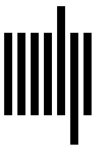
Privacy on the Line

The Politics of Wiretapping and Encryption

By: Whitfield Diffie, Susan Landau

Citation:

Privacy on the Line: The Politics of Wiretapping and Encryption
By: Whitfield Diffie, Susan Landau
DOI: 10.7551/mitpress/5572.001.0001
ISBN (electronic): 9780262256018
Publisher: The MIT Press
Published: 2010



The MIT Press

6

Privacy: Protections and Threats

Protecting the national security and enforcing the laws are basic societal values. Often they stand in competition with another basic societal value: privacy. The competition is hardly an equal contest. National security and law enforcement not only have political constituencies, they are represented by major societal organizations. Privacy has no such muscle behind it. As a result, although an attachment to privacy endures and at times grows, privacy is often violated.

The Dimensions of Privacy

Our focus throughout this book is on privacy in communications. However, it is valuable to draw back and view privacy in a broader context.

Two hundred years ago, if you chose to speak to a colleague about private matters, you had to do it in person. Others might have seen the two of you walk off together, but to overhear your conversation an eavesdropper would have had to follow closely and would likely have been observed. Today, the very communication links that have made it possible to converse at a distance have the potential to destroy the privacy such conversations previously enjoyed.

From video cameras that record our entries into shops and buildings to supermarket checkout tapes that list every container of milk and package of cigarettes we buy, privacy is elusive in modern society. There are records of what we do, with whom we associate, where we go. Insurance companies know who our spouses are, how many children we have, how often we have our teeth cleaned. The increasing amount of transactional

information—the electronic record of when you left the parking lot, the supermarket's record of your purchase—leaves a very large public footprint, and presents a far more detailed portrait of the individual than those recorded at any time in the past. Furthermore, information about individuals is no longer under the control of the person to whom the information pertains; such loss of control is loss of privacy.

Privacy as a Fundamental Human Right

Privacy is at the very soul of being human. Legal rights to privacy appeared 2000 years ago in Jewish laws such as this: "[If one man builds a wall opposite his fellow's] windows, whether it is higher or lower than them . . . it may not be within four cubits [If higher, it must be four cubits higher, for privacy's sake]." (Danby 1933, p. 367) The Talmud explains that a person's neighbor "should not peer and look into his house."

Privacy is the right to autonomy, and it includes the right to be let alone. Privacy encompasses the right to control information about ourselves, including the right to limit access to that information. The right to privacy embraces the right to keep confidences confidential and to share them in private conversation. Most important, the right to privacy means the right to enjoy solitude, intimacy, and anonymity (Flaherty 1989, p. 8).

Not all these rights can be attained in modern society. Some losses occur out of choice. (In the United States, for example, candidates for office make public much personal information, such as tax and medical records, that private citizens are allowed to keep private.) Some losses are matters of convenience. (Almost no one pays bills in cash anymore.) But the maintenance of some seclusion is fundamental to the human soul. Accordingly, privacy is recognized by the international community as a basic human right. Article 12 of the 1948 Universal Declaration of Human Rights states:

> No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks. (Academy on Human Rights 1993, p. 3)

The 1967 International Covenant on Human Rights makes the same point.[1]

The Soviet Union, East Germany, and other totalitarian states rarely respected the rights of individuals, and this included the right to privacy. Those societies were permeated by informants,[2] telephones were assumed to be tapped and hotel rooms to be bugged: life was defined by police surveillance. Democratic societies are supposed to function differently.

Privacy in American Society

Privacy is essential to political discourse. The fact is not immediately obvious, because the most familiar political discourse is public. History records political speeches, broadsides, pamphlets, and manifestos, not the quiet conversations among those who wrote them. Without the opportunity to discuss politics in private, however, the finished positions that appear in public might never be formulated.

Democracy requires a free press, confidential lawyer-client relations, and the right to a fair trial. The foundations of democracy rest upon privacy, but in various democratic societies the protection of privacy is interpreted in varying ways. Britain, for example, has much looser laws regarding wiretaps than the United States. A number of European nations extend more protection to individuals' data records than the US does.

Privacy is culture dependent. Citizens of crowded countries such as India and the Netherlands hold very different views of what constitutes privacy than citizens of the United States. The American concept developed in a land with a bountiful amount of physical space and in a culture woven from many disparate nationalities.

In the 1970s, as rapid computerization brought fear of a surveillance society, some nations sought to protect individuals from the misuse of personal data. Sweden, Germany, Canada, and France established data-protection boards to protect the privacy and the integrity of records on individual citizens. When the US Congress passed a Privacy Act with a similar goal,[3] President Gerald Ford objected to the creation of another federal bureaucracy, and no US data-protection commission was ever established (Flaherty 1989, p. 305). A number of states have data-protection and security-breach notification laws and California includes a right to privacy in its state constitution. It would, however, be a mistake to view the lack of a major regulatory apparatus in the United States as a complete lack of legal protection of privacy.

Privacy Protection in the United States

Most Americans believe that privacy is a basic right guaranteed by the Constitution. The belief has some truth to it, but not nearly as much as some believe. Nowhere is the word privacy mentioned in the Constitution, nor is a right to privacy explicit in any amendment. Privacy is nonetheless implicit to the Constitution.

The First Amendment protects the individual's freedoms of expression, religion, and association. The Third Amendment protects the private citizen against the state's harboring an army in his home, the Fourth against unreasonable search or seizure. The Fifth Amendment ensures that an individual cannot be compelled to provide testimony against himself. The Ninth Amendment reserves to "the people" those rights that are not enumerated in the Constitution. And "the Fourteenth Amendment's guarantee that no person can be deprived of life, liberty or property without due process of law, provides an additional bulwark against governmental interference with individual privacy" (USSR 93 *Federal Data Banks*, p. ix).

The Early Years

Three hundred years ago, the colonists' portion of the North American continent consisted of farms, small towns, and a few small cities. Eavesdroppers were easily avoided by walking to a place where one could not be overheard. Although the colonists' application of English common law provided for the punishment of eavesdroppers (Friedman 1973, p. 254), more typically such crimes were handled by their discoverers (Flaherty 1989, p. 89).

The problem of the mail being less than private was less easily disposed of, for mail delivery entailed dependence on others. In colonial America mail delivery was haphazard; letters from Europe would be left by a ship's captain at a local tavern, awaiting pickup by their intended recipients but meanwhile open to inspection by all passersby. Within the colonies mail was delivered by travelers and merchants, or by special messengers, and privacy was likewise not assumed. In 1710, in creating a postal delivery system in the colonies, the British government established privacy protection similar to what existed in England; at least in law, the

opening of letters and other forms of tampering was forbidden without authorization by the secretary of state (Seipp 1977, p. 11).[4]

Despite the law regarding privacy of the mails, the British government maintained a "secrets office . . . whose staff routinely opened correspondence that the government considered potentially subversive" (John 1995, p. 43). Letters from London and the countryside were opened in the Secretary's private office, while Irish correspondence were opened by a clerk in Dublin Castle (Ellis 1958, p. 64). Foreign mail was opened in a special office whose names over the years were the "Private Foreign Office," "Secret Department," and "Secret Office" (ibid., p. 65). The size of this office varied; by 1810, there were ten on staff (ibid., p. 69). The French maintained a *cabinet noir* for a similar purpose (John 1995, p. 43).

