observed, commented on and criticized, they find it much harder to do anything that deviates from accepted social behavior. There does not even have to be an explicit threat of retaliation. "Visibility itself provides a powerful method of enforcing norms."\textsuperscript{21} Most people are afraid to stand apart, to be different, if it means being subject to piercing scrutiny. The "deliberate penetration of the individual’s protective shell, his psychological armor, would leave him naked to ridicule and shame and would put him under the control of those who know his secrets."\textsuperscript{22} Under these circumstances they find it better simply to conform. This is the situation characterized in George Orwell’s \textit{1984} where the pervasive surveillance of “Big Brother” was enough to keep most citizens under rigid control.\textsuperscript{23}

Therefore privacy, as protection from excessive scrutiny, is necessary if individuals are to be

\begin{itemize}
\item \textsuperscript{21}ibid, p. 20.
\item \textsuperscript{22}ibid, p. 32.
\item \textsuperscript{23}George Orwell, \textit{1984}, New York: Harcourt and Brace (1949).
\end{itemize}
free to be themselves. Everyone needs some room to break social norms, to engage in small “permissible deviations” that help define a person’s individuality. People need to be able to think outrageous thoughts, make scandalous statements and pick their noses once in a while. They need to be able to behave in ways that are not dictated to them by the surrounding society. If every appearance, action, word and thought of theirs is captured and posted on a social network visible to the rest of the world, they lose that freedom to be themselves. As Brian Stelter wrote in the New York Times on the loss of anonymity in today’s online world, “The collective intelligence of the Internet’s two billion users, and the digital fingerprints that so many users leave on Web sites, combine to make it more and more likely that every embarrassing video, every intimate photo, and every indelicate e-mail is attributed to its source, whether that source wants it to be or not. This intelligence makes the public sphere more public than ever before and sometimes forces personal lives into public view.”

This ability to develop one’s unique individuality is especially important in a democracy, which values and depends on creativity, nonconformism and the free interchange of diverse ideas. That is where a democracy gets its vitality. Thus, as Westin has observed, “Just as a social balance favoring disclosure and surveillance over privacy is a functional necessity for totalitarian systems, so a balance that ensures strong citadels of individual and group privacy and limits both disclosure and surveillance is a prerequisite for liberal democratic societies. The democratic society relies on publicity as a control over government, and on privacy as a shield for group and individual life.”

When Brandeis and Warren wrote their seminal article on privacy over one hundred years ago, their primary concern was with the social pressure caused by excessive exposure to public scrutiny of the private affairs of individuals. The problem for them was the popular press, which

---

represented the “monolithic, impersonal and value-free forces of modern society,” undermining the traditional values of rural society, which had been nurtured and protected by local institutions such as family, church and other associations. The exposure of the affairs of the well-bred to the curiosity of the masses, Brandeis and Warren feared, had a leveling effect which undermined what was noble and virtuous in society, replacing it with the base and the trivial.

Even apparently harmless gossip, when widely and persistently circulated, is potent for evil. It both belittles and perverts. It belittles by inverting the relative importance of things, thus dwarfing the thoughts and aspirations of a people. When personal gossip attains the dignity of print, and crowds the space available for matters of real interest to the community, what wonder that the ignorant and thoughtless mistake its relative importance.... Triviality destroys at once robustness of thought and delicacy of feeling. No enthusiasm can flourish, no generous impulse can survive under its blighting influence.\textsuperscript{27}

For Brandeis and Warren, privacy was a means of protecting the freedom of the virtuous to maintain their values against the corrupting influence of the mass media that catered to people's basest instincts.

Although the degrading effect of the mass media is still a problem, today a more serious threat to freedom comes from governments and other large institutions. Over the last century, governments have developed sophisticated methods of surveillance as a means of controlling their subjects. This is especially true of totalitarian states, as the passage from Westin quoted above indicates. The Soviet Union, Communist China, Nazi Germany, Fascist Italy and white-run South Africa all used covert and overt observation, interrogation, eavesdropping, reporting by neighbors and other means of data collection to convince their subjects that independent, “antisocial” thought, speech and behavior was unacceptable. In many cases the mere presence of the surveillance was enough to keep people in line. Where it was not, the data collected was used to identify, round up and punish elements of the population that were deemed dangerous. For example, Ignazio Silone, in his book \textit{Bread and Wine}, described the use of surveillance in


\textsuperscript{27}Brandeis and Warren, p. 196.
Fascist Italy in this way:

It is well-known [says Minorca] that the police have their informers in every section of every big factory, in every bank, in every big office. In every block of flats the porter is, by law, a stool pigeon for the police.... This state of affairs spreads suspicion and distrust throughout all classes of the population. On this degradation of man into a frightened animal, who quivers with fear and hates his neighbor in his fear, and watches him, betrays him, sells him, and then lives in fear of discovery, the dictatorship is based. The real organization on which the system in this country is based is the secret manipulation of fear.²⁸

While totalitarian regimes may not seem as powerful or as sinister as they did 50 years ago, surveillance is still used in many places as an instrument of oppression. For example Philip Zimmerman, the author of the PGP (Pretty Good Privacy) data encryption program, reports receiving a letter from a human rights activist in the former Yugoslavia that contained the following testimonial:

We are part of a network of not-for-profit agencies, working among other things for human rights in the Balkans. Our various offices have been raided by various police forces looking for evidence of spying or subversive activities. Our mail has been regularly tampered with and our office in Romania has a constant wiretap.

Last year in Zagreb, the security police raided our office and confiscated our computers in the hope of retrieving information about the identity of people who had complained about their activities.

Without PGP we would not be able to function and protect our client group. Thanks to PGP I can sleep at night knowing that no amount of prying will compromise our clients.²⁹

More recently social media and the Internet played major roles in the “Arab Spring” uprisings in the Middle East, causing Egypt and Libya to shut down the Internet in their countries in an attempt to stifle dissent.³⁰ In China there has been an ongoing battle between the government and activist groups over government monitoring and censorship of the Internet.³¹

---


²⁹ Philip Zimmerman, in a posting to the Cyberpunks newsgroup: cyberpunks@toad.com, (March 18, 1996).


Even in a democracy, there is always the danger that surveillance can be used as a means of control. In the United States, for example, where freedom is such an important part of the national ethos, the FBI, the CIA, the National Security Agency (NSA) and the armed forces have frequently kept dossiers on dissidents. The NSA from 1952 to 1974 kept files on about 75,000 Americans, including civil rights and antiwar activists, and even members of Congress. During the Vietnam war, the CIA's Operation Chaos collected data on over 300,000 Americans. Since then the NSA has had an ongoing program to monitor electronic communications, both in the U.S. and abroad, which has led to constant battles with individuals and groups who have sought to protect the privacy of those communications through encryption and other technologies.

Some of the most famous incidents of surveillance of dissidents, of course, occurred during the Nixon administration in the early 1970s. For example, when Daniel Ellsberg was suspected of leaking the Pentagon Papers, an internal critique of government conduct of the Vietnam war, Nixon's agents broke into the office of Ellsberg's psychiatrist and stole his records. And it was a bungled attempt at surveillance of Nixon's political opposition, as well as illegal use of tax returns from the IRS, that ultimately brought down the Nixon administration. More recently, during the 1996 presidential campaign, it was revealed that the Clinton White House had access to the FBI investigative records of over 300 Republicans who had served in the Reagan and Bush administrations. The Clinton administration claimed it was all a mistake caused by using an out-of-date list of White House staff, while the challenger Bob Dole accused them of compiling an "enemies list." Whatever the motivation, the head of the FBI termed the use of the files

32Burnham, pp. 130-131.
34Burnham, p. 176.
35ibid, p. 104.
"egregious violations of privacy."

Since the 9/11 terrorist attacks in 2001, there has been even greater urgency in the government's efforts to monitor the activities and communications of people, both foreigners and its own citizens, in order to identify and prevent terrorist threats. The Patriot Act, passed less than two months after 9/11, greatly expanded the government's authority to intercept electronic communications, such as emails and phone calls, including those of U.S. citizens. As a result government agencies have been building the technological and organizational capabilities to monitor the activities and communications of their own citizens. For example, Wired magazine revealed in a recent report how the National Security Agency has transformed itself into the largest, most covert, and potentially most intrusive intelligence agency ever created. In the process—and for the first time since Watergate and the other scandals of the Nixon administration—the NSA has turned its surveillance apparatus on the US and its citizens. It has established listening posts throughout the nation to collect and sift through billions of email messages and phone calls, whether they originate within the country or overseas. It has created a supercomputer of almost unimaginable speed to look for patterns and unscramble codes. Finally, the agency has begun building a place to store all the trillions of words and thoughts and whispers captured in its electronic net. And, of course, it's all being done in secret. To those on the inside, the old adage that NSA stands for Never Say Anything applies more than ever.

The FBI, the Drug Enforcement Agency and the Department of Homeland Security also have many programs to monitor citizens in general, not just those who are under suspicion. These efforts include sifting through media references, tracking chatter on social networks, and

monitoring peoples’ movements through license plate scanners and video cameras.

The mere knowledge that American citizens could be the subjects of surveillance can in itself have a chilling effect on political freedom. "Now it is much more difficult than it once was to dismiss the possibility that one's phone is being tapped, or that one's tax returns may be used for unfriendly political purposes, or that one's life has become the subject of a CIA file. The realization that these activities might take place, whether they really do or not in any particular instance, has potentially destructive effects on the openness of social systems to innovation and dissent."

At times the government in the United States has gone beyond surveillance and intimidation and has used the data gathered as a basis for overt oppression. One of the most blatant examples is the internment of over 100,000 Japanese Americans, most of them American citizens, during World War II. The Justice Department used data from the Census Bureau to identify residential areas where there were large concentrations of Japanese Americans, and the army was sent in to round them up. They were taken away from their homes and held in concentration camps for the duration of the war.

Governments do need information, including personal information, to govern effectively and to protect the security of their citizens. But citizens also need protection from the overzealous or malicious use of that information, especially by governments that, in this age, have enormous bureaucratic and technological power to gather and use the information.


44 ibid, pp. 20-25.
But...Privacy is not Absolute

When we speak of privacy, particularly as a right, we focus on the individual. The individual must be shielded from the prying curiosity of others and from prejudice and discrimination. The individual's autonomy and control over his or her person must be preserved. The individual must be protected from intimidation and coercion by government.

These are important considerations; but not the whole story. For the human person does not exist purely as an individual. People live their lives as members of society. In fact they are members of many societies, which may include families, circles of friends, work organizations, churches, voluntary associations, civic organizations, city, state and nation.\textsuperscript{45} These associations are not merely preferences or matters of convenience. To be human is to be in relationship. Therefore social obligations, that is, all that is required to maintain the complex Web of relationships in which each person lives, are fundamental human obligations. Moreover each individual has an obligation to contribute to the good of society, the so-called "common good."

These obligations include the sharing of personal information, which is a necessary part of any meaningful relationship, whether it is personal, community, political or bureaucratic. Friendship necessarily requires self-revelation, as do family relationships on an even more intimate level. Belonging to a voluntary association entails sharing something of one's history, one's ideas and aspirations, and one's current circumstances. And, as we have seen previously, government requires a certain amount of information on its citizens in order to govern efficiently, provide for their security and distribute benefits and obligations fairly. The same in general can be said of employers and their employees.

The obligation to share information for the common good does not always take precedence over the right to privacy. Rather the two must be held in balance, for both are necessary for a fully human life. According to John B. Young, in his book on privacy,

The right to privacy is inherent in the right to liberty, but the life of the individual in all

societies has to strike a balance between freedom and discipline. Insufficient freedom will subdue the spirit of enterprise and resolution on which so much of civilized progress depends, whereas unbridled freedom will clash inexorably with the way of life of others. It is inevitable therefore that there must be some measure of restraint on the activities of members of a community, and in order to control people in a modern and complex society information about them and their behavior is indispensable. The concomitant price which the individual must pay can be measured in terms of loss of privacy.  

