12
Conclusion

Control of society is, in large part, control of communication. From the right to assemble enumerated in the US Constitution to the anti-trust laws prohibiting competitors from agreeing on prices there is a tension between the right to communicate and limitations on communication. As society evolves, particularly as technology evolves, the government's power to control communications changes.

Telecommunication, barely a century and a half old, has so transformed society that, for most people in industrialized countries, it is a necessity, not an option. People move thousands of miles from friends and family, knowing that they can keep in touch by phone and email. People telecommute to work or, having commuted to the office, spend the day doing their work via telephone, email, and Web. People order goods from dealers on the other side of the continent by dialing 800 numbers or opening web pages. For a remarkable range and an increasing number of activities, telecommunication stands on an equal footing with physical communication.

Side by side with the growth of telecommunications there has grown up a major "industry" of spying on telecommunications. Communications interception has played a crucial role in intelligence since World War I, and despite improvements in communication security it continues to grow. The growth of interception is a consequence of the essential fact that the most important effect of the improvements in communications technology on communications intelligence has been to draw more and more valuable traffic into telecommunications channels. As a result,

spying on such channels becomes more and more rewarding for governments, businesses, and criminals.

Imagine three versions of an event, one taking place in 1945, one in 1995, and one in 2005. Each involves a major company with physically separated facilities. In 1945 it starts with a brief call, a minute or two. It invites you to an end-of-year project review. You must take a two-day trip to the Pfister Hotel in Milwaukee. It is a nuisance just before Christmas, but there is no alternative. By 1995, the invitation comes not by phone but by email. The project review is to be conducted by conference call and the associated final report will be sent to all the participants by fax or email. In 2005, the invitation again comes by email but now the meeting will take place using web-based collaboration and conferencing tools.

Now consider the significance of the changes from the viewpoint of industrial espionage. A 1945 spy who taps the phone has learned only that interesting information will be available at the Pfister Hotel in Milwaukee a few days hence. The spy knows where to go to get the information, but is still separated from it by substantial cost, work, and risk. On the other hand, the spy of 1995 can expect to have all the information appear on the same phone line the meeting invitation was issued. All that is necessary is to keep listening. The spy of 2005 is in a more complex position. The web conferencing tools operate over the Internet with its combination of high bandwidth and mobility. It is entirely possible for the spy to learn about the meeting—because one participant does email from a cafe with a free and unencrypted wireless connection—but be unable to capture the meeting itself—because the same participant attends from the office. A spy located inside the telecommunication system or, more likely, one who has ways of getting access to intercept facilities built into the telecommunication system, is in a much better position.[1]

The potential impact on privacy is profound. Telecommunications are intrinsically interceptable, and this interceptability has by and large been enhanced by digital technology. Communications designed to be sorted and switched by digital computers can be sorted and recorded by digital computers. Common-channel signaling, broadcast networks, and communication satellites facilitate interception on a grand scale previously unknown. Laws will not change these facts.

Governments have responded to the existence and relative transpa-

rency of telecommunications with some willingness to acknowledge rights of communication—in particular rights of private communication—where necessary but have been resistant to developments that could curtail this new ability to watch the citizenry.[2] The result has been an ongoing battle over the legal regulation of communications interception, the inclusion of facilities for interception in communication systems, and the deployment of security measures, particularly by the private sector. The first battleground was cryptography.

When it is not be possible to prevent communications from being intercepted, it may still be possible to protect them. The primary technology for protecting telecommunications is cryptography, which, despite its ancient origins, is largely a product of the twentieth century. For the first 50 years after radio brought cryptography to the fore in World War I, the field was dominated by the military. Then, in the late 1960s and the early 1970s, a combination of the declining cost of digital computation and foreseeable civilian needs brought a surge of academic and commercial interest in the field.

The work of the civilian cryptographers revealed two things. One was that cryptography was not a field that could effectively be kept secret.[3] In the 1930s and the 1950s—both formative periods in American military cryptography—computational capabilities lagged so far behind requirements that building secure cryptosystems took a lot of cleverness and used techniques not applicable elsewhere. By comparison, in a world in which inexpensive digital computing is ubiquitous, cryptography does not usually represent a large fraction of the computing budget.[4]

Today, constructing cryptographic devices and programs is regarded as easy. Developing sophisticated cryptographic hardware is within the abilities of a talented engineer or a small startup company.[5] Developing cryptographic programs is far easier; it is within the means of any competent programmer who possesses a copy of, for example, Bruce Schneier's book *Applied Cryptography*.