Before the establishment of the United States, Postmaster-General Benjamin Franklin believed that his own mail was being opened and read (Franklin 1907, pp. 461–462). Later, Thomas Jefferson held a similar concern.[5]

The political revolutionaries who established the United States thus had a visceral understanding of the importance of the postal privacy. In the Postal Act of 1792, Congress did three important things: postal officials were prohibited from inspecting the contents of mail (unless the mail was undeliverable); the mailing of newspapers was at a very low cost, thus encouraging political discourse; and Congress was given the right to determine postal routes (John 1995, p. 31). The latter two had surprising consequences. Because the legislature had—and used—the ability to expand postal routes, including into locales in which the postal routes were not self-supporting, the US postal service expanded rapidly. By 1828, the United States had twice as many post offices as Britain and five times as many as France (ibid., p. 5).[6] Because of the democratizing effects of the Postal Act, fears about a strong federal postal system did not emerge. Rather, the postal service was one of the few strong federal institutions early in the nation's history (Starr 2003, p. 3).

In 1825 Congress addressed the problem of spying in the mails with the Postal Act (4 Stat. 102, 109), which prohibited prying into another person's mail. Practice did not necessarily follow the law. During the 1850s there were complaints about the "greedy fingers" through which the mail passed,[7] and during the Civil War there were government attempts to

open private civilian mail.[8] In 1878 the Supreme Court ruled that the government could not open first-class mail without a search warrant (*Ex Parte Jackson*, 96 US 727, p. 733).

The invention of the telegraph led to a new way of communicating and two new ways of eavesdropping: one could tap the wire[9] or one could read the messages later from copies kept by the telegraph companies. The latter was the search method preferred by the government.

At the beginning of the Civil War, the government took control of the telegraph wires and seized copies of all telegrams sent within the previous 12 months (Plum 1882, p. 69). For the duration of the war, the federal government censored all dispatches emanating from Washington (Randall 1951, pp. 482–483). But the War Department did not have full success in controlling the medium. In 1864, attempting to track down the source of a false newspaper story that the president planned to call up an additional 400,000 men, the government sought copies of all telegrams sent out from Washington, but company operators refused to cooperate. They were arrested and held for several days until Army investigators uncovered the perpetrator—a stock manipulator (Bates 1907, pp. 228–243).

Some of the complexity of the fight over the privacy protection afforded to telegraphs was due to the fact that, unlike the mails, this new communication medium was controlled by private enterprise. The government sought two seemingly contradictory goals: to protect privacy of communications from the prying eyes of operators (Seipp 1977, pp. 83–95) and to establish broad search privileges for itself.

Telegraph companies sought to assure the public that communications would be private (ibid., pp. 89–90). The government's determination to obtain copies of telegrams pressed against this, and the conflict came to a head in 1876 with the contested presidential election between Hayes and Tilden. During a fight over electoral votes from Louisiana and Oregon, a House committee questioned the manager of Western Union's New Orleans office about telegrams. Under orders from Western Union's president, the manager refused to reveal the contents of the disputed dispatches. The House held the manager in contempt. Another Western Union manager in Oregon faced a similar situation with the Senate. The company responded that it would henceforth destroy copies of telegrams

as quickly as account keeping would allow (*New York Tribune* 1876). However, the policy was never carried out, and on January 20, 1877, with the manager of the New Orleans office in custody at the Capitol and the company's president ill, Western Union gave in to congressional pressure, and responded to the subpoena (Seipp 1977, p. 54). Western Union prepared a bill for Congress in which telegrams were provided the same legal protections as US mail (*New York Tribune* 1880). Although the bill was reported favorably out of committee, it was not heard of again.

Several court decisions put a partial closure on the issue. One of these involved a St. Louis grand jury investigation of a gambling ring that allegedly involved Missouri's governor and the police commissioner of St. Louis. When the manager of the Western Union office refused to hand over copies of telegrams (*New York Times* 1879), the company appealed and won a partial victory; the Missouri Supreme Court ruled that, although telegraph messages were not accorded the privacy protection the company sought (the same as for US mail), any request for copies of telegrams had to include both the date and the subject of the message (*Ex Parte Brown*, 72 Mo. 83 95 (1880), in Seipp 1977, p. 58). A number of other decisions around that time reached the same conclusions (ibid., p. 59).[10]

After the Civil War the United States experienced rapid industrialization and urbanization. Small towns have never been much known as respecters of privacy, but in such locales the ubiquity of gossip was mitigated by the fact that news did not travel far. As the invention of rotary presses, linotypes, and automatic folders led to a sharp increase in the number of newspapers and to the advent of "yellow journalism," that ceased to be true. Against such a backdrop Samuel Warren, a socially prominent paper manufacturer, and his former law partner Louis Brandeis, later to become a Supreme Court Justice, wrote an article on privacy for the 1890 *Harvard Law Review*. Warren and Brandeis argued that the changes caused by technology called for a response in law:

> That the individual shall have full protection in person and in property is a principle as old as the common law; but it has been found necessary from time to time to define anew the exact nature and extent of such protection.... [I]n very early times, the law gave only for physical interference

> with life and property ... Later, there came a recognition of man's spiritual nature, of his feelings and his intellect. Gradually the scope of these legal rights broadened; and now the right to life has come to mean the right to enjoy life,—the right to be let alone.... (Warren and Brandeis 1890, p. 193)
>
> Instantaneous photographs and newspaper enterprise have invaded the sacred precincts of private and domestic life; and numerous mechanical devices threaten to make good the prediction that "what is whispered in the closet shall be proclaimed from the housetops." (ibid., p. 195)

The success of the US Postal Service in contributing to the development of the country in the nineteenth century rested on two characteristics not shared by other postal systems of the time. On one hand, it promoted rural growth by subsidizing rural mail; the cost of sending a letter within the US was the same regardless of where it went. A letter that had to be carried miles to a postbox on a country road cost the same as one that was delivered to an address near the central post office of a big city. The other was one not shared by European mail systems: the US mail was not the agent of government spying. Postal patrons could send letters secure in the knowledge that their mail was private.[11]

By comparison, the French mail was very much a tool of surveillance.

Privacy as a Principle of Law

Law review articles may shape legal philosophy, but it is statutes and court decisions that determine the law. In the first round between telephone technology and privacy, privacy lost.

In 1928 Prohibition was still in force and illegal liquor distribution was big business. Among the "businessmen" were Roy Olmstead and his partners, who had a large liquor importing and distribution operation in Seattle. The enterprise employed 50 people, including salesmen, dispatchers, deliverymen, bookkeepers, and even an attorney. Outside the city they had a ranch with an underground hideaway for storage, and throughout the city they had smaller caches. Their headquarters, in a large downtown office building, had three phone lines in the main office. In addition, Olmstead and several of his associates had office lines at home.

Federal agents installed wiretaps in the basement of the headquarters building and on lines in streets near the conspirators' homes. For months four prohibition officers eavesdropped on the conspirators as they or-

dered cases of liquor, arranged bribes for the Seattle police, and reported news of seized alcohol. The wiretap evidence played a crucial role in Olmstead's conviction, but should the evidence have been admitted? No warrants were sought, but neither did the agents enter private homes or offices to place the taps (*Olmstead* 1928). Because the evidence had been obtained from warrantless wiretaps installed by the government, the defendants claimed that the wiretapped evidence had been obtained in violation of the Fourth Amendment. Use of the evidence also violated the Fifth Amendment, the defendants argued, because they had unwillingly become witnesses against themselves.