Even Alan Westin, the great privacy advocate acknowledges,  

The individual's desire for privacy is never absolute, since participation in society is an equally powerful desire. Thus each individual is continually engaged in a personal adjustment process in which he balances the desire for privacy with the desire for disclosure and communication of himself to others, in light of the environmental conditions and social norms set by the society in which he lives.

These considerations lead to the following principle on information privacy: *Just as the human person pursues personal freedom and self-realization in the context of relationship, with all the obligations, constraints and tensions that that entails, so the right to privacy coexists with, and is circumscribed by, the obligation to serve the common good.*

**Summary**

Based on the above considerations, we can define an invasion of (informational) privacy as having the following elements:

1. It involves personal information that gives access to the subject's life, for example, his or her thoughts, words, actions, habits, history, plans, aspirations, and so on.

2. The information is made available to others without the consent of the subject.

3. The information was not previously published or otherwise made public knowledge, and there is no reasonable expectation that it would be public knowledge.

4. There is no overriding, legitimate public interest in collecting this information and making it available.

---


The third condition recognizes that a person comes to be known in many ways in the course of everyday life, and that is not, in itself, an invasion of privacy. It may be well known to Jason's neighbors that he goes jogging through the neighborhood at 7 AM every day. There is no invasion of privacy there because it is reasonable to assume that he would be observed and recognized by them. If he wanted his jogging to be completely private, he would have to find a more secure and sheltered place to do it. However, there is still an issue of how widely this information should be publicized. Just because *some* people know something, it does not mean that *everyone* ought to know. For example, if his neighbors compile every shred of observable evidence about Jason's life -- for example, that he and his wife often have loud arguments, that their trash is full of empty whiskey bottles, and that their son visits a probation officer once a month -- and publish it in the local newspaper, it may well be a moral, if not a legal, invasion of privacy.

Condition 4 should be interpreted restrictively as well. Sensitive information collected without the consent of the subject because it was necessary for the public welfare should be available only to those who have a legitimate need for it.

Invasions of privacy as we define them here are of concern for a number of reasons:

1. The more widely sensitive information is disseminated, the greater the danger of error, misunderstanding, discrimination, prejudice and other abuses.
2. The lack of privacy can inhibit personal development, and freedom of thought and expression.
3. It makes it more difficult for individuals to form and manage appropriate relationships.
4. It restricts individuals' autonomy by giving them less control over their lives and in particular less control over the access others have to their lives.
5. It is an affront to the dignity of the person.
6. It leaves individuals more vulnerable to the power of government and other large institutions.
Computer-Related Threats to Privacy

There were problems with privacy long before there were computers. But computers, because they add new capabilities for collecting, organizing, analyzing and transmitting information, aggravate some existing privacy problems and add some new ones.

We will describe here some of the important ways in which the use of computers can erode privacy.

Errors

Both government agencies and private companies keep vast databases containing very sensitive and very personal information about tens or hundreds of millions of subjects. For example, the FBI's National Crime Information Center (NCIC) keeps records on arrests, outstanding warrants, criminal histories, and other data that might be of use in investigating crime. It currently processes an average of 7.5 million transactions each day.\textsuperscript{48} When subjects are stopped by the police, their identities are often checked against the NCIC to see if they are currently wanted for a crime, on probation, or considered dangerous. In the private sector, large credit agencies such as TransUnion and Equifax, keep computerized credit histories on close to a hundred million people. These are searched hundreds of thousands of times each day by thousands of subscribers, whenever a customer requests credit of any kind, whether it is to apply for a loan or simply make a credit card payment.\textsuperscript{49}

These databases are used to make many critical decisions affecting peoples’ lives. Someone can be arrested and detained or denied a mortgage or the use of a credit card based on the data stored in them. Yet the sheer size of these databases, as well as the procedures used to collect, process and maintain the data in them, ensure that they will contain many inaccuracies. A study done by Kenneth Laudon for the Office of Technology Assessment (OTA) found that only 25.7 percent of the records sent by the FBI's identification division were "complete, accurate and

\textsuperscript{48}\url{http://www.fbi.gov/about-us/cjis/ncic}

\textsuperscript{49}Burnham, pp. 43-45.
unambiguous." A higher percentage, about 46 percent, of the criminal history records in the NCIC met these standards. When Laudon checked a sample of open arrest warrants on file with the FBI against records in the local court houses where they originated, he found that over 15 percent of them were invalid, either because there was no record at all of them or they had already been cleared or vacated. Thus 15 percent of the warrants on record put their subjects at risk of being arrested for no justifiable reason.50

There are also documented problems with credit databases. For example, according to David Burnham, in 1980 TRW was receiving 350,000 complaints a year from consumers who felt their credit reports were inaccurate, which resulted in 100,000 of the records being changed. And these were only the errors detected by subjects and acknowledged by the company.51 A 1990 sample of credit reports done by Consumers Union uncovered "major inaccuracies" in 19 percent of them.52 In 2004 the National Association of State Public Interest Research Groups, in a study of consumer credit reports, estimated that as many as 79 percent of those reports could have some error and 25 percent of the reports could have an error serious enough to lead to the denial of credit.53 A comprehensive study of the reliability of credit data done by the Federal Reserve Bank, also in 2004, while acknowledging the prevalence of errors in the data, found that the overall impact of the errors on the credit scores of the consumers affected was “modest.” However, it also pointed out that the negative effects fell disproportionately on those who were most vulnerable, in that “individuals with relatively low credit history scores or those with thin files are more likely to experience significant effects when a data problem arises.”54

51 Burnham, pp. 44-45.
The errors in these massive databases, whether in the public or in the private sector, can be quite damaging. For example, Burnham describes the case of Michael DuCross, who was stopped for a routine traffic violation, when a check with the NCIC showed that he was AWOL from the Marine Corps. DuCross was arrested and held for five months before it was found that he had not been AWOL at all, but had been discharged legitimately. Burnham also tells the story of Lucky Kellener, who, after paying his brother's rent for him, was mistakenly listed in the court papers when his brother was evicted from his apartment. When Lucky went to rent a new apartment for himself, he was turned away by several potential landlords, until he finally found that, because he was named in the eviction notice, he was marked as an undesirable tenant by an investigative service often used by landlords. As another example, a man named Charles Zimmerman was charged 25 percent more than he should have been for medical insurance because a database used by insurers to investigate risk factors mistakenly identified him as being an alcoholic.

Inaccurate data can arise from simple data entry errors, from sloppy data collection at the source, or from the misunderstanding or misinterpretation of information, either at its origin or where it is used. Some of this is inevitable, given the volume of data involved; but those who collect and maintain the data contribute to it with their poor or nonexistent auditing and control procedures. A study by the OTA, for example, found that it is rare for federal agencies to audit data quality, and they generally have very low standards for accuracy. When TRW was sued for transmitting an inaccurate credit report, it argued that it had no legal obligation to ensure the accuracy of the information it had received from its sources. On the other hand, once the

---

55Burnham, pp. 33-34.
56ibid, pp. 34-35.
57Gary A. Seidman, "This is Your Life, Mr. Smith...: An Insurance Data Base Knows All. But Who Uses it? What If it is Wrong?" The New York Times, (August 1, 1993): 7.
59Burnham, p. 44.
information has been entered in the database, those who use it seldom question its validity. The attitude is, if it is in the computer it must be right. For example, the company that overcharged Mr. Zimmerman for his health insurance later admitted that it had not conducted its own investigation to verify the data on him in the database, although it was expected to, according to the policies of the bureau maintaining the database.  

Data can also be erroneous or misleading because it is incomplete. Sometimes the basic facts that are stored in the database may be accurate, but some critical supporting material is left out, either because it was neglected or unknown or because it did not fit into the database design. For example a credit record may show that a customer has unpaid credit card bills but not add the important qualification that the bills are in dispute and that is why they are unpaid. Based on the material in the database, the customer could be labeled unfairly as a bad credit risk. Data can also be incomplete because more recent facts relevant to the case have not been added. A crime database might show an outstanding warrant for someone without showing that the charges have since been dropped so that the warrant is no longer valid.

Another source of error is fraud. "Identity theft," in which malefactors collect enough personal information about victims to be able to masquerade as them, has been identified as the fastest growing crime in the United States. Criminals can obtain this information from a variety of sources. The most attractive targets are credit card numbers. Social Security numbers are also useful, because, combined with a name and birthdate, usually easily obtainable, they can be used to open an account or obtain other credentials in someone else’s name. Such information can be obtained by breaking into the victim’s personal computer; but it is far more productive to break into a corporate database that stores thousands of pieces of information. Or

60Seidman.

61 Rebecca T. Mercuri, "Scoping Identity Theft: The computer’s role in identity theft incidents may have been misgauged through overestimates of reported losses," *Communications of the ACM* 49(5) (May 2006), pp. 17-21.

one can purchase them from a third party who has already done the dirty work. So-called “carder” Web sites make this particularly convenient. Sometimes this data is mistakenly made public by its custodian, put on the Web through some error or oversight for anyone who wants to access it. Low-tech solutions work just as well. Credit card numbers, Social Security numbers and other identifying data can often be found on carelessly discarded records (“dumpster diving”) or obtained by calling the victim and impersonating a bank or other trusted agent and asking for identification (“phishing”). The thieves then use the victims’ data to impersonate them and obtain credit in their names, running up big bills and ruining the credit ratings of their victims. Usually the scam is not detected unless and until the victim is denied credit somewhere and decides to investigate. It takes even longer to correct the record. Sometimes these false identities are used when the impersonator is caught committing a crime, giving the victim an undeserved criminal record.

It is difficult in general to detect errors in databases. Usually the burden of identifying and substantiating the error is left up to the subject, the one to whom the data refers. It is even more difficult to get the database administrator to make the change. Moreover, because of the way data is shared among computers and propagated from one database to another, sometimes correcting the data in the original database is not enough. The bad data persists long after the correction has supposedly been made. As one example of that, Forester and Morrison relate the story of a man who was mistakenly arrested because someone had stolen his wallet, adopted his identity and subsequently committed a crime. Even after the victim was cleared of the charges, 

66 Mindy Fetterman, “Most ID theft takes place offline,” USA Today, (January 27, 2005), p. 5B.  
he was arrested five more times over the next 14 months. He then received a letter from the local authorities explaining that he was not a suspect in the crime, but still ran into trouble with law enforcement authorities when traveling in other states. It took a long court battle to get all traces of the erroneous record eradicated.\textsuperscript{68} In cases such as this, the data seems to take on a life of its own, beyond the control even of those who were originally responsible for it.

Even when data is correct, it can be misinterpreted because it has been removed from its original context. A man, for example, might file charges against his estranged wife as retaliation in a bitter domestic dispute. That would most likely be known by law enforcement officials in their local community. But if she were traveling elsewhere and officials looked up her record, they would only see that she had charges against her. They might treat her very differently in that case. The problem is that once the information is entered in the computer system, it becomes divorced from its source and from the context that gives it its significance. As a result the information can be misused and people mistreated because of it. An example of the danger of taking information out of context occurred in Massachusetts, where an elderly woman had her Medicaid benefits terminated because the balance in her bank account was greater than the maximum assets allowable under Medicaid. However, part of her balance was held in trust for funeral expenses, which by law should not have counted in the calculation of her assets. Yet the origin and purpose of the assets did not appear in the bank records, just the balance; and based on what was in the record she was denied the benefits to which she was entitled.\textsuperscript{69}

\textit{Data Aggregation}

One powerful new capability the computer gives us is the ability to compile large amounts of data from disparate sources to create a detailed composite picture of a person or to identify people who meet some criterion or stand out in some way. This has numerous uses and abuses.

\textsuperscript{68}ibid, pp. 90-91.