In the 1970s, independent cryptographers startled the cryptographic world by demonstrating that privacy can be manufactured "end to end" without the help of any centralized resources. Diffie-Hellman key exchange allows two parties to derive a secret from negotiations in which every bid and every response is public. This changed the basic power re-

lationships in cryptography. Before public-key technology, cryptography always required centralized facilities to manufacture and distribute keys, a feature particularly compatible with the top-down organization of the military. By contrast, public-key cryptography was developed to support the interactions of businesses in a community of equals.

Privacy is the best-known benefit of cryptography; however, it is not the only one, and it may not be the most valuable one. Cryptography also provides authenticity, which enables communicators to be sure of the identities of the people with whom they are communicating.[6] In a business transaction, authentication verifies that the person acting in one instance is the same person who acted in another—that the person who is writing a check, for example, is the same person who opened the account and put the money in it.

The US military responded to the rise of private cryptography by attempting to reestablish control over the technology through Atomic Energy Act-like prior restraint of research and publication.[7] When this effort appeared to have failed (largely as a result of its obvious unconstitutionality), the government attempted to control cryptographic products directly, first through standardization and later through regulation of exports. In 1993, it unveiled the concept of key escrow—cryptography that would provide protection against everyone except the US government. Although the notion was not well received, its proponents (most of them in the government) kept pushing, constantly giving ground to business objections but holding firmly to the view that it is the government's right to take measures to guarantee that citizens cannot encode things so that the government cannot read them.

Despite the government's intransigence, business pressures carried the day. Slightly less than seven years after the announcement of the key-escrow program, the export regulations—the only actual law with much effect on the use of cryptography—were changed.

In relaxing export controls on cryptography in early 2000 and abandoning its attempts to make escrowed encryption the norm, the US government effectively acknowledged defeat in its battle to control cryptography at a direct regulatory level. Cryptography, however, is not a technology that is easy to use on a large scale and those who predicted

that ubiquitous cryptography would make wiretapping and signals intelligence things of the past were flatly wrong.[8]

Ever since the explosion in cryptography brought on by the advent of radio in the early twentieth century, the technique has been at its best in protecting the communications of closely knit groups like national military organizations. Cryptography has been less successful when applied to serve the needs of looser groups like coalitions. Before the development of public-key cryptography, the use of cryptography in diverse communities was a non-starter. Cryptography is now a central technique, but many problems of scale are far from solved. It should not be surprising that the decline of regulation was not sufficient to deliver the overnight growth spurt that cryptography required to fulfill its promise.

The government's retreat from the attempt to stifle widespread use of cryptography has not been derailed by anti-terrorist fervor post-9/11; in fact, government promotion of cryptography has grown. The formal adoption of a high-grade cryptographic system as the Advanced Encryption Standard took place on November 26, 2001. A little over a year later, the system was approved for protection of classified information, and in 2005 NSA bestowed that status on a full suite of public cryptographic algorithms. The NSA's actions are seen as serving two ends. The algorithms are expected to lead to widespread commercial incorporation of the approved algorithms and thereby lower government procurement costs. They will also facilitate improved secure communication among the parties to the overnight coalitions that are so active in promoting modern wars.

The deployment of cryptography maintains slow but steady growth and, in the absence of a new regulatory assault, will eventually become ubiquitous. The high profile of the "crypto wars," however, drew attention away from other developments in communications privacy that may prove more important. At present, the battle over communications privacy is moving in new directions, focusing less on the protection of communications and more on their exploitation.

Over roughly a century US law has evolved the concept of wiretapping as a form of search to be controlled by court-issued warrants even more tightly regulated than those required for searches of physical premises.

Although law-enforcement agencies had been intercepting communications since the 1890s, it was not until 1968 that Congress put law-enforcement wiretaps on a solid legal footing. The Omnibus Safe Streets and Crime Control Act, which limited the use of wiretaps to certain crimes and established stringent warrant requirements, was upheld by the courts. As a result, wiretapping has become a generally accepted and ever more widely employed police practice. Law enforcement views the tool as essential, but a closer look at the data shows that things are not so clear cut.[9] Law enforcement spoke freely of its "right to use court-ordered wiretaps" and saw the use of cryptography as a threat to this right.