The US Supreme Court did not buy these arguments, and five of the justices voted to uphold a lower court's conviction. In an irony of history, the most famous opinion to come out of the case is Justice Louis Brandeis's dissent, which includes these passages:

> When the Fourth and Fifth Amendments were adopted, "the form that evil had heretofore taken" had been necessarily simple. Force and violence were then the only means known to man by which a Government could directly impel self-incrimination. It could compel the individual to testify—a compulsion effected, if need be, by torture. It could secure possession of his papers and other articles incident to his private life—a seizure effected, if need be, by breaking and entry. Protection against such invasion of "the sanctities of a man's home and the privacies of life" was provided in the Fourth and Fifth Amendment by specific language. . . . But "time works changes, brings into existence new conditions and purposes." Subtler and more far-reaching means of invading privacy have become available to the Government. Discovery and invention have made it possible for the Government, by means far more effective than stretching upon the rack, to obtain disclosure in court of what is whispered in the closet. (Brandeis 1928, p. 473)

> Unjustified search and seizure violates the Fourth Amendment. . . . [I]t follows necessarily that the Amendment is violated by the officer's reading the paper without a physical seizure, without his even touching it; and that use, in any criminal proceeding, of the contents of the paper so examined . . . any such use constitutes a violation of the Fifth Amendment.
>
> The protection guaranteed by the Amendments is much broader in scope. The makers of our Constitution undertook to secure conditions favorable to the pursuit of happiness. They recognized the significance of man's spiritual nature, of his feelings and his intellect. . . . They sought to protect Americans in their beliefs, their thoughts, their emotions and their sensations. They conferred, as against the Government, the right to be let alone—the most comprehensive of rights and the right most valued by civilized man. To protect that right, every unjustifiable intrusion by the Government upon the

> privacy of the individual, whatever the means employed, must be deemed a violation of the Fourth Amendment. And the use, of evidence in a criminal proceeding, of facts ascertained by such intrusion must be deemed a violation of the Fifth. (ibid., pp. 477–478)

A decade later, in the Nardone cases (*Nardone v. United States*, 302 US 379 (1937) and 308 US 338 (1939)), the Supreme Court avoided constitutional questions and used the Federal Communications Act as a basis for making warrantless wiretapping illegal. In effect, though not in law, this supported the principles Brandeis had espoused in *Olmstead*. In later rulings the Court outlawed the use of warrantless electronic surveillance of any type. Other cases before the Court further helped to define the parameters of privacy.

A 1958 ruling held that the First Amendment right to free association included the privacy of such association. In an effort to curb the political activities of the National Association for the Advancement of Colored People, Alabama filed suit against that organization, which had helped organize the Montgomery bus boycott and secure the admission of blacks to the segregated state university. The NAACP was ordered to produce a number of records, including its membership list. In the climate of the times, this would have been dangerous to the individuals named, and the NAACP refused to comply. The Court sided with the defendants:

> [O]n past occasions revelation of the identity of its rank-and-file members has exposed these members to economic reprisal, loss of employment, threat of physical coercion, and other manifestations of public hostility.... (*NAACP v. Alabama.* 357 US 449, 1958, p. 462)

> [I]mmunity from state scrutiny of membership lists that the Association claims on behalf of its members is here so related to the rights of the members to pursue their lawful private interests privately and to associate freely with others in so doing as to come within the protection of the Fourteenth Amendment.[12] (ibid., p. 466)

Seven years later, in *Griswold v. Connecticut*, the Supreme Court greatly expanded privacy protections by including rights that were not specifically enumerated within the Bill of Rights. Connecticut's Birth Control Act outlawed the sale and use of contraceptives, and the state had prosecuted the executive director of Planned Parenthood and a New Haven doctor who had given out contraceptive information. The

Supreme Court ruled that the state had no business legislating on matters having to do with what goes on in the privacy of the bedroom. In so doing, it developed the theory that the protections afforded by the Bill of Rights cast wide shadows:

> This law … operates directly on an intimate relation of husband and wife and their physician's role in one aspect of that relation.
>
> The association of people is not mentioned in the Constitution nor in the Bill of Rights. The right to educate a child in a school of the parents' choice —whether public or private or parochial—is also not mentioned. Nor is the right to study any particular subject or any foreign language. Yet the First Amendment has been construed to include certain of those rights. (*Griswold v. Connecticut*, 381 US 479, 1965, p. 482).

> In *NAACP v. Alabama*, 357 US 449, 462, we protected the "freedom to associate and privacy in one's associations."… In other words the First Amendment has a penumbra where privacy is protected from governmental intrusion.…
>
> [S]pecific guarantees in the Bill of Rights have penumbras, formed by emanations from those guarantees that help give them life and substance.… (ibid., p. 483)

Two years later, the Supreme Court ruled that telephone calls, including those made in public places, were private. Charles Katz had placed a $300 bet from a phone booth in Los Angeles. An FBI team investigating interstate gambling had, without benefit of a search warrant, installed an electronic bug in the phone booth and picked up Katz's portion of the conversation. The Court ruled:

> [T]he Fourth Amendment protects people, not places. What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection.… But what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected. (*Charles Katz v. United States*, 389 US 347, 1967, p. 311)

Katz's conviction was overturned. However, the Supreme Court was not heading down a one-way path to greater privacy protection, as Mitchell Miller, who used his checking account for an illegal moonshine business, discovered.

In December 1972, a deputy sheriff in Houston County, Georgia, stopped a suspicious van driven by Miller's business partners. The van was carrying materials for making a still. Several weeks later, during a

fire at a warehouse Miller had rented, firemen and police discovered a distillery and whiskey, on which no taxes had been paid. The Bureau of Alcohol, Tobacco, and Firearms issued a subpoena to Miller's bank for his account records, which the bank gave to federal agents. A grand jury subsequently indicted Miller on various moonshining charges. Arguing that because the seized material constituted self-incriminating material the subpoena was an illegal search and seizure, Miller tried to suppress the account information. The Court did not support him:

> We find there is no intrusion into any area in which respondent had a protected Fourth Amendment interest. . . .
>
> On their face, the documents subpoenaed here are respondent's "private papers". . . . (*United States v. Miller*, 425 US 435, 1976, p. 440)

> [I]f we direct our attention to the original checks and deposit slips, rather than to the microfilm copies actually viewed and obtained through the subpoena, we perceive no legitimate "expectation of privacy" in their contents. The checks are not confidential communications, but negotiable instruments to be used in commercial transactions. All of the documents obtained, including financial statements and deposit slips, contain only information voluntarily conveyed to the banks and exposed to their employees in the ordinary course of business. (ibid., p. 442)

Here the Court deemed only that which has an "expectation of privacy" worthy of Fourth Amendment protection. Such a decision is very much a double-edged sword for privacy. On the one hand, it forms the basis for such privacy rulings as the Kyllo decision (*Kyllo v. United States*, 533 US 27, 2001), in which the Supreme Court ruled that the warrantless use of a thermal-imaging device to determine "hot spots" in a private house (and thus the likelihood that marijuana was being grown) was a violation of Fourth Amendment rights.[13] On the other, the lack of privacy in Internet communications leaves that domain highly unprotected under the "expectation of privacy" standard. This is why privacy protection for communication is often established by legislative enactment. Statutes define what the expectation of privacy is for new technological environments.