One application of this is with what David Burnham calls "transaction data." Now that many ordinary daily activities, such as making a telephone call, purchasing an item with a credit card, and renting a video, are computerized, the details of all of these transactions are recorded and saved. There are legitimate reasons for collecting this information: billing, inventory, predicting future needs and so on. But out of this mass of seemingly innocent details, an enterprising sleuth can assemble a revealing portrait of a person and his or her activities. Phone records can disclose a person's movements, friends, associates, business dealings, preferences and perversions. They could tell us, for example, that Jackie calls his mother every morning, his bookie at noon, and a phone-sex number at least three evenings a week. They can tell us that he was in Atlanta last week, where he spoke with a suspected drug dealer. Credit card records give details on one's travel, taste, habits, schedule and lifestyle. They can tell us that Ophelia likes Polo Sport perfume, Gap jeans, and underwear from Victoria's Secret, that she reads *Vanity Fair* and *Cosmopolitan*, that she just bought a new HDTV and that she has been to Paris twice in the past year. And when Robert Bork was nominated for the Supreme Court, we found out what can be learned from records of video rentals.

Online retailers such as Amazon.com collect similar data on their customers. Not only do they collect and store information on customers' purchases, but also on what they looked at on the Web site. This is used to build profiles of their millions of customers, which is then used to make personalized recommendations and place individually targeted ads whenever a customer visits their site. Large data brokers draw on many sources to build massive data bases with detailed records on hundreds of millions of consumers, then sell the information, quite legally, to a wide variety of marketers. One reporter described the largest of these, a little known company in Arkansas named Acxiom, this way: "It peers deeper into American life than the F.B.I. or the I.R.S. or those prying digital eyes at Facebook and Google. If you are an American adult, the odds are that it knows things like your age, race, sex, weight, height, marital status, education

---

70Burnham, pp. 55-56. Here he describes the government's use of phone records to investigate the rather unusual activities of Billy Carter during his brother's presidency.
level, politics, buying habits, household health worries, vacation dreams – and on and on.”

Search services like Google, AOL and Yahoo! compile vast amounts of data on the searches of all their visitors. These seemingly innocent little bits of data, when taken together, can be very revealing. From a person’s search queries, one could infer, rightly or wrongly, medical and psychological issues, legal problems, employment status, personal interests, sexual activities and preferences, relationships, fantasies, economic circumstances, geographical location and a host of other characteristics. Taken together they can suggest a fairly comprehensive portrait of a person, including that person’s most intimate problems and vulnerabilities. It may seem that this information is anonymous for unregistered users, but it is connected to the network address from which the queries come, so it can be traced to a particular computer. Moreover little bits of data called cookies left on the user’s computer by other interactive sessions, which can include logins and other identifying information, are often enough to uncover the identity of the user. Even without that information, the pattern of inquiries itself is sometimes enough to narrow down the user’s origins and identity, sometimes to a single individual.

As companies like Google have extended the services they offer to include email, document storage and processing, news, Web browsing, scheduling, maps, location tracking, video and photo sharing, voice mail, shopping, social networking and whatever else might be of interest to their users, they gain access to even more personal data, which they collect, store and cross-reference. Now a single database can have information not only on what searches one has done, but also all one’s emails and voicemails, what videos one has watched, one’s photos and who is in them, where one has been, what meetings and events one has attended, who one is in touch with and what information they have shared, what purchases one has made and a myriad of other

---

details, and can compile and analyze them to produce an intricate profile that includes every aspect of one’s life, including the most intimate details. This has prompted one critic to claim, “Google knows more about you than your mother” and that the company “is expecting consumers to trust it with the closest thing to a printout of their brain that has ever existed.” Polls have shown that while consumers continue to expand their use of these services and therefore entrust more and more personal data to them, they are growing uneasy with that information being used to build detailed profiles of them, even if just to provide more personally relevant ads and services. It is not surprising, then, that there have been a number of legal actions, in both the U.S. and Europe, that challenge changes made in Google’s privacy policy that allow it to integrate user data across applications without the subject’s consent.

The data accumulated and stored by Facebook and other social networks can also be very revealing, especially when compiled and analyzed to find patterns and correlations. A great deal can be inferred about a person from his or her associates or “friends” and their circles of “friends,” as well as all the thoughts, reflections, activities, commitments, “likes” and other information shared among them. As just one example, a couple of MIT researchers, by analyzing the Facebook profiles of some 4000 students, were able to tell with a fair degree of accuracy (78 percent) which ones belonged to gay males. As with sites such as Google and Yahoo!, the myriad bits of information collected by Facebook can be used to compile a detailed and penetrating profile of an individual, one that is if anything even more personal. In the hands of a

77 John Ribeiro, “Google faces class action lawsuits against new privacy policy: Google's new privacy policy is already under scrutiny in the U.S. and Europe,” Computerworld, (March 22, 2012), http://www.computerworld.com/s/article/9225406/Google_faces_class_action_lawsuits_against_new_privacy_policy
company that professes a philosophy of “radical transparency,” this can leave the subject very vulnerable, not just to having personal information exposed but to being discriminated against because of it.\textsuperscript{79}

Even information that is accessible to the public, when assembled from different sources into a comprehensive dossier, can create a revealing picture of a person. A simple Google search can turn up an enormous amount of information about an individual, though the accuracy of much of it is questionable. As one researcher put it, “while the quantity of publicly available information about individuals to be found online is vast, it is riddled with inaccuracies.”\textsuperscript{80} If one is willing to pay, even more is available. A "credit header," which is available for a small fee to anyone who has, or claims to have, a business interest in a person, gives the person's Social Security number, date of birth and list of addresses. With the Social Security number, it is possible then to obtain the person's driving history. For a little more money an investigative service will find the person's criminal history, education and employment record.\textsuperscript{81} A careful search of court records, many of them now online, can also reveal the person's history of marriages and divorces, civil suits, property holdings, liens, bankruptcies and so on.

The capability the computer gives of being able to assemble these seemingly innocent and insignificant facts into a comprehensive personal profile and to make it widely available gives that information a different significance. Even though limited groups of people may have legitimate reasons to have access to some of those facts for specific purposes, when the facts are all put together into a dossier they become much more personal and invasive. They thus present many of the dangers of other invasions of privacy. The information can be used for purposes other than those for which it was intended. For example information provided for billing

\textsuperscript{79} Lori Andrews, “Facebook is Using You,” \textit{The New York Times}, (February 4, 2012), \url{http://www.nytimes.com/2012/02/05/opinion/sunday/facebook-is-using-you}.

\textsuperscript{80} Robert L. Mitchell, “What the Web knows about you: How much private information is available about you in cyberspace? Social Security numbers are just the beginning,” \textit{Computerworld}, (January 27, 2009), \url{http://www.computerworld.com/s/article/9125058/What_the_Web_knows_about_you.html}.

purposes can reveal a person's movements, whereabouts and habits. The subject loses control of who knows what about him or her and what they do with it. And strangers can get a much more intimate look at the person's life than the person would allow if consulted.\textsuperscript{82}

In addition, when a determined inquirer can get such a comprehensive picture of a person, whether accurate or not, there is an increased danger of misuse, prejudice and discrimination. Often the purpose of such investigations is to make judgments about people. Someone could be denied a mortgage, a job or health insurance because his or her profile fits the pattern of a "high risk" prospect. The person may live in the wrong neighborhood, associate with the wrong people, hang out in the wrong places or have a suspicious history. Certain young children may be judged "at risk" because of the personal profiles the school or the state has developed on them, and placed in school accordingly. That designation could then follow those children through school, denying them the chance to develop normally with their peer group. Whole neighborhoods, families or ethnic groups could also be subject to discrimination because they have "dangerous" profiles, a practice that has come to be known as "Weblining," by analogy with the practice of "redlining," where certain neighborhoods were deemed not eligible for mortgages because of their demographics.\textsuperscript{83}

Apart from the obvious potential for error and prejudice, this use of profiling is objectionable because it dehumanizes those being judged, as well as those making the judgments. It substitutes calculation for human judgment on what should be very sensitive human issues, and thus treats those profiled as objects, as collections of facts, rather than as persons.\textsuperscript{84}

\textsuperscript{82} Jaikumar Vijayan, “Online Data Broker Spokeo Settles FTC Charges for $800,000,” \textit{Computerworld}, (June12, 2012),
\url{http://www.computerworld.com/s/article/9228024/Online_data_broker_Spokeo_settles_FTC_charges_for_800_000}.


One of the great advantages of the computer is that it provides such easy access to data, through powerful search facilities, ease of communication, and sophisticated analysis capabilities. When the data is sensitive and personal, however, this can lead to serious abuse, because it opens the way for the data to be used for purposes quite different from its intended use. This can happen for a number of reasons. The rules governing who can use the data and for what purpose may not be clear or restrictive enough to protect the intentions and interests of the subjects. Or those who control the data may not enforce the rules. Or they may not have sufficient control over who accesses the data. Whatever the reason, this can lead to severe problems.

Potential employers, for example, have a great interest in the medical, financial and criminal records of applicants. They often request and receive such information. A congressional survey in 1978, for instance, found that 20 percent of the criminal history records given out by the states went to private corporations and government agencies not involved in criminal justice. Employers can also obtain credit records, medical and insurance records, and histories of workers' compensation claims. If they are willing to pay investigative services that operate outside the law, they can also get bank records, credit card charges, and IRS tax records, among others.

Some of this information is no doubt relevant to employment decisions. One should not hire a convicted child molester as a day care worker. But much of the information is not relevant, and its use can be discriminatory and unfair. An arrest without a conviction should certainly not

---

85 For example, an audit by the General Accounting Office of the information system for the Federal Family Education Loan Program, published on June 12, 1995, found that the system "did not adequately protect sensitive data files, applications programs, and systems software from unauthorized access, change, or disclosure." See also Robert S. Boyd, "In Cyberspace, Private Files are Becoming an Open Book," *The Houston Chronicle*, (December 8, 1995), p. 3.

86 Burnham, pp. 78-79.

87 Rothfeder, "Invasion of Privacy."

88 Ibid.
be grounds for denying employment. Lots of people get arrested for all kinds of reasons, most of which have nothing to do with their employability. Yet, as noted earlier, studies show that many employers will reject an otherwise acceptable candidate if the candidate has an arrest record. Even if there was a crime, if it was minor, unrelated to the responsibilities of the job in question, or far in the past, it should not determine whether someone should be employed or not. That can make large segments of the population unemployable. Furthermore it can make it impossible for those who want to turn their lives around to do so, since their pasts follow them around and frustrate any attempts to change. In the same way, information from medical records or insurance claims, such as disabilities or past illnesses, should not be used to refuse employment, yet they often are. Thus the easy availability of this kind of information frequently leads to unfair and discriminatory treatment of those seeking employment.

In addition employers can often gain access to employees’ and applicants’ profiles on social media, including photos, comments, histories and lists of associates, either because the subject did not make them private or because someone who had access made them available. Some of this information, though it may seem innocent enough in context, such as pictures taken at a party, can compromise the subject’s professional identity. Or the employer may see remarks critical of the company or its management that was meant only for a few trusted colleagues. This violates one of the fundamental principles of privacy, that a person must be able to control how much personal information is revealed to different parties, depending on the nature of the relationship and level of trust with each one.

Marketers have an immense appetite for personal information too. They use collective data, along with sophisticated statistical analysis techniques and psychological models, to predict peoples’ purchasing preferences and behavior and to identify those factors that most strongly influence consumers’ loyalty and choices. They then combine this intelligence with detailed

89 Silverstein, "Applicants: Past May Haunt You."
information on specific individuals and subgroups of consumers to try to engage them and influence their buying decisions. Not only do they want contact information, such as names, addresses, phone numbers, email addresses and net IDs, but also more personal information, such as shopping habits, amount of assets, type of car owned, family situation, age, gender, and so on, to target and adapt their advertising. This information can be purchased from credit agencies, motor vehicle departments, the post office and many other sources, as well as gleaned from public records. It can also be generated internally. Supermarkets, department stores and other retailers can now keep track of the items purchased by each customer, both online and in-store, and, if the customer uses a credit card, bank card or store identification, can link the purchases with the customer's name and address, age, gender and other characteristics. But the richest and most lucrative source of information, as well as direct contact with consumers, is through information portals like Google and social networks, particularly Facebook. This information can be used to personalize ads according to the characteristics, circumstances and preferences of each individual, especially when the ads are delivered directly online. Now, with the development of mobile apps that track a user’s location in real time, the ads can even be adapted to the recipient’s current location.  