In discussions of the right to use cryptography, attention focused on the clearly discernible difference between the right to listen and the right to understand what one has heard. The doctrine of wiretapping as a type of search takes for granted the government's ability to practice wiretapping, just as the Fourth Amendment to the Constitution takes for granted the government's ability to break down doors and look under floorboards. It recognizes the power to intercept telecommunication, like the ability to search houses, as having such potential for abuse as to require stringent judicial control. It regulates the right to listen.

Guaranteeing the right to understand is different. To do that, you must regulate the individual to prevent him from taking actions that would otherwise be within his power to protect his communications from being understood. This seems analogous to the ludicrous notion that the government's right to search your house entails a right to find what it is looking for and a power to forbid people to hide things.

There is a important respect in which wiretaps are in conflict with the traditional notion of search in Anglo-American law. Searches have been, by legal intention and usually by physical fact, obvious. It is difficult to search a property and be sure that the search will not be detected. Furthermore, in a tradition dating back to English common law, secret searches were forbidden; where possible, the searchers were expected to knock and to announce their presence.

The no-secret-searches doctrine has been eroded in US law, at first by judicial tolerance and later by congressional action. In the 1970s courts began allowing federal agents to make secret entries into private property

in order to plant bugs (Burnham 1996, p. 133). As an outgrowth of the Aldrich Ames case—in which a secret search was conducted, but the legitimacy of the evidence so obtained never enjoyed court scrutiny—the Foreign Intelligence Surveillance Court was given the power under the PATRIOT Act to order secret searches.

Wiretaps, in contrast with searching or bug planting, are inherently difficult to detect. Although it behooves anyone who takes the privacy of communication seriously to assume that every word is being recorded, obtaining confirmation of that fact in any individual instance is usually impossible. Treating wiretaps as searches thus leaves open the possibility that wiretapping may be rampant, may be used as a mechanism of political and social control far beyond the bounds of proper law enforcement, and yet may go unchecked because of public ignorance. Under the "Title III" law of 1968, Congress sought to preclude this possibility by means of stringent reporting requirements. Individuals must be notified that they have been wiretapped, even if they are not prosecuted, and details of all legal wiretapping activity are collected and published in the annual *Wiretap Report*. In 1978, however, Congress created new authority to wiretap, primarily for counterintelligence purposes. Under the Foreign Intelligence Surveillance Act of 1978, only the total numbers of wiretaps are reported. Details need never be made public.[10]

In the shadows of the government's attempts to control the citizens' access to technology for protecting their communications (and thereby guarantee its ability to understand what it intercepts) lurked plans for a dramatic expansion of the basic ability to wiretap. The Communications Assistance for Law Enforcement Act of 1994 (CALEA) requires that telephone companies make their networks "wiretap ready" so that new features in communications do not interfere with government wiretapping.

This expansion of government power to search flies in the face of a gradual acceptance of a basic human right to privacy. Although it was already recognized in ancient times, privacy has come into its own as a legal entity only in recent centuries. In large part this has been a response to the developments of the technological age. Through a series of court decisions (including *NAACP v. Alabama*, *Griswold*, *Katz*, and *Kyllo*), the US Supreme Court expanded the notion of privacy that is implicit,

if never called by name, in the Constitution. Though private businesses often intrude upon individual privacy, the consequences of their intrusions pale beside the consequences of government intrusions. Over the past 50 years, government has, on myriad occasions, invaded the privacy of individuals in ways that threaten their fundamental rights. Citizens engaged in peaceful political activity (including the Socialist Workers Party, the civil-rights movement, and Vietnam War protesters in the 1950s and the 1960s, the Committee in Solidarity with the People of El Salvador in the 1980s, and the L.A. 8 in the last two decades), journalists and editors and political leaders (including Supreme Court justices) all have been wiretapped. Members of Congress who disagreed with the president's policies during the Vietnam era were subjects of biweekly FBI reports. Even politically uninvolved citizens who happened to use mail or telegraph to communicate internationally have had their communications intercepted.[11] Information obtained by the government for use in one venue has often been used in another. Census data were used to locate Japanese-Americans so they could be interned during World War II. Some "national-security" wiretaps under various presidents were actually investigations aimed at domestic politics.[12]

The government's record of privacy violations means that any broadening of its snooping powers must be viewed with the gravest concern. CALEA is the basis for a vast expansion of government surveillance powers. Even if the government's record of using its powers were not strewn with tales of abuse, there would be reason to worry.