Privacy Threatened

In the name of efficiency, the US government and many businesses have amassed huge databases containing profiles of their "customers." The gains in efficiency are accompanied by losses of privacy.

Credit cards leave a trail of where their holders travel, where they shop, and what they buy. Studying billing patterns, the European branch of American Express tailors the promotional material it sends its customers to their individual purchasing patterns, and plans are afoot to offer the same "service" in the United States. "'A Northern Italian restaurant opens in midtown Manhattan,' [the CEO of American Express] says, by way of an example. 'We know from the spending of card members which of them have eaten in Northern Italian restaurants in New York, whether they live in New York or Los Angeles. We make the offer of a free or discounted meal available only to those card members.'" (Solomon 1995, p. 38) The long-distance telephone company MCI offers its users discounts on calls to the ten numbers they call most often, and the carrier identifies those numbers for the customers. These companies are not unique in the amount they know about their customers' purchasing patterns, though they are perhaps more public about it.

Although there has been no public protest of the two transactional data collections described above, there are periodic episodes in which the public says to a company "Leave us alone." In the early 1990s the software firm Lotus and the Equifax credit bureau were developing a CD-ROM that would contain the names, estimated incomes, and purchasing habits of 120 million Americans. The companies received 30,000 letters opposing the project, and it was killed (Piller 1993, p. 11). Similarly, for exactly 10 days Lexis-Nexis, a leading information broker, offered an online service that included access to Social Security numbers. An outpouring of objections from customers caused the company to discontinue the service (Flynn 1996).

On occasion the federal government has stepped in to safeguard privacy. In 1970 Congress passed the Fair Credit Reporting Act, which ensures that individuals have rights in connection with credit records maintained by private databases. The publicity surrounding Judge Robert Bork's rental habits[14] led to the Video Privacy Protection Act of 1988,

which prohibits release of video rental records. The Federal Privacy Act places limits on the types of information federal agencies may collect on individuals. California, Connecticut, the District of Columbia, Illinois, New Jersey, and Wisconsin all have laws that protect cable TV subscribers' records against release. Almost all states recognize the doctor-patient privilege (*Privacy Journal* 1992). Legislative protections of privacy are sparse but not unknown.

In the United States of the mid 1990s, there were over 500 commercial databases buying and selling information (Piller 1993, p. 10). Despite this proliferation of private purveyors of information, US citizens fear their government more. A Harris survey showed that in response to the question "Which type of invasions of privacy worry you the most in America today—activities of government agencies or businesses?" Fifty-two percent of the respondents answered that government agencies were their greater worry; 40 percent said business (Center for Social and Legal Research, p. 7).

Data collection by the US government dwarfs that by private enterprise. It is a rare American indeed who is not in a government database; most are in many. In the early 1990s, the agencies of the federal government supported 910 *major* databases (USGAO 1990, p. 2) containing personal data: 363 in the Department of Defense, 274 in the Department of Health and Human Services, 201 in the Department of Justice, and 109 in the Department of Agriculture (ibid., p. 41). Fifty-six percent of these systems allowed access by other federal, state, and local agencies; some even allowed access by private organizations (ibid., p. 18). Computer matching promotes efficiency and curtails fraud and duplication.[15] We no longer know how many federal databases there are; in 1996, the reporting requirements of the 1974 Privacy Act[16] were diminished and the data are effectively no longer made public.[17] Other things changed too.

The 1974 Privacy Act requires data minimization (only data "relevant and necessary" to the task should be kept) and puts into place rules about data sharing between agencies (with a clear description of the records to be shared and not without a written agreement describing the purpose and justification). There is, however, no set of requirements on what data the government is allowed to purchase from databrokers; such companies

did not exist in 1974, when the Privacy Act was passed. While in the early 1990s data collection by the US government dwarfed that by private enterprise. that is no longer the case. Inexpensive storage[18] and fast matching algorithms have made commercial databrokers a profitable—and almost completely unregulated—business, completely changing the meaning of "know your customer." This revolution has also changed the information available to government.

After the 9/11 attacks, the US government turned to databrokers to expand its information on the US population. One of these is Acxiom, an Arkansas company with "information on almost 200 million people living in 110 million households" (O'Harrow 2005, p. 61). Acxiom's information on American households includes not only "names, birth dates, genders, addresses," but "number of adults [in the household], the presence of children, their genders and ages and school grades," house assessment and market value, the families' occupations and net worth and estimated income (ibid., p. 49). It appears that there is not much that Acxiom doesn't know. Another large databroker is ChoicePoint, a Georgia company marketing to state police, with over seventeen billion online public records—and forty thousand more records added each day (ibid., p. 145). It is estimated that ChoicePoint has records on more than 220 million people (ibid., p. 145).

The lack of regulation delimiting government acquisition of information collected by private databrokers is a serious hole in government privacy law, but one seemingly difficult to change at a time when fear of terrorism drives the political agenda. In the 1950s and the 1960s, when fear of communism was paramount, the government response included investigating and disrupting political activities and attempting to discredit civil-rights leaders, including Martin Luther King Jr. The government's power is immense, and has often been used to invade citizens' privacy. In the 1950s and the 1960s, those invasions were a matter of policy. Now technology has been developed to enable such invasions of a far grander scale. Changing public policy is rarely easy. Changing policies that are buttressed by widespread commercial practices and large investments in equipment is rarely possible.

Privacy Lost

Invasions of privacy have occurred despite legal provisions to the contrary. The debate about cryptography is a debate over the right of the people to protect themselves against government surveillance. But privacy intrusions are difficult to uncover. Many are suspected but few are proven. Those that are discovered are frequently exposed only as a result of years of litigation or through a major investigation like the Church Committee hearings of the 1970s.[19] Thus in order to judge the citizenry's need for protection against government surveillance, we take the long view and we look more closely at the government invasions of personal privacy over the last 50 years.

The 1940s

Article 1 of the US Constitution requires that a census be taken every 10 years to determine proper representation in Congress. In the first 50 years of the republic census questions were limited to numbers and age (Wright and Hunt 1900, pp. 132–133), but by 1840 the census included questions about the employment of family members (ibid., p. 143). Public objection led the Census Bureau to tell the public that the public statistical tables included only aggregate data and to remind the census takers that "all communications made to [you] in the performance of this duty … [are] strictly confidential" (ibid., p. 145). By 1880 the questionnaire had become considerably more detailed, asking about employment status, education level, and place of birth. The 1890 census showed a similar interest in personal detail, and people objected. In New York City alone, 60 people were arrested for refusing to answer census questions (*New York Tribune* 1890).

For the 1900 census, Congress made unauthorized disclosure of information about individuals a misdemeanor; for the 1920 census, a breach of confidentiality was made a felony (Davis 1973, p. 200). The current law, passed in 1929, explicitly states that no one other than "sworn employees of the Census Office"[20] shall be able to examine individual reports.