There are some advantages to this kind of targeted marketing. It has the potential to get specific information about products to those who are most likely to use it and to craft it in a way that is most appealing to them. Thus consumers will find out about the products they are most likely to want. Moreover, the data can help retailers and providers of services to understand their markets much better and develop products that best meet their customers’ needs and desires.  

Advertisers can get a larger payback on their investment because they can identify and reach

---


their target audience more efficiently and effectively. Because the detailed and personal data is so valuable and because the ability to reach the target market directly online is so desirable, services such as Google and Facebook, which both provide the data and serve the ads to the intended recipients, are paid well for their part in the process. Indeed targeted advertising is by far the greatest source of revenue for their businesses and what makes it possible for them to provide their services to their users free of charge. The idea, therefore, is that in taking advantage of the free services, the users in return agree to give the company access to their personal information, which it then uses to generate revenue that covers the cost of providing those services. It seems that everyone benefits.

The arrangement is legitimate as long as the users have knowingly consented to the collection and use of their personal data and that use is limited to what was agreed to. However, in many cases it is questionable whether these conditions have been properly met. Many users of these services do not realize that service providers are constantly monitoring users' online behavior and the information they store and communicate through the site, storing, compiling and analyzing the results, using it for the service's own purposes and sharing it with others. The companies point out that this information is contained in their terms of service and/or privacy policies, and claim that anyone who uses the service implicitly agrees to those terms. However, the policies are generally very long and complex. In many cases the user is not required to read them, let alone take some positive action to acknowledge that he or she accepts the terms. Also the conditions are often all-or-nothing. Either users agree to surrender all control over their personal information or they cannot use the site. Moreover companies frequently change their privacy policies and practices without giving users adequate notice. Facebook, for one, has done this a number of times. In particular in 2009, Facebook users were stunned to find out that

personal information they thought was available only to their chosen “friends” had been made public. Google has also run into trouble a number of times for changing its privacy policy or practices. 96 Just recently, in response to pressure from governments, consumer groups and other critics, some companies have begun to give users better control over how and where their information is collected, stored and used, through providing “opt-out” provisions and finer privacy controls. 97

Even when users give consent, it is questionable whether they do so freely and knowingly. As one critic put it, “too much is made of consent in this context. To be meaningful, consent must be informed and freely given. However, most users are probably not aware that their transactions with Google leave a personally identifiable, permanent track record, much less agree to such a result. Thus, user consent is not well-informed, nor is it freely given.” 98 Moreover, since similar sites all have essentially the same policy, any user who wants to use a search engine, virtually a necessity today, has to accept that searches will be monitored, stored, aggregated, cross-referenced, analyzed and used for unspecified purposes. The situation with social networks is even more restrictive. If one wants to connect with people, and increasingly institutions, who are on Facebook, which now encompasses most of the U.S. population and an increasing percentage of the rest of the world, one has to be on Facebook. Opting out is not a serious option for many. This is a “market failure,” because consumers really have no power to negotiate and are therefore forced to accept whatever terms the companies set. 99

An even greater concern is these sites’ selling or other transmission of users’ personal data to


98 Tene, op. cit., p 1469.

99 Schwartz, op. cit., p. 2076.
third parties without users’ effective knowledge or consent. This is a serious point of tension between online retailers, search and information services and social networks, and those who care about privacy. For those companies especially that provide free information and communication services to their users, the data they gather from those users are their greatest resource, and turning it into revenue is at the heart of their business model. Therefore they want as few limits as possible on what they can do with that data; and their privacy policies reflect that. For example, one generally sympathetic chronicler of Facebook has noted, “The reality is that nothing on Facebook is really confidential. The company’s own privacy policy is blunt on this score. Any of your personal data may become publicly available.” Even when companies give assurances, as Google and Facebook currently do, that they do not sell their data to unaffiliated outsiders, it is still available to their advertising “partners,” which gives the companies, not to mention the subjects of the data, even less control over where it goes and how it is used. Moreover it can be commandeered by government bodies for use in surveillance, investigations, and criminal and legal proceedings. The record of these companies in defending user privacy against government intrusion has been mixed at best. Most users have no awareness that their personal thoughts, interests and habits are so exposed. “When you enter a search query in Google you simply do not expect it to haunt you in criminal or civil proceedings, nor do you expect it to be transferred to third-party businesses for marketing or data-mining purposes.”

Defenders of the unconstrained collection, storage and use of users’ personal data claim that

100 Joel Stein, “You Data, Yourself: Every detail of your life—what you buy, where you go, whom you love—is being extracted from the Internet, bundled and traded by data mining companies. What’s in it for you?” Time, (March 21, 2011), pp. 40-46.
102 Loek Essers, “Online services increased their efforts to protect user data, EFF says: The Electronic Frontier Foundation hopes to stimulate transparency and encourage companies to stand up for user privacy,” Computerworld, (June 1, 2012), http://www.computerworld.com/s/article/9227663/Online_services_increased_their_effort_to_protect_user_data_EFF_says.
103 Tene, *op. cit.*, p. 1489/
in this networked world, where everyone is living online and putting their personal lives out there for everyone else to see, people no longer care about privacy, especially teenagers and young adults. As former Sun Microsystems’ CEO Scott McNealy famously said, “You have zero privacy anyway. Get over it.”\textsuperscript{104} Yet the data belies those claims. A 2010 study by the Pew Research Center found that “More than half (57 percent) of adult Internet users say they have used a search engine to look up their name and see what information was available about them online, up from 47 percent who did so in 2006.” Moreover the study found that young adults are even more careful about what they reveal about themselves online and with whom than older users.\textsuperscript{105} MIT scholar Sherry Turkle, in a thorough and thoughtful study of how teenagers use and are affected by social networks, found that those she studied were very careful and intentional about how they crafted their online identities. These young people cared a great deal about their privacy, but were often naïve about the rules under which they were operating and about how their personal information could be used.\textsuperscript{106} Their age and lack of experience and wisdom leaves them very vulnerable to exploitation. Furthermore, they are at an age when they are discovering and defining their identities. They need room to experiment, explore and, inevitably, make mistakes. It is essential that they have a safe, protected space in which to do this. That is why privacy is especially important for adolescents.\textsuperscript{107} Their participation in social networks and other online activities should not be taken as permission to collect, use and broadcast their personal information. This becomes even more of a concern with reports that Facebook is considering allowing children under 13 to join.\textsuperscript{108}


\textsuperscript{105} Mary Madden and Aaron Smith, “Reputation Management and Social Media,” Pew Internet & American Life Profect, (May 26, 2010), \url{http://pewInternet.org/Reports/2010/Reputation-Management.aspx}.


\textsuperscript{107} \textit{Ibid}, p. 260.

\textsuperscript{108} Brandon Bailey and John Boudreau, "Facebook explores alternatives to banning kids under 13," \textit{San Jose Mercury News}, (June 5, 2012), \url{http://www.mercurynews.com/business/ci_20779017/facebook-tests-accounts-pre-
Another abuse of privacy is the publication or distribution of supposedly confidential information. Many public figures have been victimized in this way. For example, in 1992, when Rep. Nydia Velazquez was running for office, information from her hospital records, including a record of a suicide attempt, was taken from the computer and leaked to the media.\textsuperscript{109} In a less public but more extensive case, an investigation by the Internal Revenue Service found that hundreds of IRS employees were accessing information on tax returns without justification, in some cases out of curiosity about friends, neighbors, antagonists or celebrities, in other cases to check up on business associates, and in some cases to alter the tax returns.\textsuperscript{110} There have also been many cases of hospital employees and others looking up the computerized medical records of patients without authorization.\textsuperscript{111}

The heavy reliance on electronic communication also leads to greater possibilities for outsiders to tap into sensitive personal information. One spectacular example of this abuse is the British phone hacking scandal, where it was revealed that reporters at Rupert Murdoch’s \textit{News of the World} had been accessing the voice mails and phone records of hundreds of subjects, including members of the Royal Family, and using the very personal information thus gained in published stories. Those charged claimed this was routine practice among the British tabloids.\textsuperscript{112}

What characterizes all of the situations in this section is that personal data is used for purposes other than those for which it was intended. This is a serious attack on the autonomy and dignity of the individual subject. If someone reveals personal information as part of an application for a credit card, it is because the person decides it is worth the benefit, and because the person is establishing a relationship of mutual trust with the credit provider and its agents. It

\textsuperscript{109}Rothfeder.


\textsuperscript{111}See, for example, Alison Bass, "Computerized Medical Data Put Privacy on the Line," \textit{The Boston Globe}, (February 22, 1995): 1.

should be the same with an online retailer, email provider, search service, or social network. If the holders of the information provide it to an employer or sell it to a marketer without authorization, they are violating the intent of the subject and committing a breach of trust. A patient gives a hospital permission to keep a medical history with the expectation that it will facilitate medical care. If this very sensitive and personal information is handed over to an employer or appears in the newspapers, the patient has lost control over an important aspect of his or her life. In effect part of the patient's person has been taken away and used for someone else's purposes and benefit. When that happens, the reaction is often that of Rep. Velazquez, who said she felt "violated" when her medical history became public knowledge.

Matching

Matching is the comparison of personal data from two or more different sources in a search for anomalous conditions. The anomaly might be the existence of a person in two different data sets where that is not expected or allowed. For example, persons drawing welfare or unemployment benefits should not also appear in a list of workers currently employed by the federal government. If they do, the presumption is, they are "double-dipping," drawing benefits fraudulently. Or, the anomaly might be the presence of the person in one set of data and absence in another, where any person in one should be in the other. When registration for the draft was mandatory for 18-year-old males, for example, a list of males over 18 years of age holding drivers licenses might be checked against a list of draft registrants to see if any in the former list were missing from the latter. Finally the anomaly might be an inconsistency in the data for the same individual in two different data sets. The Internal Revenue Service, for example, might be interested in a discrepancy between the income declared on an individual's tax return and the income listed for the same individual in an employer's records.

These searches often involve looking for matches among millions, even hundreds of millions, of records. It is the processing power of the digital computer and the existence of voluminous computerized databases that make them feasible. In order to identify matches reliably, it is also
necessary to have a way of identifying individuals that is unique and consistent across all the databases to be compared. Names do not work because different individuals can have the same name. In the United States the identifier most often used is the Social Security number (SSN). That is one of the reasons why so many different institutions, both in government and in the private sector, require that clients supply their SSNs. Most other countries have some kind of national identification numbers that all citizens are required to have.

In the United States, computer matching has been used extensively since the 1970s to check recipients of benefit programs for possible fraud and abuse. By 1982, there were about 500 different matching searches carried out regularly by state and federal agencies. These were tied to government attempts to make benefit programs less wasteful and thereby to reduce their drain on state and federal budgets. A number of federal laws, for example, require that states implement matching programs if they are to receive federal funding for welfare programs. As a result welfare recipients are often subject to matching. For example, those receiving Aid to Families with Dependent Children (AFDC) are checked against "data from state income tax, motor vehicle registration, school records, correction files on inmate status, veteran records, worker's compensation, and low income home compilations together with bureau records from employers, banks and credit agencies," in order to find conditions that might make them ineligible. The welfare reform bill passed in the early 1990s, responding to the popular concern over the welfare costs caused by parents, mostly fathers, who abandon their children, requires that lists of parents who default on child care payments be checked against "Directories of New Hires" to be set up in every state and nationally. In both these cases, it should be noted, the search includes records from the private sector as well as government records. The Social Security Number is almost always the linking identifier.