Intentions can change far more quickly than capabilities. Today the authority of most government officials to use wiretaps is tightly regulated by laws, but laws can change. Were Congress to decide that wiretaps should be usable by any police department without court supervision —much as the police are free to employ stool pigeons without court supervision—the situation would change overnight. The capacity of the telephone system to support wiretaps, by contrast, would not. Although the pre-CALEA phone system was quite capable of supporting the 1500 or so wiretaps that occurred each year, it was not capable of supporting 10 or 100 times as many. Today, more than a decade after the passage of CALEA, this may no longer be the case. The way has been paved for a

vast expansion in government surveillance, and only an act of Congress will be required to bring it about.

The push to expand the interception of communications comes at a time when police have experienced an unprecedented expansion of their powers of surveillance in almost every area. Advances in electronics permit subminiature bugs that are hard to detect electronically or physically. Video cameras watch streets, shops, subways, and public buildings. Vast databases keep tabs on the credit, the possessions, and the criminal records of most of the population. Many of these facilities play far greater roles in criminal investigations than wiretaps.

The broadening and deepening penetration of telecommunications into our lives has also shifted the standards of non-governmental surveillance of communications. Although the telephone calls of workers who deal directly with the public are often monitored or recorded for "quality control and training purposes," in other areas of employment some respect for employee privacy seems to prevail. Whether actually required by law, customary, or merely seeming proper to everyone involved, there is still a notion that probable cause is required before an employee's communications can be spied on.

The Internet has changed all of this in two ways: surveillance has become nearly universal, and it is done not by people but by machines. The new instrumentalities of surveillance, moreover, are not passive, like tape recorders; they are active, blocking, censoring, and deleting communications. A number of factors have come together to bring this about.

The most conspicuous are the real dangers of Internet communication to enterprises. Break-ins, denials of service, viruses, and worms are all capable of interfering with enterprise computing, a feature of business that now is just as important as power and light and good employee health. Businesses have responded by installing firewalls that prevent the entry of any malevolent material they can recognize. Not only would it be hard to deny the legitimacy of this action, but in most cases it serves the interests of all parties. Employees are, by and large, grateful when their email is not so cluttered with spam that they miss messages on which doing their jobs depends.

Other measures put employees more at odds with their employers.

Although an employee could tell a company secret to an unauthorized person over the phone, that was not a channel by which an actual copy of a confidential document could be conveyed. Today companies ask "What is to prevent my employees from mailing my most valuable secrets to my competitors?" Responses vary. In extreme cases, like the intelligence agencies, there are separate internal and external networks with only the most tightly controlled connections. More commonly email is recorded so that leaks can be confirmed and analyzed by later investigation if the occasion arises. For companies that do not consider recording sufficient, there are programs that attempt to detect proprietary content in communications crossing the corporate firewall and either alert a security officer or block communications altogether. For a corporate security officer, every day's mail, email, and voice mail brings new pitches from companies claiming to do this more effectively.

Controlling improper use of the Internet by employees also makes up a big piece of the modern information-security pie. From one angle, recreational on the job use of the Internet is a productivity issue. If a job requires Internet use, it is difficulty to tell whether an employee is trying to get the best price for corporate travel or planning an upcoming vacation. In this respect, it is no different for the productivity concern about an employee who spends too much time chatting with friends on the telephone rather than chatting up customers. In another respect, it is far more serious. If an employee is looking at sexy pictures on a workplace display, another employee may be justified in filing a sexual harassment complaint, with devastating consequences for the employer.

Tools used to limit Internet browsing to material employers consider safe combine limitations on the sites that can be visited with scrutiny of the material received. The technology is unsettlingly similar to that employed by parents to control their children's use of the Internet.

Prospects for Intelligence

For thousands of years, a country could strictly limit what other nations could learn about it. Even though it might have difficulty protecting its border, travel was difficult, expensive, and time consuming. Travelers were conspicuous and treated with suspicion. Even when they succeeded

in traveling, acquiring information, and returning home with their information, the process might take years. The past century and a half, however, brought the camera, the airplane, and the spy satellite. The interiors of countries are no longer closed to view. They are visible to all the major powers, and with every passing year they are more visible to smaller countries, news media, and commercial interests. In recent years, the development of space technology has served intelligence well by putting cameras and antennas in orbit, where they can collect information about any nation.

If the principal effect of advancing communication technology on communications intelligence is to bring more valuable traffic into telecommunications channels, the secondary effect is increase the complexity of extracting it. Both intentionally protective measures (such as cryptography) and measures that are not primarily protective (such as the use of optical fiber), make the traditional SIGINT practice of starting with an antenna less productive.