In 1980 the Census Bureau advertised that even during World War II, when there had been fears of a fifth column among Japanese-Americans

living on the West Coast, the Census Bureau never gave out information about individuals (Okamura 1981, p. 112). The Census Bureau lied. A 1942 War Department report described the role of the Census Bureau in the roundup of Japanese-Americans:

> The most important single source of information prior to the evacuation was the 1940 Census of Population. Fortunately, the Bureau of the Census had reproduced a duplicate set of punched cards for all Japanese in the United States shortly after the outbreak of war and had prepared certain tabulations for the use of war agencies.... These special tabulations, when analyzed, became the basis for the general evacuation and relocation plan. (USDoW 1943)

These people lost their incomes, their property, and their rights as citizens. The Census Bureau, whose data about individuals, under law, was not to be released, supplied the information that helped the military to round up the Japanese-Americans.[21]

Other Americans lost privacy rights during the war too. Expressing concern about Communist influence, the FBI wiretapped the Congress of Industrial Organizations' Council and Maritime Committee; the Tobacco, Agricultural, and Allied Workers of America; the International Longshoremen's and Warehousemen's Union; the National Maritime Union; the National Union of Marine Cooks and Stewards; and the United Public Workers of America (Theoharis and Cox 1988, pp. 10 and 438). It bugged the United Automobile Workers and the United Mine Workers.

The privacy of the mails was also invaded. Beginning in 1940 and continuing until 1973, FBI and CIA agents read the private mail of thousands of citizens.[22] The justification was the Cold War, but Senate investigators later called this "essentially domestic intelligence" (USSR 94 *Intelligence Activities: Staff Reports*, p. 561). Without warrants and without congressional or clear presidential authority, intelligence agents opened and perused the mail of private citizens, senators, congressmen, journalists, businessmen, and even a presidential candidate. Domestic peace organizations, such as the American Friends Service Committee, had their mail opened, as did scientific organizations, including the Federation of American Scientists. So did the writers Edward Albee and John Steinbeck. Americans who frequently visited the Soviet Union or corresponded with

people there were singled out, as were educational, business, and civil-rights leaders (USSR 93 *Electronic Surveillance for National Security*, pp. 574–575). In one program, more than 200,000 pieces of mail were illegally opened.

Telegrams were even less private. The National Security Agency requested copies of telegrams to and from certain foreign intelligence targets, and Western Union complied with the request. RCA Global and ITT went further, giving NSA access to the "great bulk" of their telegrams. In the early stages of this program, the government received paper tapes, and the volume of material precluded sorting on content. In the early 1960s, RCA and ITT World Communications switched to magnetic tape for storing telegrams, and then the two companies shipped copies of *all* overseas telegrams to NSA. The agency read all telegrams to or from people on the "watch list," which included both foreigners that the government had decided were attempting to exert control on US policy and Americans citizens engaged in peaceful protest against government policy (USSR 94 *Intelligence Activities: Rights of Americans*, p. 108).

The mail and telegram searches were largely untargeted invasions of privacy. There were also highly targeted ones. For example, President Harry Truman did not trust Thomas Corcoran, a Washington lobbyist who had been a close confidant of President Franklin Roosevelt. Truman asked the FBI for a telephone tap on Corcoran's phone. Conversations were recorded in which Corcoran and Supreme Court justices Hugo Black, William O. Douglas, and Stanley Reed discussed the pros and cons of various possible nominees for chief justice (Charns 1992, p. 25). After considering sitting justices William O. Douglas and Robert Jackson, Truman went outside the Court for his nominee, choosing Treasury Secretary Fred Vinson, his friend and poker buddy. However Truman made his choice for chief justice, he is known to have discarded certain nominees after seeing the Corcoran transcripts. We do not know if the wiretapped conversations influenced Truman in his decision, but we do know that the other participants had not intended Truman to be a silent participant.[23]

The 1950s

The opening of mail continued after World War II and after the Korean War. Various programs to photograph mail remained in effect, and photos were indexed, filed, and stored.

Throughout the 1950s the FBI aggressively pursued Communists wherever it thought they might be found. By the mid 1950s even many FBI agents did not view the American Communist Party as a serious threat,[24] but the bureau continued to investigate the party and related groups, conducting searches that were far out of proportion to the perceived threats. For example, the Socialist Workers Party was the subject of 20 years of wiretaps, burglaries, and bugs by the government investigators, even though the FBI knew that the group did not advocate violence (Shackelford 1976). Through warrantless break-ins the bureau photographed such papers as "Correspondence identifying contributors to SWP election campaign fund," "Correspondence re arrangements for [name deleted] to debate at Yale University," and "Letter ... detailing health status of ... Nat'l Chairman."[25] Eventually the Socialist Workers Party sued the US government for violations of constitutional rights, winning more than $250,000 in damages.[26]

The FBI's pursuit of Communists led to investigations of such subversive domestic organizations as parent-teacher associations, civil rights organizations, and various racial and religious groups (USSR 94 *Intelligence Activities: Rights of Americans*, p. 67). The FBI launched probes of the Ku Klux Klan and the John Birch Society. It also investigated the Southern Christian Leadership Conference (SCLC), the Congress of Racial Equality, and the NAACP, despite the fact that these three were all staunch advocates of non-violence. FBI agents overstepped many bounds in these inquiries, including those of personal privacy.

The 1960s

In all the inappropriate investigations, one victim stands out, a man whose privacy was repeatedly and egregiously violated by the FBI: Martin Luther King Jr. For a number of years the FBI had been investigating King's alleged ties to the Communist Party. King's closest connection to the Communist Party was through his friend and advisor Stanley Levison. But Levison had left the Party in 1954. The FBI was well aware of this:

in 1960 it had attempted to recruit Levison in order to have him rejoin the Party as an FBI spy (Friedly and Gallen 1993, p. 24).

In 1963, during debates on a pending civil rights bill, Senator James Eastland of Mississippi, using information given to him by the FBI, charged that King and the SCLC were being advised by Communists. Attorney General Robert Kennedy authorized wiretaps on King (USSR 93 *Electronic Surveillance for National Security*, pp. 111–112). The FBI decided that the bugging of King was also authorized (ibid.). No evidence of Communist influence was discovered, but King remained a subject of wiretaps and bugs. The surveillance had uncovered other information too valuable for FBI Director J. Edgar Hoover, who hated King, to ignore.

Electronic surveillance in hotel rooms King stayed in when traveling picked up the minister telling bawdy stories and raucously partying (Darrow 1981, p. 109). Although this information had nothing to do with Communist activity in the civil rights movement, the FBI used the tapes in an attempt to discredit King. A version of the tapes was sent to his wife, and Hoover played the tapes for President Lyndon Johnson.

In a further attempt to discredit King, William Sullivan, Associate Director of the FBI, wrote a monograph on Communist influence in the civil rights movement that was then made available to the heads of intelligence agencies, the Department of State, the Department of Defense, and the United States Information Agency; it included a salacious section on King's personal life, apparently based on information from the bugs (USSR 94 *Intelligence Activities: Staff Reports*, pp. 173–174). The impetus for this siege was King's having received the Nobel Peace Prize. Enraged by this international honor, Hoover tried to spread the news of King's personal life anywhere honors for the civil rights leader were being contemplated.