113 Clarke, "Information Technology and Dataveilance," p. 504.
114 ibid, p. 504.
116 Boyd, "In Cyberspace, Private Files are Becoming an Open Book," p. 3.
Matches are used to try to increase revenue as well as control costs. The Internal Revenue Service checks tax forms against local government and private employer records to try to catch undeclared and underreported income.\textsuperscript{117}

Matching can also be used for enforcement in areas not directly tied to the budget. During the Vietnam War, matches were run against various lists of males who should be eligible for the draft to try to catch draft evaders. Since 9/11, the Department of Homeland Security, the FBI and the Defense Intelligence Agency, among others, have carried out numerous searches that sift through massive amounts of data from a wide variety of sources, including Internet searches, looking for anomalies that might be signs of terrorists and terrorist activities. These searches involve U.S. citizens as well and foreign nationals. This activity continues even though Congress recently killed a similar effort because of concerns about privacy and civil rights.\textsuperscript{118}

With the development of facial-recognition technology, the use of matching has extended into databases of photos and videos. For example, one type of program used by at least 34 states, combs through databases of driver’s license photos, looking for matches that might indicate that someone has created a second, false identity. Unfortunately the program creates false positives that cast suspicion on innocent people, sometimes with dire consequences. The same technology is being adopted in many other areas, as well. The State Department, for example, uses it to check visa applications; and now some police departments are preparing to use facial recognition to take pictures of people they encounter and check them against databases of known offenders.\textsuperscript{119}

The United States is not alone in its use of computer matching. In Germany personal data linked through Social Security numbers is used to expose fraud and regulate the work permits issued to foreigners. In Australia a national identification system permits the government to

\textsuperscript{117}Simits, p. 716.
match data relevant to taxation. Sweden also uses extensive data collection to support the tax system.\textsuperscript{120}

It is easy to see why matching is attractive to government authorities. They cannot investigate individually the millions of taxpayers and welfare and Social Security recipients they deal with every year. Matching provides a very efficient way of detecting possible cases of fraud and abuse. It has helped catch people who have been receiving welfare benefits for which they were not eligible, found health-care providers who were double-billing Medicare, and detected thousands of cases where Social Security checks were being sent to deceased beneficiaries. In 1984 Richard Kusserow, the head of the federal Department of Health and Human Services, claimed that in one year matching programs contributed to $1.4 billion in savings by his department.\textsuperscript{121} The potential of matching to uncover terrorist plots is also attractive to many.

Nevertheless, matching raises some serious problems. One is reliability. Whatever the problems are with maintaining a single data file on a group of individuals, they are far worse when trying to relate two or more separate ones with different origins and administrators. Social Security numbers and other identifiers can be misread, mistyped, intentionally falsified or missing altogether. This can lead to many missed matches and false matches. Files can have different formats or coding systems, so that data in one or both files are incomparable or subject to misinterpretation. Data can be out of date, incomplete or in error. Moreover the problem of taking the data out of context is far more serious. What comes out of a matching program is usually just a list of identifiers for records that matched (or did not match) in the two data files. Therefore not only is the data divorced from its original context and meaning, but the list of matches is removed from the data that gave rise to it. This makes it even more likely that the users will draw false conclusions from it.\textsuperscript{122} Trying to match photos of faces has its own set of

\textsuperscript{120}Simits, pp. 716-17.
\textsuperscript{122}Clarke, p. 506.
problems and inaccuracies. Even the best-trained human experts are often wrong.

An incident some years ago in Massachusetts indicates how unreliable matching programs can be. In 1994 the state ran a search to find families that were receiving welfare benefits simultaneously from Massachusetts and another state. They found 642 "hits," which supposedly meant that those families were receiving benefits illegally. However, when the state tried to cut off benefits, several of the families sued, and the court found that at least 378 of the 642 families identified were mistakenly accused.\textsuperscript{123} Unfortunately cases such as this with error rates of 50 percent or more are not that unusual. When the US Department of Health, Education and Welfare ran its list of welfare recipients against a list of its own employees to find welfare cheaters, it generated 33,000 matches. After a year of investigation, this was reduced to 638 cases of possible fraud, and of these only 55 were taken to court.\textsuperscript{124}

The above cases highlight another problem with matching programs: lack of due process. Matches in themselves are often interpreted as evidence of wrongdoing. Therefore in welfare investigations, for instance, authorities will move to cut off benefits for those identified by the matching program. The accused must then go to court to get the benefits restored, an expensive and time-consuming process, during which the accused may have no means of support. Thus those identified by the program lose their right to the presumption of innocence based on the outcome of a machine sifting through millions of records, without any human being looking at their case or checking the validity of the outcome. The burden of proof is shifted to the accused, which is unfair, especially given the unreliability of the matching procedure.

There is a more fundamental objection to matching, which addresses the nature of the activity, quite apart from any consequences. The problem is that a matching program accesses the personal information of large numbers of people, mostly innocent, without their knowledge or consent. Often information given by the subject for the purposes of credit, banking, employment, education or health care is used to check on compliance with government

\textsuperscript{124}Clarke, p. 508.
programs. On the face of it, this is a violation of the subjects' autonomy. Furthermore people are accused of wrongdoing and subject to sanctions based on the outcome of a computer program looking for certain conditions in a large volume of data. This reduces people to collections of facts, or, worse yet, computer codes, which is a violation of the obligation to treat them as persons. Some critics, like John Shattuck, also argue that matching violates the right to freedom from “unreasonable searches and seizures” protected by the Fourth Amendment of the United States Constitution, which decrees that the government is only allowed to investigate people when it has an indication that they are involved in wrongdoing. It was directed against mass house-to-house searches and arbitrary “stop-and-frisk” operations on the street. The argument is that combing through the personal data of large populations looking for anomalies is the same kind of arbitrary intrusion into innocent people's lives.125

Those who defend matching, on the other hand, claim that when people apply for welfare or Social Security, or pay their taxes, they implicitly give their consent to using relevant data for checking on their eligibility. This is the argument made, for example, by Rubin E. Cruse, Jr., in an article in the *Computer/Law Journal*.126 According to Cruse, when people apply for benefits, they must reveal their incomes and assets. Therefore when the government checks records of such data, it is simply looking at information that the applicants have already consented to give. Furthermore the government only gains new information on people who gave false information on their applications. It is only the wrongdoers who are identified by the matching process. The others and their data go unremarked. And those who have been shown by the matching process to have discrepancies in their data can legitimately be investigated, because there is now evidence that they have been involved in wrongdoing. Implicit in this argument is the assumption that when personal data is run through a computer with no human monitoring, there


is no violation of confidentiality, except for the data that is reported out.

The case of taxpayers is similar, Cruse argues. When they file their tax returns they disclose to the IRS their incomes. When the IRS checks these figures against income reports from employers, banks and so on, it is not gaining access to any information that it does not already have unless there is a discrepancy between self-reported income and income listed in other sources. But in that case there are grounds for an investigation.

This clever argument does capture the sense most people have that privacy and confidentiality should not be a cover for fraud. It depends, however, on an interesting philosophical assumption that not everyone would grant. It assumes that there is no access to records except when someone looks at them. But when a government agency runs a match on data from another source, particularly in the private sector, the government does appropriate the personal data of many thousands or even millions of people, most of whom have no reason to be subject to an investigation. And it is only when the run is finished that government knows which subjects are suspect. Furthermore, the argument that the investigators only look at the records of those whose data is suspicious assumes a high degree of reliability in the matching process. As we have seen, that is a difficult assumption to justify. If the error rate were 1 percent, or even 10 percent, it might be possible to claim that a "hit" was enough to throw suspicion on the subject. But when the error rate is 50 percent, or 90 percent, that is not such a convincing assertion.

Even if we grant its underlying assumptions, the argument that matching has the implicit consent of its subjects is valid only under limited circumstances. First it must be used only on people who have provided information, either freely in return for some benefit, or in response to some legitimate government mandate, such as paying taxes. Second it can be used only to verify information that the subjects have provided. And third, the possibility of a matching program and accompanying investigation must be known and understood by the subjects when they provide the information.

Institutional Power
As we have already noted, one of the purposes of privacy is to maintain a balance between individual freedom and institutional dominance. And one of the dangers of the information processing power of the computer is that it can be used to upset that balance.

Computer power is available to anyone who can afford it; but it is predominantly large institutions that have the resources to obtain it and many will use it as a means of control. Bureaucracies value efficiency, predictability and uniformity. It makes their jobs easier. And a certain amount of regularity and authority is beneficial to society. But society also needs diversity, freedom, dissent, creativity, even a certain amount of mischief. It hurts society as well as individuals when control is too rigid and all-encompassing.

The most obvious agent of control is government. In the name of security and enforcement of the obligations of citizenship, governments are always on the lookout for those who show abnormal social behavior, as noted earlier. But control is an issue in the private sector as well. Employers now use computers to screen and monitor employees. The employers contend that the monitoring information is needed to make their operations more efficient, to gain more reliable information about employee performance and to hold employees accountable. But many employees experience it as intrusive and controlling.

Many employers also monitor employees' electronic mail and online activity. As far back as 1993, a Macworld survey of companies in a variety of industries found that 21.6 percent of the companies searched employees' computer files, electronic mail and other electronic communications. Less than 10 years later, a survey by the American Management Association found that the percentage of employers monitoring their employees had almost quadrupled to 78 percent.

A frequent target of this monitoring is employee email. Email monitoring is relatively easy for employers, because electronic mail messages are stored as files on computers owned and

---

operated by the company. Normally either the messages are kept on a centralized computer waiting for employees to read them, or they pass through such a computer in transit. In either case the messages can be copied, stored, read and passed on to superiors by a system administrator or automated process. Even if the messages exist only on an employee's desktop computer, they can usually be accessed over a network.

There are a number of reasons why employers might want to monitor employees' email. It might reveal fraud, theft of intellectual property or other illegal activities. For example the software company Borland International used recovered email messages as part of an investigation leading to criminal charges against a former employee for stealing trade secrets.\textsuperscript{129} Email monitoring can also alert employers to employee activity that is wasteful, disruptive or against company policy. In 1990, for instance, two employees of Nissan Motor Corp. were fired when supervisors reading their email found they were receiving messages that were "sexually suggestive."\textsuperscript{130} Companies are increasingly finding it necessary to watch for and regulate emails and other online workplace communications that could be taken as harassing, in order to protect their employees and protect themselves from liability.\textsuperscript{131} Even when there is no question of wrongdoing, email monitoring can help employers assess employee performance, by showing how employees are spending their time, what they are accomplishing, and so on. Or it can help managers track the progress of a project by seeing what work is being done, what problems have been encountered and what responses have been tried.

Some companies also have more comprehensive monitoring of employees' online activities while they are in the workplace. They track what programs employees use, what Web sites they visit, messages posted on bulletin boards, chat rooms and social networks, and so on. They can


even inspect files that are stored on company computers, servers and storage devices. They do this for many of the same reasons they watch email, to find and stop illegal and destructive activity and to assess employees’ performance.

Employers generally claim ownership of employee email. They argue that because it is created, transmitted and stored on company systems, generally on company time, they should be able to inspect it. They make similar claims about other online employee communications when they use company-owned computers and the company’s network. This has generally been accepted by the courts, as long as employees are informed that they are being monitored and they receive due process before any punitive action is taken.132

There are, however, some serious privacy concerns connected with monitoring employee email. Employees do use it for personal communications, usually with the expectation that it is a private medium. And, as studies show, there are aspects of email that encourage that sense of privacy. The user usually creates the message while working alone on a personal desktop system, using an email account that is password protected. Normally there are few sensible indicators that anyone but the addressee will have access to the message. Indeed, because computers seem so impartial and create a distance between human correspondents, many people find it easier to disclose personal information through the computer than via other media.133 To the user, then, email is not substantially different from telephone calls or personal letters; and in that mentality employers therefore have no more right to monitor email than to eavesdrop on telephone calls or open personal letters. It is generally recognized that the privacy of these more traditional media is protected both legally and morally. Why not email? One could make a similar argument regarding other private online communications and activities.