In consequence, the character of the COMINT product is changing, improving in some respects and declining in others. Because people are often prone to mourn the loss of something on which they have come to depend and slow to see the possibilities of the unfamiliar, it would not be surprising to find that the change is perceived as decline by many COMINT professionals.

One area in particular in which COMINT has surpassed all other forms of intelligence, with the possible exception of HUMINT, is the discovery of opponents' intentions. Listening to people's communications—particularly when they are speaking or writing candidly out of misplaced faith in their security—can reveal their real objectives and the unspoken desires that underlie their public negotiating positions. This coveted capability is one that COMINT may have to surrender, and a replacement for it seems hard to find.

On the other hand, improvements in communications and increasing human dependence on communications will open new areas of intelligence. Network-penetration techniques will make it possible to capture information that is being stored rather than communicated, and such information is less likely to be encrypted. Even more exciting is the prospect that, in a world with hundreds of countries and thousands of

other centers of authority, there will be innumerable agencies responsible for issuing credentials and authorizing acceptance of other agencies' credentials. We will no doubt see numerous cases in which information is leaked to opponents because they are not recognized as opponents. Active network intelligence measures will become the HUMINT of the next century, and it will interact extensively with traditional HUMINT.

In the United States, and perhaps elsewhere, communications intelligence plays less of a role in industrial espionage than in national espionage. Businesses often have a better means of acquiring information: hiring workers away from their competitors. In the world of the Cold War, a world of open hostility between two major coalitions, changing sides was difficult. It did happen, and some people[13] made a big success of it, but it was a risky business and hard to do more than once. In a world of shifting alliances in which international competition is more commercial than military, defection may become as big a feature of national intelligence as of industrial intelligence.

Cryptography is much less successful at concealing patterns of communication than at concealing the contents of messages. In many environments, addresses (and, equally important, procedences) must be left in the clear so that routers will know how packets are to be forwarded. In most environments, the lengths and timings of messages are difficult to conceal. SIGINT organizations are already adept at extracting intelligence from traffic patterns and will adapt to extract more. The resulting intelligence product, abetted by increases in computer power, may not give as detailed a picture in some places but will give a more comprehensive overview.

Some improvements in SIGINT technology cannot easily be categorized as tactical or strategic. They take the form of increased speed and flexibility of the sort that has changed many organizations over the past decades. The current intelligence cycle in SIGINT is a slow one that can be summarized as follows:

- Intelligence consumers formulate requirements.
- The requirements are translated into guidelines about what to intercept.

- Intercepted material is acquired "in the field" and shipped home for analysis and interpretation.[14]
- On the basis of cryptanalysis, interpretation, and political analysis, the information is judged, as are the guidelines under which it is acquired.
- The guidelines are either continued or modified. New intercept facilities may be assigned to a project, new facilities may be built, new instructions on traffic characteristics may be issued, or the project may be dropped.

This process may take weeks, months, or years. Often, significant information will not be acquired simply because it was not being looked for.

Increasing automation and decreasing size and cost of electronic equipment will make for vast improvements in this cycle, resulting in a tighter "target, intercept, analyze" loop. This will be aided by the development of tamper-resistance technology. The secrecy of many SIGINT processes makes intelligence organizations reluctant to use them anywhere but in the most secure areas of their own headquarters. Tamper-resistant chips allow intercept equipment in the field to perform such sensitive operations as cryptanalysis. This permits them to search the contents of ciphertext messages just as they would the contents of plaintext messages.[15]

An example of a SIGINT technology with unfathomed potential is emitter identification. The vanishing cost of signal processors has reduced the cost of this technology and so expanded the range of possible uses.[16] In many cases, emitter identification will counter the concealment of addressing by link encryption.

Not all the growth that can be expected in SIGINT will result from SIGINT technologies. A fast-growing portion of the telecommunications market all over the world is *fixed-position cellular telephony*. The cost of radio technology has dropped to the point that in many rural areas it is cheaper to have a cellular telephone in each house than to run wire. The result is that a whole segment of the telecommunications market that was once effectively out of reach of intelligence organizations is now coming, at least partly, within its grasp.

From a practical viewpoint, it is important to note that nothing will

happen overnight. The vast legacy of equipment, services, experience, and investments in communications from the twentieth century will guarantee the future of much of communications intelligence well into the twenty-first.