There was also political espionage against King. At the request of the White House, the FBI sent 30 special agents to the 1964 Democratic National Convention in Atlantic City. Their job was to assist the Secret Service and to make sure that the convention was not disrupted by civil disturbances. The FBI interpreted the latter charge broadly enough to cover political activities. Johnson was especially concerned about a challenge to the seating of the regular Mississippi delegation by the Mississippi Freedom Democratic Party. From an FBI wiretap of King's

hotel room in Atlantic City,[27] Johnson's staff discovered the efforts of King and his associates to unseat the Mississippi delegation. A Senate investigating committee later observed that "an unsigned White House memorandum disclosing Dr. King's strategy in connection with a meeting to be attended by President Johnson suggests there was political use of these FBI reports."[28]

The investigations of King were not based on national-security considerations. In the case of the Democratic National Convention, the purpose of the wiretap was to provide political intelligence for the president. As was well known to the FBI at the time, the other wiretaps and bugs had no legitimate purpose.

Where many saw peaceful dissent in the civil rights movement and in the protests against the Vietnam War, the FBI saw domestic upheaval and began a massive program of surveillance. Riots in Los Angeles and other cities in the summer of 1965 led to heavy FBI surveillance of black neighborhoods. In 1966, FBI field offices were told to begin preparing semimonthly summaries of "existing racial conditions" and of the activities of all civil rights organizations (USSR 94 *Intelligence Activities: Rights of Americans*, p. 71). By 1972 the bureau had over 7400 informants in the ghettos, including, for example, "the proprietor of a candy store or barber shop" (ibid., p. 75). The informants were to attend meetings held by "extremists," to identify them when they came through the ghetto, and to identify persons distributing extremist literature (Moore 1972). Since the FBI's definition of extremists included such advocates of nonviolence as Martin Luther King and Ralph Abernathy,[29] it is not surprising that so many informants (one of every 3300 black Americans) were employed by the FBI during this period.

Fear of potential Communist infiltration led the FBI to investigate the anti-war movement (USSR 94 *Intelligence Activities: Rights of Americans*, p. 49), and agents conducted their probes as if these apprehensions had a factual basis. For example, during the spring of 1968, the FBI sought to wiretap the National Mobilization Office, which was planning to hold demonstrations during the Democratic National Convention in Chicago. In this case, despite several requests by the FBI, Attorney General Ramsey Clark refused to give the bureau permission to wiretap (Clark 1968).

The FBI also investigated the women's liberation movement and various university, church and political groups opposed to the Vietnam War (USSR 94 *Intelligence Activities: Rights of Americans*, p. 167). A woman whom the FBI had hired to report on the group Vietnam Veterans against the War later told a Senate committee: "I was to go to meetings, write up reports ... on what happened, who was there, ... to try to totally identify the background of every person there what their relationships were, who they were living with, who they were sleeping with. ..." (USSH 94 *Intelligence Activities: FBI*, p. 111)

A Senate subcommittee estimated that between 1967 and 1970 the US Army maintained files on at least 100,000 Americans (USSR 92 *Army Surveillance*, p. 96), including Joan Baez, Julian Bond, Rev. William Sloane Coffin Jr., Arlo Guthrie, Jesse Jackson, Martin Luther King Jr., Representative Abner Mikva, Dr. Benjamin Spock, and Senator Adlai Stevenson III.[30]

Much of the information contained in the Army's files was personal. "For example, the profile of a well-known local civil rights leader reported that he had four brothers, five sisters, and a widowed mother. An entertainer was recorded as married and the father of six children. ... Another sketch stated that due to flat feet and torn ligaments, ___ failed to pass Selective Service physical examinations, and his draft board classified him 1-Y." (USSR 93 *Military Surveillance*, p. 56) Though these people had not served in the Army, the Army's files contained information about their financial affairs, sex lives, and psychiatric histories (USSR 92 *Army Surveillance*, p. 96).

The military also kept files on the American Friends Service Committee, Americans for Democratic Action, the Congress of Racial Equality, Clergy and Laymen Concerned about the War, the NAACP, the National Mobilization Committee to End the War in Vietnam, the SCLC, Veterans and Reservists to End the War, and Women's Strike for Peace, among others (USAINTC 1969). Army agents reported on such subversive activities as labor negotiations conducted by the sanitation workers' union in Atlanta and actions by Wisconsin welfare mothers who wanted higher payments (Stein 1971, p. 274). As a Senate subcommittee observed, "considerations of privacy, relevance, and self-restraint were cast to the winds" (USSR 93 *Military Surveillance*, p. 56).

The 1960s were also a time when President John Kennedy used national security as a pretext for FBI wiretaps on opponents of his administration's Sugar Bill (see chapter 6) and on several journalists,[31] and when the FBI kept President Johnson supplied with political intelligence through biweekly summaries of contacts between foreign officials and various senators and congressmen (USSR 94 *Intelligence Activities: Rights of Americans*, pp. 119–120).

Despite his use of the King wiretaps and his reliance on the FBI for political surveillance of congressional opponents to the Vietnam War, President Johnson turned against the use of wiretaps.[32] Johnson called the Title III provisions for wiretapping undesirable even as he signed the Omnibus Crime Control and Safe Streets Act of 1968 (*Congressional Quarterly Weekly* 1968b, p. 1842).[33] Richard Nixon took his oath of office as president 7 months later. In his first full day as president, Nixon told a reporter that his attorney general, John Mitchell, would govern wiretapping "with an iron hand" (White 1975, p. 125). Within 4 months, and without Mitchell's approval, Nixon's administration began wiretapping for political purposes.

The political wiretapping began after the *New York Times* reported that the United States had been bombing Cambodia for some time. Henry Kissinger, Nixon's national security advisor, asked J. Edgar Hoover to have the FBI find out who had leaked this information to the *Times*. Seventeen people, including several journalists, were wiretapped in this investigation.

Two of those tapped, John Sears and James McLane, were domestic-affairs advisors with no access to classified national-security material (USSR 94 *Intelligence Activities: Staff Reports*, p. 337). White House speechwriter William Safire was also wiretapped; he had been overheard on an existing tap promising a reporter background material pertaining to a presidential address on revenue sharing and welfare reform (USSR 94 *Intelligence Activities: Staff Reports*, p. 337). No national-security leaks were ever uncovered by this investigation.