Another issue is the consent of the employees being monitored. Employers claim that employees know, or should know, that email and other communications are easily accessed and

133ibid, pp. 45-46.
intercepted, and that employers have reason and authority to do so. Therefore by using email on
the company system, employees are implicitly assenting to having the email inspected. This
argument does not hold up in all cases, however. Some companies do not have a stated policy on
monitoring. In the *Macworld* survey, for example, only 18 percent of the companies surveyed
said they have a policy on electronic privacy.\textsuperscript{134} If a company does not clearly inform employees
that all online activity is subject to inspection, they cannot assume that the employees agree to it.
Even if there is a stated policy that email will be monitored, the practice is still a threat to the
privacy of outside correspondents who send personal email to employees not knowing that it
may be read by others.

Finally online monitoring, like the other practices considered in this section, threatens to
upset the balance in the relationship between the institution and those that are subject to it. Even
employees have rights to a certain measure of privacy and autonomy, which must be balanced
against management's legitimate need for information about employee behavior and
performance. Shifting employee communication to a system that is much easier for employers to
monitor changes the balance. Management now has more access to employees' personal and
work lives, which gives management more leverage and control, leaving employees more
vulnerable. Granted that a company is not required to provide employees an electronic mail
system for personal use, once it is there, especially when employees are required to use it for
their work, there must be restraints on management to protect employees from too much
intrusion into their personal communications. Nor is it sufficient for management to warn
employees to use online communications only for work. Good employees invest their persons in
their work, and work relationships are also personal relationships. The two are not so cleanly
separable.

It is even more problematic when employers monitor employee activity on social networks
and other communication sites, when the activity takes place on the employee’s own time and

\textsuperscript{134}Piller, p. 7.
with his or her own equipment. Yet that is a growing practice. A 2012 study by Gartner found that about 10 percent of corporations monitored the postings of employees on Facebook, YouTube and other social media; but they expect that to grow to 60 percent by 2015. The companies’ main reason for doing this, according to the report, is to find instances of employees posting confidential information online. Businesses have a legitimate interest in protecting confidentiality; and one could make an argument that looking for potential security leaks is justified if the postings are public. However, employers have also been looking into employees’ or potential employees’ personal activities on social networks to see if they are doing anything that seems unprofessional there, as well as searching for critical remarks employees might be making about the company. This raises some serious privacy issues. As one critic put it, “Actually much of what is discussed [in the Gartner report] is unwarranted snooping in people's personal lives. There is no valid reason for it and companies that engage in such activities should be called out for their unethical activity.” Another pointed out that a company could be charged with discrimination if they seem to be basing personnel decisions on personal information involving protected areas such as religion or sexual orientation or attempting to suppress free speech.

Some employers have reportedly even gone so far as to require applicants for employment to submit their login and password information for Facebook and other social networking sites so the company can look at their personal data. This is clearly an invasion of privacy and has provoked a strong reaction from the public, which has been picked up by the government. The state of California, for one, passed a bill banning the practice; and there have been calls for similar legislation at the federal level.


136 Idem.

137 Cameron Scott, “California moves to stop employers demanding Facebook passwords: The move is part of a wave of legislative activity to block the practice,” Computerworld, (May 10, 2012), http://www.computerworld.com
Another area where computers give large institutions an advantage over individuals is in the use of massive databases of personal data, as discussed earlier. Banks and insurance companies try to reduce their risks by learning more about potential customers and weeding out those who, because of their history, neighborhood, ethnic ties, economic status or similar factors, seem that they might pose greater than normal risks. This creates a conflict between the companies' self-interest and society's goal of providing equal opportunities for health care, housing, economic advancement and so on to all its citizens. As the companies gain more power through computers to characterize and discriminate among potential clients, society's goals for equity are less well served.

Many of the data gathering and processing techniques noted already, such as matching and compiling dossiers, can be used to identify, investigate and suppress "deviants." Those who do not conform can be singled out, publicized, and pressured or ostracized. In many cases just the knowledge that such control can occur can have an inhibiting effect.

There are other computerized methods that have been developed to exercise social control. One is personal profiling. This goes beyond detecting behavior that is considered dangerous, threatening or expensive and tries to predict it. The idea is that historical data and sometimes presumptive rules are used to build a characterization of an ideal, normal or acceptable subject. Those who differ too much from the norm or fall outside the limits of acceptability are then pressured to conform or excluded from participation.

For example, in Germany data on medical costs were analyzed to build a model of patient behavior that would lead to the lowest costs. When patients did not conform to this model, they were contacted and asked to consult with a doctor about ways of controlling costs. In a number of countries, including France, Germany and Norway, data on the early childhoods of children who later showed troublesome behavior was studied to identify characteristics of the high risk child. Children who showed these characteristics were then subject to social and

/s/article/9227072/California_moves_to_stop_employers_demanding_Facebook_passwords.

138 Simits, p. 711.
medical interventions. In the United States, the Internal Revenue Service analyzes samples of tax returns to build a model of the potential tax evader. Returns that fit this model are then selected for audit.

With the increased ability to collect and analyze genetic material and to use it to predict medical and psychological risks, as well as future behavior and other outcomes, this activity could extend into even more sensitive and personal areas. This led the United States in 2008 to pass the Genetic Information Nondiscrimination Act, which prohibits employers and insurers from discriminating against applicants based on genetic characteristics. Nevertheless, with the growing use of genetic databases, there is still potential for abuse.

In these and similar cases, the objective is to identify and control people who might not fit the norm for a “good” citizen or client. This could prevent harmful, destructive or costly behavior. In some cases it could even be in the best interests of the people who are singled out for special treatment, such as the high risk children. Nevertheless the implications are ominous. These programs are intended to force conformity on the entire population. Everyone is subject to examination; there is no place to hide for someone who chooses to be different. There are the usual objections to using data without permission for purposes other than those for which it was intended. And most distressing of all, people are judged not on anything they have done, but on what a model predicts they might do. At best there could be some evidence that some individuals with similar profiles have caused some problems. At worst these individuals simply don’t fit some bureaucrat’s idea of a “model” citizen. There is too much room for injustice here. It leaves people who are different, for any number of reasons, vulnerable to discrimination, harassment and exclusion.

---

139 ibid, p. 713.
140 Clarke, p. 504.
Privacy and the Law

Most governments recognize the need to protect the privacy of their citizens, to some degree at least. These protections occur at different levels of government, and have different concerns and styles. In this section we will look at some of the ways in which privacy is protected by the law, particularly in the United States. We will consider common law privacy protection, the Constitutional right to privacy, and privacy legislation in the U.S. Then we will compare the situation in the United States with that in some other countries.

Common Law Protection of Privacy

As noted earlier, the Anglo-American case law tradition, as recognized in most states, offers some protection for privacy of personal information. It is illegal to reveal private facts about someone if the average person would find it objectionable to have that information made public, provided that the subject of the information is not a public figure and there is no legitimate public interest in making the information known. It is also an offense to place a person in a false light. It is not necessary that the false information ruin the person's reputation; only that it be objectionable. Appropriation of someone's name, image, or some other aspect of the person's identity is another offense. Finally intrusions, such as intercepting private communications, are also illegal, unless there is a legitimate reason for doing so or the parties to the communication have given consent. In any of these cases the victim can sue the perpetrator and recover damages.

Privacy and the Constitution

There is no explicit mention of privacy in the United States Constitution. But the courts have

---

142 The exceptions are Nebraska, New York, Oklahoma, Utah, Virginia and Wisconsin, where privacy rights are established by law. See Warren Freedman, The Right of Privacy in the Computer Age, New York: Quorum Books (1987), p. 12.

found a constitutional basis for privacy rights in the broad sense of freedom from interference in certain intimate realms of personal life. This is based on the protection of individual liberty from government interference in the Fourth, Fifth and Fourteenth amendments to the Constitution.\textsuperscript{144} The First Amendment protection of the freedoms of speech, assembly, religious practice, and so on, could also be seen as privacy protection in this sense. On the other hand, the right to free speech could be used to defend someone who invaded the privacy of others by publishing or disclosing their personal information.

Informational privacy has not been given the same strong constitutional protection by the courts to date. The Supreme Court, in \textit{Whalen v. Roe}, found that a New York law that required physicians and pharmacists to report all prescriptions of certain types of drugs to the state for storage in a comprehensive drug-use database, did not violate constitutional right, in spite of the protests of some patients and doctors involved that it was an invasion of privacy. The Court was willing to give the state interest in tracking drug use more weight against the individuals' interest in privacy because “informational privacy is not a fundamental right.”\textsuperscript{145} Therefore, though the courts recognize some rights to privacy of information, these must be balanced, case-by-case, against the public interest in disclosure. In one subsequent case, \textit{United States v. Westinghouse}, the Third Circuit Court worked out a “balancing test” for deciding between these competing interests. Some of the factors to be considered included what kind of information is sought, the harm that could be done by any further disclosure, the care taken to guard the information from any further disclosure, and the degree of public interest in its disclosure.\textsuperscript{146}

In 1967 in \textit{Katz v. United States}, the Supreme Court extended Fourth Amendment protections to include some types of electronic communications and therefore informational privacy. Katz was convicted of illegal gambling based on FBI recordings of phone calls he made from a public

\textsuperscript{145}ibid, p. 147.
\textsuperscript{146}ibid, p. 148.
pay phone. The recordings were made by a listening device placed outside the phone booth without a warrant. The appeals court allowed the conviction on the grounds that the FBI had not invaded a private space or tapped into a private network to obtain the evidence. The Supreme Court reversed the decision, finding that the recording of Katz’s conversations was a violation of his Fourth Amendment privacy rights. What was determinative, the majority said, was not whether the space he was in was public or private, but whether his conversation could reasonably be considered a private one. The justices concluded that making a telephone call in a phone booth with the door closed met the criteria. The Katz case gave rise to the “reasonable expectation of privacy” test that is still used today to define the limits of government surveillance.147 For example in January 2012 the Supreme Court overturned the conviction of an alleged drug dealer because it was based on evidence gathered from a GPS tracking device surreptitiously placed on his car.148

These cases have limited applicability and do not affect the private sector, where many privacy issues arise. Therefore there is a need for legislation to set clearer guidelines on when and to what extent personal information is to be protected. Over the last few decades the federal government has enacted a number of such laws. As a whole these are spotty: domain-specific, inconsistent and full of loopholes. Still, they provide some protection in certain areas. The four most important laws are the Fair Credit Reporting Act (FCRA), which is concerned with record-keeping in the private sector; the Privacy Act (PA), which regulates record-keeping by the federal government; the Electronic Communications Privacy Act (ECPA), which safeguards the confidentiality of electronic transmissions; and the Health Insurance Portability and Accountability Act (HIPAA), which protects medical records. Other laws cover more specific issues.

The Fair Credit Reporting Act (FCRA)

The FCRA,149 passed in 1970, was designed to protect consumers from information gathering in the private sector. Specifically it regulates credit reporting agencies, which collect data on consumers and their financial status and offer that data to business subscribers. The bill addresses several concerns about the reporting of credit information:

1. Knowledge of the subject. Individuals have a right to know what is in their records and who has accessed the information.

2. Inaccuracies. Credit agencies are required to take "reasonable" steps to guarantee the accuracy of the information they collect, store and report. An individual who is denied credit because of a credit report must be notified of the action and the source of the information. An individual may challenge the information in his or her record and have it changed if it can be proved wrong. If the individual is not satisfied with the agency's response to the challenge, he or she may place a statement in the record stating the reason for the challenge.