Prospects for Law Enforcement

The dramatic growth of technology in the twentieth century has given law enforcement a wide variety of technical capabilities, one of which is wiretapping. At present, law-enforcement personnel are worried that advances in communications technology, particularly in cryptography, will lead to a decline in the usefulness of wiretaps. Should this happen, its effect on law enforcement is likely to be modest. Even among tools of electronic surveillance, wiretaps are generally overshadowed by the many kinds of bugging devices used to intercept face-to-face conversations. Electronic surveillance, furthermore, plays a minor role in police investigation by comparison with record keeping, photography, and a broad spectrum of forensic techniques.

Even before CALEA, wiretapping would appear to have gained more than it has lost (and perhaps more than it stands to lose) from modern technology. At one time a wiretap was, literally, a pair of wires attached somewhere between the target's telephone and the telephone office. Its placement and its use entailed a risk of discovery and brought the listeners only disembodied voices. Today, even without the vast wiretapping capacity envisioned by CALEA, wiretaps are "installed" in the software of digital telephone switches. Knowledge about installed wiretaps can be kept to a few telephone-company employees. More important, the taps carry with them extensive call-status information that often makes the identities of the talkers or their locations immediately available.[17]

Law enforcement's gains from advances in technology are not, however, limited to investigation. The police are a mechanism of social control (Manning 1977, p. 23), and their work goes hand in hand with other mechanisms of social control. Improving communication is enhancing "employee supervision" throughout society. In the past, ambassadors and senior military commanders were sent off to the other side of the world with general mission statements and no opportunity to report their

successes and failures—let alone ask for advice—for months or years. Today, the president can reach his senior emissaries at a moment's notice anywhere on Earth. At lower levels, employees in many jobs are now monitored by machines. Workers who once had substantial autonomy, such as truck drivers, find that they are subject to the same sort of close monitoring that might have been expected on a factory floor.[18]

Society is also gaining an ability to keep close track of individuals' interests and expertise. Online uses of information resources are intrinsically less private than paper ones. For example, monitoring which documents visitors to libraries consult or what pages they copy would be expensive and, despite the FBI's Library Awareness Program, is probably rare. When people consult sources of information on the Internet, however, monitoring is inexpensive and hard to separate from services the users value. Commercial Web pages record IP addresses and other available information about the "callers" and use it for marketing. Exchange of information among Web sites presents the prospect of a comprehensive profile of each Web user.

The current debate is not, as it was in the 1990s, about the public use of strong cryptography, but rather about communications security and building wiretap capabilities into network infrastructure. At a hearing on the subject of CALEA in 1994, FBI Director Louis Freeh and Senator Larry Pressler had a spirited discussion of the issue (USSH 103 *Digital Telephony*, p. 202).

Asked to state his view of the proper scope of CALEA, Freeh said: "From what I understand . . . communications between private computers, PC-PC communications not utilizing a telecommunications common net, would be one vast arena, the Internet system, many of the private communications systems which are evolving. Those we are not going to be on by the design of this legislation." Pressler pressed him: "Are you seeking to be able to access those communications also in some other legislation?" Freeh responded: "No, we are not. We are satisfied with this bill. We think it delimits the most important area and also makes for the consensus, which I think it pretty much has at this point." Pressler then asked: "Yes but in the future, will you be seeking the ability to tap into those other forms of communication?" Freeh gave a prescient response: "It is certainly a possibility. I am sure if, God forbid, somebody

blows up the World Trade Center 10 years from now using a PC-PC private communications network, a question would validly be raised in the Congress and by the President as to whether that form of communication now needs to be accessed. But we are not taking that position now. We are not contemplating coming back and asking for additional coverage." Pressler asked for clarification: "So what we are looking for is strictly telephone to telephone, what is said over a telephone?" Director Freeh said: "That is the way I understand it, yes, sir."

In 2001, the World Trade Center was blown up (or at least "knocked down") and, although no one has suggested that the Internet played any significant role, the FBI is indeed seeking to extend CALEA. Is extending built-in wiretapping from the switched telephone network to the Internet a wise precaution or an imprudent risk?[19] In addressing a parallel issue, the National Research Council report on cryptography concluded that "on balance, the advantages of more widespread use of cryptography outweigh the disadvantages" (Dam and Lin 1996, p. 6). Apparently accepting this view, the US government began encouraging the development of strong cryptography in the infrastructure in 2000. We believe the same course would be appropriate here. On balance we are better off with a secure communications infrastructure than with one that builds surveillance into the network fabric. At times this may press law enforcement to exercise more initiative and imagination in its investigations. On the other hand, in a society completely dependent on computer-to-computer communications, the alternative presents a hazard whose dimensions are as yet impossible to comprehend.