Joseph Kraft, a columnist, was another target. Kraft had once been a favorite of Nixon's, having coined the term "Middle America" to describe Nixon's supporters. But in the spring of 1969 Kraft criticized Nixon's peace efforts, and in June John Ehrlichman, Nixon's counsel,

arranged for Kraft's phone to be tapped. A "security consultant" to the Republican National Committee installed the warrantless wiretap (USHH 93 *Impeachment Inquiry*, p. 150). Kraft flew to Paris a week later to cover the Vietnam peace talks, and the tap was removed. But the Assistant Director of the FBI, William Sullivan, followed Kraft to Paris and arranged for further electronic surveillance (Sullivan 1969). The switching system of the hotel made it impossible to install a phone tap, so a microphone was placed in Kraft's room (USSR 94 *Intelligence Activities: Staff Reports*, p. 323). No evidence was ever found to support Ehrlichman's claim (Ehrlichman 1973) that Kraft was tapped for reasons of "national security." Indeed, in 1974, William Ruckelshaus, formerly a Deputy Attorney General and now Acting FBI Director, told Congress: "The justification would have been that [Kraft] was discussing with some —asking questions of some members of the North Vietnamese Government, representatives of the government. My own feeling is that this is just not an adequate national security justification for placing any kind of surveillance on an American citizen or newsman."[34] (Ruckelshaus 1974, pp. 320–321)

These wiretaps were ordered for national-security reasons, but summaries forwarded to the White House included such information as this:

> "meat was ordered [by the target's family] from a grocer," that the target's daughter had a toothache, that the target needed grass clippings for a compost heap he was building, that during a conversation between his wife and a friend, the two discussed "milk bills, hair, soap operas, and church" (FBI 1975b)

Although the FBI observed that this was "non-pertinent information" (USSR 94 *Intelligence Activities: Staff Reports*, p. 344), agents transcribed the conversations and faithfully sent the contents on to the White House. At least once the agents exercised some discretion. A wiretap on the home line of Henry Brandon, a *London Sunday Times* correspondent, picked up a conversation between the journalist's wife and her close friend Joan Kennedy, wife of Senator Ted Kennedy, in which Mrs. Kennedy discussed "problems with Teddy." The agent in charge said "I knew what those people would do with this stuff," and he destroyed the transcript (Hersh 1983, p. 324). President Nixon described the informa-

tion he did receive as "gobs and gobs of stuff: gossip and bull" (USHR 93 *Statement of Information*, p. 1754).

Under Attorney General Mitchell, the FBI was empowered to collect political intelligence on the anti-war movement. On November 15, 1969, some 250,000 people marched on Washington in what the next day's *New York Times* described as "a great and peaceful army of dissent" (Herb 1969). Nine days earlier, Mitchell had approved an FBI request to wiretap the march's organizers.[35]

The excesses of the Nixon era were not limited to wiretaps. Tom Huston, a White House staffer, had been put in charge of developing a report on the connection between domestic unrest and foreign movements and had devised a plan in which the resources of the Central Intelligence Agency, the Defense Intelligence Agency, the Federal Bureau of Investigation, and the National Security Agency were to be pooled to fight domestic unrest. NSA—contrary to law—would intercept communications of US citizens using international facilities. Rules regarding mail interception, electronic surveillance, and surreptitious entry would be relaxed. "Covert [mail] coverage is illegal, and there are serious risks involved," wrote Huston. "However, the advantages to be derived from its use outweigh the risks." (Huston 1970, p. 194) Regarding surreptitious entry, Huston wrote: "Use of this technique is clearly illegal: it amounts to burglary." (ibid., p. 195) Yet President Nixon approved the plan. Five days later—before it took effect—he rescinded his approval. That the Huston plan came within a hairsbreadth of being national policy shocked the nation when it was revealed several years later.

The 1970s and the 1980s

The purpose of the FBI's Library Awareness Program, conducted between 1973 and 1988 at a number of public and university libraries,[36] was to investigate their use by foreigners. The FBI wanted to know about "Soviets [who] have come ... [with] unusual database requests" (Foerstal 1991, p. 56), about "computerized literature searches performed for library patrons" (ibid., p. 69), and about "reading habits of a visiting Russian student ... and anyone else 'similarly suspicious in nature'" (Robins 1988).

The FBI ran into trouble when it attempted to enlist librarians in

surveillance. Librarians have a deep and abiding commitment to disseminating information, not protecting it. Librarians also strongly defend the privacy of their patrons. When the FBI sought to discover who was borrowing "unclassified, publicly available information relating more often than not to science and technical matters" (FBI 1987), many librarians would not comply with the informal requests and refused to release information about patrons without subpoenas. The American Library Association publicly opposed the Library Awareness Program. By 1989, most states had adopted laws making borrowers' records confidential (Foerstal 1991, p. 133).

When the Reagan administration came to power, a cornerstone of its foreign policy was support of the Duarte regime in El Salvador. The Committee in Solidarity with the People of El Salvador (CISPES) was a group of Americans who supported the opposition movement. In 1981 the FBI began an investigation of the Dallas chapter of CISPES to determine whether the group was in violation of the Foreign Agents Registration Act.[37] It was not.

In 1983, using information supplied by an informant, the FBI began a second investigation of CISPES, this time focusing on the group's alleged connections with international terrorists. "The FBI undertook both photographic and visual surveillance of rallies, demonstrations, etc., in its investigations of CISPES," the bureau later reported. "This technique involved the taking of photographs during demonstrations, surveillance of rallies on college campuses, and attendance at a mass at a local university. The purpose of taking photographs during demonstrations was for use or future use in identifying CISPES leaders." (FBI 1989, p. 2) The bureau kept files on more than 2300 individuals and 1300 groups (ibid.). One source "provided the FBI a copy of another person's address list by gaining unconsented access to the desk where the address list was located." In another case, "FBI agents posing as potential home buyers toured the home of a subject of the investigation with a real estate agent" (ibid., pp. 5–6). The FBI expanded the investigation using long-distance telephone records of the Dallas chapter; agents added 13 CISPES offices to the list of those being probed, and the investigation grew.

There was no justification for these actions. The investigation was based on the words of an unreliable informant. CISPES was not a terror-

ist organization, nor was it allied with one. Testifying before Congress in 1988, FBI Director William Sessions said: "The broadening of the investigation in October 1983, in essence, directed all field offices to regard each CISPES chapter, wherever located, as a proper subject of investigation. Based on the documentation available to the FBI by October 1983, there was no reason . . . to expand the investigation so widely." (Sessions, p. 122) Once again the privacy of Americans engaged in political protest had been violated.

The Senate investigating committee observed: "The CISPES case was a serious failure in FBI management, resulting in the investigation of domestic political activities that should not have come under governmental scrutiny. It raised issues that go to the heart of this country's commitments to the protection of constitutional rights. Unjustified investigations of political expression and dissent can have a debilitating effect upon our political system. When people see that this can happen, they become wary of associating with groups that disagree with the government and more wary of what they say or write. The impact is to undermine the effectiveness of popular self-government." (USSR 101-46 *FBI and CISPES*, p. 1)

The 1990s

Those words describe what happened to a group of seven Palestinians and one Kenyan living in the Los Angeles area in the 1980s, a group that became known as the L.A. 8. Beginning in 1987, the FBI, working with the Immigration and Naturalization Service, tried to deport the eight. At issue were the L.A. 8's support for the Popular Front for the Liberation of Palestine (PLFP), an organization that is included in the US State Department's list of terrorist organizations (USDoS 2005, p. 183).

It is undisputed that in 1986 the group of seven men and one woman had helped organize a fundraiser for the Palestinian cause; what constitutes the cause was, and remains, the issue. The fundraiser was a very public event—1200 people attended (King 2005a)—and was a festival to celebrate the eighteenth anniversary of the founding of the PLFP. As the *Los Angeles Times* reported many years later, "The preparations seemed fairly unremarkable. Posters were taped to walls. Palestinian magazines, including copies of a PFLP publication, *Al Hadaf*, were arranged on

tables. A troupe of amateur dancers practiced a folk dance known as the dabka." (King 2005a) The fundraising, according to the L.A. 8, was for orphanages and hospitals; the FBI held otherwise. But did the government even believe its own case?