3. Out of date information. Certain damaging events cannot be reported after a set period of time: 10 years for bankruptcies, seven years for civil suits and criminal charges. However, there is an exception when the subject is applying for more than $50,000 worth of credit or insurance or for a job paying more than a certain amount.

4. Legitimacy of use. The bill defines the purposes for which a credit report can be given. These include the granting of credit, insurance, licensing and hiring. Reports can also be provided in response to a court order or with the consent of the subject. Unfortunately there is, in addition, a big loophole that allows anyone to purchase a report for a "legitimate business need."

Though the FCRA does give consumers some protection, it is widely recognized as inadequate, for a number of reasons. First, its scope is too narrow and its coverage too vague.

---

149 15 USC 1681-1681t.
For example, it is much too permissive about who can receive credit reports. Second, it puts the burden of finding and correcting errors on the consumers, not on the companies collecting and distributing the information. Furthermore consumers cannot actually inspect their files. They can only see a report about what is in them. Third, the consumer has no recourse until there has been an abuse. The bill does very little to prevent the abuse in the first place. Finally the bill only regulates the credit bureaus themselves, not those who purchase the information from them.\(^{150}\)

There is plenty of evidence that, in spite of the FCRA, it is easy to gain access to consumer credit information, with or without a "legitimate business need."

In 2003 Congress revisited the FCRA with the Fair and Accurate Credit Transactions Act (FACTA), adding some additional protections for consumers. For example credit reporting agencies cannot include medical information in their reports, and consumers must upon request be given a free copy of their credit report each year.

Other Laws Affecting the Private Sector

The Right to Financial Privacy Act (RFPA),\(^{151}\) dating from 1978, limits the government's access to the bank records of individuals. In order to see a customer's financial records, the government must have a warrant or subpoena or the customer's permission. The government may also make a written request for the records, in which case the customer is notified and may challenge the request. However, the government has broad access to identifying information, such as "name, address, account number and type of account."\(^{152}\) Furthermore the restrictions in the bill only apply to the federal government, not state agencies, corporations and private citizens.

The Fair Debt Collection Practices Act (FDCPA, 2003) curbs abuses by debt collection


\(^{151}\text{12 USC 3401-3422.}\)

\(^{152}\text{Freedman, } The Right of Privacy in the Computer Age, p. 14.\)
agencies, including harassing the debtor; calling third parties, such as family members or employers, who are not cosigners of the loan; and making false statements about the debtor. However, the so-called Bankruptcy Abuse Prevention and Consumer Protection Act of 2005 weakened some of these curbs.

The Cable Communications Policy Act\(^{153}\) (1984) controls a cable system’s collection and dissemination of transactional information on its subscribers. This information can include the programs ordered, information services used, items purchased through home shopping channels, and so on. The Act requires cable companies to inform their subscribers of what personal information is being collected and who has access to it. Furthermore it does not allow the companies to collect or disclose personal information on subscribers without their consent, except for what is needed to do business or in response to a court order. One exception is that names and addresses of subscribers can be given out, as long as the subscribers have a chance to withdraw permission to do so. Finally the Act mandates that subscribers have access to their records.

The Video Privacy Protection Act (1988), otherwise known as the Bork Bill, forbids video renters from revealing the rental records of their customers.

*The Privacy Act*

The Privacy Act (PA)\(^{154}\) was enacted in 1974, at the time of Watergate, to assert some control over the gathering and dissemination of personal information by the federal government. The law regulates information collection and use in several ways:

1. Agencies are to gather only the information necessary and relevant for their mission. They are to get it as much as possible from the individual to which it refers, and they are to inform the individual of the purpose and use for which the information is being collected.

\(^{153}\) 47 USC 551
\(^{154}\) 5 USC 22a
2. There is to be no disclosure of the information to anyone else without the consent of the individual subject. There are, however, a long list of exceptions to this rule, including employees within the agency that holds the data, Congress, the General Accounting Office, consumer reporting agencies, in response to a court order, for a “compelling” need to protect the health and safety of an individual, for use in census data, statistical studies, the archives, criminal law enforcement, and for “routine use,” meaning use compatible with the purpose for which it was given.

3. Agencies are to keep records of disclosures. If corrections are made to any of the data, previous recipients of the data are to be informed of the corrections.

4. Agencies are responsible for the accuracy and security of the data they hold.

5. The existence of any collections of personal data is to be published in the Federal Register.

6. Individuals are to have access to the information held about them. If they find the information erroneous, they can challenge its accuracy. A procedure is set up for resolving any disputes arising from such challenges.

The CIA, FBI and other law enforcement agencies are completely exempted from these regulations. There are also exemptions for agencies that use the data for law enforcement and security or for evaluating candidates for employment and promotion within the federal government.

The law in its present form also contains some minimal regulations for matching programs. It requires a written agreement and statement of purpose before any federal data can be used in such programs, procedures for the verification of results, and some general oversight of such programs by the federal government.

While the bill is commendable in its intent and some of the principles on which it is based are sound, it has been ineffectual. For one thing, it is leaky. There are many exceptions. Some, such as the provision for “routine use,” are so broad and open to interpretation that they can be used to justify almost anything. Furthermore the law never questions the need for data collection
programs. Any agency that decides it needs personal data can collect it. Finally the law is difficult to enforce and in practice has rarely been invoked. A great deal of information held by federal agencies is routinely available, not only to other agencies, but to state and local governments, private corporations and individuals. One critic has called the Privacy Act and Fair Credit Reporting Act “toothless vestiges of the precomputer age.”

Other Laws Affecting Government Record-Keeping

The Family Education Rights and Privacy Act (1974), controls access to student records at educational institutions. This is a very sensitive area, because these records can include not only grades and notations of disciplinary actions, but also psychological reports, family histories, personal data and teachers' observations and comments. The Act gives students, or their parents if the students are minors, the right to inspect the students' records and request corrections if needed. It also limits third party access to students' files.

The Privacy Protection Act (1980) is meant to help reporters for newspapers and magazines protect their sources. It limits the circumstances under which federal, state and local law enforcement agencies can seize records held by the print media. Either the one who holds the records must be suspected of criminal activity, or the information must be needed to prevent great harm, such as death or serious injury, or the destruction of evidence.

The Crime Control Act sets standards for privacy and security of information systems used in criminal justice agencies at the state level. Any state that receives federal aid to upgrade its system must implement these standards.

155 Rosenberg, p. 207.
156 Rothfeder, "Invasions of Privacy," p. 152.
157 20 USC 1221.
158 Rosenberg, p. 207.
159 52 USC 2000aa-11.
160 42 USC 3789g.
The Electronic Communications Privacy Act (ECPA)

The ECPA\textsuperscript{161} was enacted in 1986 as an addition to the Wiretap Act of 1968. It extended some measure of privacy protection to new communication technologies such as pagers, cellular phones, electronic mail and other forms of computer-to-computer communications.

The significance of the act, from the point of view of computer privacy, is that it forbids the interception, use and disclosure of any “electronic communication,” which includes electronic mail and other transfers of electronic data. There are, of course, some exceptions to this. For example system operators are allowed to monitor and store transmissions “in the normal course of ... employment,” e.g., as needed to forward the communication to another system, to diagnose problems in the system, or to prevent fraud or misuse of the system. Surveillance by law enforcement officials and their agents is allowed when properly authorized. Anyone who is a party to the communication, whether as sender or addressee, or has the permission of one of the parties, can intercept it. The prohibition also does not apply to systems that are set up so that communications are publicly accessible, such as electronic bulletin boards.

The act also has provisions to protect stored communications. It is unlawful to break into a system that is used for electronic communications; and it is unlawful for the operator of a system to disclose any electronic communications stored on the system except for the reasons listed above.\textsuperscript{162}

The act does not have any special provisions to cover employer monitoring of employee email and other communications. Before the passage of the act, the courts gave employers broad latitude in employee monitoring, including their communications. The main tests were whether there was a legitimate business purpose for the monitoring and whether employees had a “reasonable expectation of privacy.” As long as employers warned employees or employees had other reason to expect monitoring, it was allowed. The ECPA has not changed that

\textsuperscript{161}18 USC 2510.

significantly.\textsuperscript{163} Several employee lawsuits against email monitoring, such as the Nissan case mentioned earlier, have failed. It appears that the ECPA does not give added privacy protection to employees.\textsuperscript{164}

As mentioned earlier, the USA PATRIOT Act of 2001 weakened many of the protections against electronic surveillance, including those contained in the ECPA. It both expanded the scope of allowed interceptions of electronic communications and weakened judicial oversight. For example, authorities may now access routing information on packet-switched networks like the Internet, which often contains indications of the content of emails and Web pages. They can, with the permission of the operator, intercept communications carried out on computers that host interstate and foreign communications, which were previous protected. They can also subpoena not only subscriber data, but also details of use, from Internet service providers. The Act also greatly expanded the definition of who could authorize electronic surveillance and how broad the scope could be.

\textit{Medical Records and HIPAA}

Medical records contain some of the most sensitive material of any personal databases. They can include family backgrounds, psychiatric histories and evaluations, accounts of past breakdowns, suicide attempts, drug and alcohol use, physical and mental disabilities, and medication used. There are many parties that would like to know that information, including insurance companies, researchers, marketers, employers, legal adversaries, law enforcement officials, coworkers, the press and the curious. Not all of these have the patient's best interest at heart, and few have the permission of the patient to view the records.

Until 1996 there was no federal protection of privacy in medical records; and state laws varied widely. That changed with HIPAA. The purpose of HIPAA, as noted earlier was to


\textsuperscript{164}Sipior and Ward, "The Ethical and Legal Quandry of Email Privacy," p. 53.
encourage and facilitate a transition to electronic medical records. There are a number of advantages to this. The computerized records are more readily accessible to physicians and other health care workers, even at remote locations. When a traveler is brought to the emergency room far from home, doctors can check her records for past medical problems, current medication, possible allergies and so on. This can lead to better, safer care. Better-organized and more easily accessed records can also support more efficient billing, payment and reimbursement. Finally having a large base of medical data online can support important medical research, which can lead ultimately to better understanding and treatment of disease. However, as with other types of personal data, having the information on computers, easily searchable and available over networks, makes it more likely that it will end up in the hands of those who have no business looking at it.

Another threat to the privacy of medical records is institutional: the move to managed care in the health industry. In their attempts to control costs, payers are demanding more and more detailed information on patient conditions, diagnoses and treatments. Therapists, for example, must now give detailed accounts of their clients' emotional states and the reasons for them, in order to collect for their treatments. 165 This is information that traditionally has been very carefully protected as part of a privileged therapeutic relationship. Now it goes into the insurance company's records, where it can easily leak out. 166

HIPPA attempted to address these problems by mandating good information protection practices for medical records. Its privacy rules, which went into effect in 2003, apply to both health care providers and payers, such as insurance plans, employee benefit plans and managed care plans. It covers any medical records that can be linked to an individual, including billing and payment information.

The law requires that the following measures be taken to protect patient privacy:

- Individuals must have access to their records.

165 ibid, p. 39.
• Individuals can require that errors in their records be corrected.
• Disclosure of medical information is allowed without the patient’s permission as needed to facilitate treatment, billing and payment and other related operations; all other disclosures require the written permission of the patient.
• Providers must track all disclosures of patient information and inform the patient of any use of that information.
• Providers must make reasonable efforts to keep communications regarding patient information confidential.

Any entity covered by HIPAA must also provide a contact and a mechanism for responding to patient complaints. As noted earlier, HIPAA has not eliminated unauthorized access to sensitive patient data; but it does give patients a remedy if they become aware of it.167 Another limitation is that, while the law regulates the use and transmission of information in a professional setting, it has not stopped the unauthorized communication of that information in less formal settings, for example over social networks.168

_Differences in Other Countries_

Alan Westin has observed that, while every culture values privacy in some way, the need for privacy is experienced in different ways in different cultures. Even among the Western democracies, there are differences in the balance struck between the individual's need for privacy and society's need for disclosure.169 There are also differences in the mechanisms used to protect privacy, depending on which aspects seem most important.