Prospects for Security

The world we face now is different from the one many of us envisioned after the demise of the Cold War. Due to various causes—the rising economies of China and India, the rapid rate of globalization—the American hegemony so visible today is likely to have faded by the end of the twenty-first century. The US will undoubtedly remain a major power, but it is unlikely to dominate the world at the end of the twenty-first century as it does at its dawn. Such changes are to be expected and should be part of any national-security planning. What has been less planned for—

or at least less anticipated by the general populace—is the rise of nonstate actors and their willingness to perform acts of violence and terror on a grand scale.

Despite poor beginnings, prospects for the security of our information infrastructure are good but only if we accommodate security in our plans from the beginning. Part of the reason for the current poor state of information security is the fear, uncertainty, and confusion created by government opposition to the use of strong cryptography in the 1990s. As the FBI acknowledged, "the use of export controls may well have slowed the speed, proliferation, and volume of encryption products sold in the US" (Dam and Lin, p. 138). Given the enemies we have now, and society's reliance on electronic communications for everything from personal affairs to control of critical infrastructure, it is vital that our computing and communications be properly secured. This means secured against attacks from the outside *and* from the inside.

Time scale is very important. Building interception into our communications system is appealing as a tactical move. The institutions that will have access to this intelligence and law-enforcement resource are institutions that have grown up over the course of the twentieth century and, despite being secretive, are known to the American public. Initially, the new facilities will be far more familiar to those who use them than to those against whom they are used and may be quite efficacious. What will happen to the control of these facilities as the decades pass is hard to assess. Undoubtedly, opponents will become more proficient at employing countermeasures to useful interception. More frightening is the prospect that opponents—particularly opponents within our own society—will learn to turn the new tools to their own advantage.[20] Although a case of this kind has yet to come to light in the United States, there has been one in Greece. For well over a year, interception facilities built into cellular telephone systems were used to tap the phones of over 100 Greek government officials.[21] Who was doing the tapping remains unknown.

In the early 1960s, President John Kennedy promised a new level of control over nuclear weapons. When Don Cotter, director of Sandia National Laboratories, called his senior staff together and told them to start working on this problem, they expressed doubts about what to do when they had only an overall direction and no detailed policies.

"Hardware," Don Cotter told them, "makes policy."[22] In one sense, laws represent a society's highest form of decision making. They are are difficult and expensive to change but not the most difficult or expensive things to change. Long-term investments in infrastructure are even harder to change. Lawrence Lessig put this another way when he titled a book *Code and Other Laws of Cyberspace*. What is committed in design, development, and availability binds everyone, often more firmly than law.

Suppose that the key-escrow program of the 1990s had been successful. Suppose that millions of devices conforming to the Escrowed Encryption Standard had been sold, rather than merely a few thousand. Can there be any doubt that the same junior lawyers in the administration who wrote memos rationalizing the expansion of SIGINT to allow warrantless interception of phone calls between a foreign phone and a domestic one, would argue that the database of escrowed keys should be put at NSA's disposal?

The lesson is simple and unavoidable. By building the machinery for surveillance into the US communication system, we overcome the largest barrier to becoming a surveillance society on a possibly unprecedented scale. By comparison with the years of development and deployment needed to put the system in place, legal decisions to use it in ways that might have been unthinkable when it was approved can be made quickly.

What Kind of Society Do We Want?

In deciding that the Constitution protected Charles Katz against electronic surveillance even though there was no intrusion onto Katz's property, the Supreme Court looked through the propertarian technicality of the Fourth Amendment to its essential objective. As human society changes from one dominated by physical contact to one dominated by digital communication, we will have many opportunities to choose between preserving the older forms of social interaction and asking ourselves what those forms were intended to achieve.

In the societies that have dominated human culture for most of its existence, a general awareness of the pattern of contacts among people was an essential feature of life. In a society dominated by telecommunication, a pattern of contacts is far less visible to the ordinary person and far more

susceptible to monitoring by police and intelligence organizations. This produces a fundamental shift of power away from the general population and into the hands of those organizations.