At first the L.A. 8 were accused of violating the McCarran-Walter Act, a McCarthy-era law which made the support of groups that advocated the "doctrines of world communism" a deportable offense. Even then the FBI knew the charges were harassment: just months after the arrest of the eight, FBI Director William Webster testified to Congress that "if these individuals had been United States citizens, there would not have been a basis for their arrest" (USHR-101 *Webster Nomination*, p. 95). When in 1989 a federal court declared the McCarran-Walter Act charges unconstitutional in *American-Arab Anti-Discrimination Comm. v. Meese* (714 F. Supp. 1060, C.D. Cal. 1989), the eight were charged with visa violations (Dempsey and Cole 1999, p. 35).[38] Congress then repealed those provisions of the McCarran-Walter Act, and the seven men and one woman were instead charged by the US government with providing material support to a terrorist organization (ibid., pp. 35–36), although *not* to a terrorist activity. This is a distinction with a difference: many organizations on the US terrorist list support social and civil infrastructure such as schools and hospitals separately from their support of military and terrorist activity. Had the FBI believed that the L.A. 8's fundraising was actually for terrorist activities, the L.A. 8 would have been so charged. When asked if the government won the case, whether the L.A. 8 would be deported, a government spokesman answered "Probably not. . . . Obviously, if we get information that suggests one of the others did something. . . ."[39] (King 2005b) The situation became ever more Kafkaesque after the terrorist attacks of 9/11, when first the PATRIOT Act[40] and then the Real ID Act[41] were retrospectively applied to 1986 activities of the L.A. 8 (ibid.).

As of this writing, the L.A. 8 have been in legal limbo for 19 years, creating lives for themselves in the United States yet not daring to leave the country for fear of not being readmitted. Their legal situation has not gone unnoticed by the Arab-American community, a community whose support is critical in the U.S. effort against terrorism. The case against the L.A. 8 was just one of a number of FBI cases investigating First

Amendment activity by Arab and Palestinian groups in the United States. For example, from 1979 to 1989 the FBI investigated the General Union of Palestinian Students, a college organization for social and political activities. While the reasons for beginning the investigation are unclear (Dempsey and Cole 1999, p. 44), there were even fewer reasons for continuing the investigation for 10 years.

Other breaches of privacy have also occurred despite safeguards. A recent government report noted that employees of the Internal Revenue Service's Data Retrieval System browsed the agency's database for information on accounts of "friends, neighbors, relatives and celebrities" (Edwards 1994).[42] Authorized users of the FBI's National Crime Information Center similarly misused that system (USGAO 1993a). These, of course, were only the activities that were discovered.

Why Privacy?

Despite strictures to prevent abuses, the US government has invaded citizens' privacy many times over the last 50 years, in many different political situations, targeting individuals and political groups. Politicians have been wiretapped, and lawyers' confidential conversations with clients have been eavesdropped upon by FBI investigators.[43]

Sometimes invasion of privacy has been government policy; sometimes a breach has occurred because an individual within the government misappropriated collected information. The history of the last five decades shows that attacks on privacy are not an anomaly. When government has the power to invade privacy, abuses occur.

Conflict between protecting the security of the state and the privacy of its individuals is not new, but technology has given the state much more access to private information about individuals than it once had. As Justice Louis Brandeis so presciently observed in his dissenting opinion in *Olmstead*,

> "in the application of a constitution, our contemplation cannot be only of what has been but of what may be." The progress of science in furnishing the government with means of espionage is not likely to stop with wiretapping. Ways may some day be developed by which the Government, without removing papers from secret drawers, can reproduce them in court, and by which it will be enabled to expose to a jury the most intimate occurrences

> of the home. Advances in the psychic and related sciences may bring means of exploring unexpressed beliefs, thoughts and emotions. . . . Can it be that the Constitution affords no protection against such invasions of individual security? (Brandeis 1928, p. 474)

Preservation of privacy is critical to a democratic political process. Change often begins most tentatively, and political discussion often starts in private. Journalists need to operate in private when cultivating sources. Attorneys cannot properly defend their clients if their communications are not privileged. As the Church Committee observed:

> Personal privacy is protected because it is essential to liberty and the pursuit of happiness. Our Constitution checks the power of Government for the purpose of protecting the rights of individuals, in order that all our citizens may live in a free and decent society. Unlike totalitarian states, we do not believe that any government has a monopoly on truth.
>
> When Government infringes those rights instead of nurturing and protecting them, the injury spreads far beyond the particular citizens targeted to untold numbers of other Americans who may be intimidated. (USSR 94 *Intelligence Activities: Rights of Americans*, p. 290)

> Persons most intimidated may well not be those at the extremes of the political spectrum, but rather those nearer the middle. Yet voices of moderation are vital to balance public debate and avoid polarization of our society. (ibid., p. 291)

What type of society does the United States seek to be? The incarceration of Japanese-Americans during World War II began with an invasion of privacy and ended in the tyrannical disruption of many individual lives. Could the roundup of Japanese-Americans have occurred so easily if the Census Bureau's illegal cooperation had not made the process so efficient? The purpose of the Bill of Rights is to protect the rights of the people against the power of the government. In an era when technology makes the government ever more efficient, protection of these rights become ever more important.

Citizens of the former Eastern Bloc countries attest to the corruption of society that occurs when no thought or utterance is private. No one suggests that people living in the United States face imminent governmental infringements of this type, but in 1972 Congressional staffers wrote that "what separates military intelligence in the United States from its counterparts in totalitarian states, then, is not its capabilities, but its

intentions" (USSR 92 *Army Surveillance*, p. 96). Electing officials we believe to be honest, trusting them to appoint officials who will be fair, and insulating the civil service from political abuse, we hope to fill the government with people of integrity. Recent history is replete with examples of abuse of power. Relying solely on intentions is dangerous for any society, and the Founding Fathers were careful to avoid it.

The right to be let alone is not realistic in modern society. But in a world that daily intrudes upon our personal space, privacy and confidentiality in discourse remain important to the human psyche. Thoughts and values still develop in the age-old traditions of talk, reflection, and argument, and trust and privacy are essential. Our conversations may be with people who are at a distance, and electronic media may transmit discussions that once might have occurred over a kitchen table or on a walk to work. But confidentiality—and the perception of confidentiality—are as necessary for the soul of mankind as bread is for the body.

Composed in LaTeX 2ε by the authors.
Set in Sabon by Loyola Graphics of San Bruno, California.
Printed and bound in the United States of America.

Library of Congress Cataloging-in-Publication Data

Diffie, Whitfield.
Privacy on the line : the politics of wiretapping and encryption / Whitfield Diffie, Susan Landau. — Updated and expanded ed.
p. cm.
Includes bibliographical references and index.
ISBN 978-0-262-04240-6 (hardcover : alk. paper)

1. Electronic intelligence—United States. 2. Wiretapping—United States. 3. Data encryption (Computer science)—Law and legislation—United States. 4. Electronic surveillance—United States—Political aspects. 5. Telecommunication—Political aspects—United States. 6. Privacy, Right of—United States. I. Landau, Susan Eva. II. Title. III. Title: Politics of wiretapping and encryption.

UB256.U6D54 2007
342.7308'58—dc22 2006035514