---


A study by Milberg, Burke, Smith and Kallman has explored these differences and some of the factors that account for them.\footnote{Sandra J. Milberg, Sandra J. Burke, H. Jeff Smith, and Ernest A. Kallman, "Values Personal Information, Privacy, and Regulatory Approaches," \textit{Communications of the ACM}, 38(12) (December, 1995): 65:74.} The authors identify six different types of regulatory systems, in order of increasing government involvement. The first is no regulation at all. Thailand is offered as an example of this. The second is the so-called “self-help” model. The subjects of data records themselves are responsible for finding inaccuracies and abuses and bringing legal challenges to them. Such a system existed in France, for example, before the EU Directive discussed below. The third type of system uses “voluntary control.” The law contains rules on the proper collection and use of data, but the organizations to which they apply are themselves responsible for enforcing them. That is the form of regulation used in Japan and the United States. The fourth system uses a government “data commissioner,” who hears complaints, gives advice on proper data handling, and does some monitoring of data use. However, the commissioner has no direct power of enforcement. Some countries that use this system are Australia, New Zealand and Canada. The fifth type of system requires that databases containing personal information be registered with the government. If there are complaints that lead to a finding of improper use or inadequate protection of the data, the organization holding the data can be decertified, thus losing its permission to operate. Denmark and the United Kingdom have such systems. The final, and strictest, type of regulation uses the “licensing model.” This is similar to the registration model in the fifth system, except that when a database is registered, the government imposes requirements on how the data is to be collected and used. The authors were not able to identify any country that uses this system.

The study goes on to identify three dimensions of cultural values that could affect countries' privacy concerns and therefore the degree of regulation they institute. The first is the “uncertainty avoidance index,” a measure of anxiety and risk aversion. The second is the inequality of power and degree of distrust between different segments of the population. The third is the degree of individualism in a society. A cross-cultural survey showed that different
cultures did differ along these dimensions, and that the differences correlated with different degrees of regulation in different countries. Greater “uncertainty avoidance” and greater inequality of power both correlate with a higher degree of government involvement in privacy protection. On the other hand, countries with a higher degree of individualism have less government involvement, presumably because such societies prefer more individualized solutions.

**European Directive on Protection of Personal Data**

In 1995 the Council of Ministers of the European Union took a step toward unified standards by adopting the Directive on Protection of Personal Data. A consistent set of rules is needed, it was felt, to facilitate the movement of data across national boundaries, an important part of the unified economy toward which the Europeans had been working. Without those rules, a country holding sensitive personal data, with an obligation to safeguard it, could not trust another country to protect it with the same care. This would inhibit the sharing of data that is so important to common economic activity.

The Directive includes the following requirements:

- Data may be collected only for legitimate purposes, which must be clearly specified.
- Data held must be kept “relevant, accurate and up-to-date.”
- Subjects should know the purpose for which data is being collected and what organizations will use it, and must be able to decide whether to disclose the information or not.
- All data processing must have a legitimate legal basis. The possible legal grounds recognized are “consent, contract, legal obligation, vital interest of the data subject or the balance between the legitimate interests of the people controlling the data and the people on whom data is held.”

---

• Subjects on whom data is held are given certain rights: “the right of access to that data, the right to know where the data originated (if such information is available), the right to have inaccurate data rectified, a right of recourse in the event of unlawful processing and the right to withhold permission to use their data in certain circumstances,” (e.g., direct marketing).

• Some particularly sensitive information, on health, sexual behavior, ethnic and racial background, political and religious associations, and so on, can only be used with the consent of the subject, except where there is an important public need, such as medical research. In that case safeguards must be instituted to protect the identity of the subject.

• Adherence to these standards should be monitored by an “independent data supervisory authority” in each jurisdiction.

• Exceptions should be granted for when the information is used only for “journalistic, artistic or literary purposes,” in order to balance freedom of expression with privacy rights.

Each member state of the European Union was responsible for implementing these requirements within three years, and by 1998 all the states in the EU had put into place legislation that conformed to the Directive.

Companies that do business in the EU are subject to the requirements of the Directive; and countries that exchange data with EU members are expected to observe policies that are consistent with the Directive’s main principles. There have been tensions between the EU and certain other countries, including the U.S., whose privacy policies are seen as too lax.

For a more detailed account of privacy laws in other countries, see Freedman.  

General Norms

Through the experience of the last half century, and reflection on it, a set of norms for the

---

172Freedman, *The Right of Privacy in the Computer Age*, pp. 121-146.
collection, dissemination and use of personal data have developed. In the U.S. an early version of these were included in a 1973 government report entitled “Records, Computers and the Rights of Citizens.” The recommendations in this report influenced subsequent legislation such as the Privacy Act and the Fair Credit Reporting Act. The Privacy Protection Study Commission, established by the Privacy Act, produced a more thorough and wide-ranging analysis and set of recommendations in 1977, in its report “Personal Privacy in an Information Society.” In Europe in 1980, the Organization for Economic Cooperation and Development (OECD) issued its “Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data,” which ultimately led to the Directive on Protection of Personal Data discussed in the last section.

Some private organizations that handle sensitive information have developed their own guidelines. For example Equifax has a set of “Information Policies,” promising fair treatment and privacy to every consumer who applies for credit.\textsuperscript{173} Several professional organizations in the data processing industry have codes of ethics, and some mention privacy, although most are too general to give any helpful guidance. However, the Association for Computing Machinery (ACM) Code of Ethics states some specific requirements for the handling of personal data:

\textit{It is the responsibility of professionals to maintain the privacy and integrity of data describing individuals. This includes taking precautions to ensure the accuracy of data, as well as protecting it from unauthorized access or accidental disclosure to inappropriate individuals. Furthermore, procedures must be established to allow individuals to review their records and correct inaccuracies.}

\textit{This imperative implies that only the necessary amount of personal information be collected in a system, that retention and disposal periods for that information be clearly defined and enforced, and that personal information gathered for a specific purpose not be used for other purposes without consent of the individual(s).}\textsuperscript{174}

Based on these sources, as well as the analysis of the issues presented here, this essay concludes with a set of norms for the collection, storage, use and transmission of personal data.

\textsuperscript{173} \textit{The Equifax Report on Consumers in the Information Age}, Atlanta: Equifax, Inc. (1990), pII.
\textsuperscript{174} \textit{ACM Code of Ethics and Professional Conduct},” Association for Computing Machinery (1992), Sec. 1.7.
The norms have three purposes. The first is to respect the autonomy of the subjects whose personal data is being used by giving them as much control as possible over what data is taken and by whom, and what it is used for. The second is to protect the subjects from harm due to the misuse or abuse of their data by controlling data quality and limiting its use and transmission. The third is to find a fair balance between the interests of the subjects and the welfare of society.

The norms are as follows:

1. **Consent.** Personal data not already publicly available should not be collected and held without the consent of the person to whom it refers unless the information is necessary to protect the safety or security of the public. Consent can be given explicitly, or it can be granted implicitly through entering into a contract or participating in an activity that clearly requires granting access to the data. For example when someone uses a credit card, it is understood that the merchant is given access to the person's credit standing. But the concept of implied consent should not be stretched too far. There should be some activity on the subject's part that can reasonably be interpreted as giving informed consent. It is always easier to assume consent when disclosure of the information is part of a transaction that benefits the subject.

   There are a number of factors that affect whether the public interest justifies the disclosure of personal data without the subject's consent. One is the severity of the need. A situation that was a serious threat to human life, such as a medical emergency or very dangerous criminal activity, is more likely to call for disclosure than one with lesser consequences. A second factor is the sensitivity of the data and the harm likely to be done if it is revealed. Especially sensitive information the revelation of which could leave a person vulnerable to humiliation or prejudice, such as a history of psychological problems or some past behavior considered deviant, should be given more careful protection than someone's street address or blood type. Another important consideration is the context in which the information was originally given. Information revealed as part of a privileged relation, such as therapist-patient or lawyer-client, has a stronger claim to
confidentiality because of the promise of protection given in the relationship.

Even when it is necessary to reveal personal data to protect the public, disclosure should be limited to the minimum amount needed. For example data needed for critical research should have identifying information stripped off or coded so that it cannot be associated with the subject.

2. **Limited use.** *Personal data should be used only for the purposes for which it was originally given.* The same qualifications used in 1 apply here as well. The subject can give consent, explicitly or implicitly, for further use. And in some extreme cases, considerations of public welfare can override the need for consent.

3. **Matching.** *The use of matching programs should be limited to the verification of information already given.* Matching is properly used to check for fraud in information given by the subject in order to receive some benefit or pursue some other interest. Matching should not make use of, search for or reconstruct information not already provided by the subject. This excludes “fishing expeditions,” that is, wide ranging searches looking for irregularities where there is not prior suspicion of wrongdoing.

4. **Subject access.** *Subjects should know about and be able to inspect data that is held regarding them, and they should be able to correct any inaccuracies or gaps in the data.* This means that the existence and purpose of any databases holding personal data should be publicized, especially to the subjects they refer to. Subjects should be able to inspect the data in their records, except what must be withheld to protect the privacy and confidentiality of others or for national security. There should be procedures that allow subjects to challenge the information held on them and provide corrections and additions.

   When a decision is made based on personal information in a database, such as the decision to refuse credit to someone, the subject should be informed of the source of the information and how it was used in the decision.

5. **Due process.** *Benefits should not be denied or other action taken against a subject based on a matching procedure or other analysis of personal data until the subject has had a
chance to understand and challenge the procedure and the data it used. Automated procedures and the data on which they are based are too unreliable, acontextual and insensitive to human realities to be the sole basis of punitive action.

6. **Locality.** *Personal data should not be disseminated any further than is necessary for its legitimate and intended use.* This is necessary to support some of the other norms. Where data is available it tends to be used, whether for unauthorized or prejudiced judgments, for demeaning publicity, or for blind searches. Moreover the further information travels from its source, the more likely it is to be distorted, misunderstood, or taken out of context. Most important, out of respect for the subject, personal information ought to be accessible only to those who have authorization and a need to know.

One corollary of this principal is that the Social Security number should not be used as a universal identifier. As it is, an enormous amount of data, of many different types and from many different sources, is accessible through the Social Security number. It is used as an identifier for medical records, bank accounts, credit records, tax returns, voter registration, school records, employee records and many other purposes. On the one hand, the SSN is often treated as a secret password, in that it is sufficient to give someone's Social Security number in order to obtain that person's records. On the other hand, it is very public, in spite of recent efforts to make it less so. It is often printed on forms and letters, posted on lists and easily obtainable as part of a credit check. The Social Security number is widely used and widely disseminated, and most of the rest of a person's data follows right after it. Furthermore, because the Social Security number is used as an identifier in so many disparate databases, computer matching of data from totally unrelated sources, often a questionable practice, is very easy. Yet the Social Security number is easy to forge or corrupt and impossible to verify, so the reliability of those matches is often dismal.

Locality demands that each type of personal data have its own system of identification and that the identifiers be safeguarded with the same care as the data itself.

7. **Accountability.** Any organization that collects, stores, analyzes, uses or distributes personal data should be held responsible for the accuracy, completeness, timeliness and security of the information entrusted to it. Those who handle personal data have been given a public trust and ought to be held accountable. They must have adequate procedures for verifying and maintaining the accuracy and completeness of the data they collect. They must make sure the data is kept current by updating it as the subject's status changes. They must guarantee that the data is available only to those who are authorized to have it and that the authorization extends no further than necessary.

There should be an authority to oversee the activities of the data handlers, which can hold them accountable. Moreover there should be remedies for those subjects who are injured by malicious or irresponsible maintenance or use of their data. The burden created by error should be borne by the data handler, not by the subject.

*Michael McFarland, a computer scientist with extensive liberal arts teaching experience and a special interest in the intersection of technology and ethics, served as the 31st president of the College of the Holy Cross.*

June 2012