Technology seems to make some losses of privacy inevitable. The capacity to build databases and feed them the details of every credit-card transaction exists, and the result is an excruciatingly detailed portrait of the shopping, traveling, and trysting habits of hundreds of millions of people. Yet, since such databases are an essential component of today's commerce and millions of people work in the industries they support, it seems realistic to accept them. The best we can hope to do is regulate their use in a way that protects individual privacy.

We also seek to preserve both the individual's and the society's security. This is where the government's plans regarding the wiretapping of VoIP and other real-time communications[23] seem remarkably short-sighted. Combining Internet surveillance with inexpensive automated search engines could lead to an unprecedented compromise of American security and privacy (Landau 2006). (The "Titan Rain" exploits described in chapter 4 give a sense of some of the potential problems.) A wiretap is, after all, nothing more than an authorized security breach. This approach is made worse by the direction of the Internet's development. Currently there are millions of devices connected to the Internet, but we are moving to a situation of billions of small devices, such as radio-frequency ID tags and sensors, many of which will communicate via the Internet (ibid.).

Noting the comments of Ayman al-Zahawiri, former leader of the Egyptian Islamic Jihad and second-in-command of al-Qaeda, that "however far our capabilities will reach, they will never be equal to one-thousandth of the capabilities of [our enemies]" (Richardson 2006, p. 232), Louise Richardson observes that we must turn the terrorist threat against itself. We should not take our strengths, which include modern and robust communication systems, and turn them into instruments of surveillance that others can use against us.

Cryptography in Context

The words of the Supreme Court's *Katz* opinion have an importance that transcends the development of American wiretap law. They echo in

concrete form Louis Brandeis's view that "time works changes." If there is a right to use cryptography, it must grow from the historical fact of private conversation. Since many conversations today can take place only by telephone, stepping away from other people is no longer a universally applicable security measure. It is not realistic to say to someone "If you don't like the possibility of being tapped, you have the choice of not using the telephone." Stepping away from other people is the expression of a right to keep conversation private in a face-to-face world; use of cryptography is an expression of that right in an electronic world.

In a sense, it is curious that the Constitution regulates the power of the police to search (and, derivatively, their power to conduct electronic surveillance) but leaves activities that are at least as dangerous and disruptive, such as the use of undercover agents and the mounting of sting operations, up to individual detectives or their chiefs.[24]

In light of the curiously small number of prosecutions in which wiretap evidence plays a significant role, it appears that wiretapping is far more valuable as an intelligence tool than as a way of gathering evidence. This utility, however, is not recognized by US law, under which wiretap warrants must name particular suspects and crimes. Police who wish to use wiretaps in the gathering of intelligence are therefore forced into the duplicitous position of representing any wiretap as an attempt to gather evidence. A reform of wiretap law might plausibly recognize the police intelligence applications of wiretapping and give courts the means to supervise it.

Technology might also be applied to streamline the courts' oversight of law-enforcement activities, just as it has made so many improvements in the activities themselves. It seems certain that at some time in the future courts will choose to accept applications and issue warrants electronically, using digitally signed messages. This would reduce law enforcement's logistic overhead and would permit warrants to be more carefully focused. Police might, for example, be more readily granted a warrant limited to communications between two people than a warrant encompassing all the communications of one person. Quick turnaround would permit police to base such warrant requests on the calling patterns of suspects and to get a new warrant promptly when a new link in a con-

spiracy was identified. Such an arrangement would respond to Brandeis's concern that "whenever a telephone line is tapped, the privacy of the persons at both ends of the line is invaded" (Brandeis 1928, pp. 475–476) by making an effort to target only calls in which both participants were suspects.

Of course, if the utility of wiretaps is no greater than the publicly available evidence suggests,[25] perhaps they should be dropped from police methodology altogether—not because they are an invasion of anyone's privacy, but merely because they are a waste of tax money.

Where Are We Headed?

In the first phase of the communications technology and privacy battle, the central question was very simple: Do people have a right to private communication, and should they be free to express and enforce this right by using cryptography? In the newer phase, the questions are more complex. It is hard to argue that society—including the government and the private sector—has a right to employ communication surveillance to counter imminent threats. On the other hand, there is little question that surveillance has a chilling effect on many activities, from art to politics to personal relations. Can we find a set of rules that give us adequate protection without stripping us of our privacy and autonomy, protected as the protectors see fit, rather than as we see fit.

For many decades a simple dichotomy has served us well in judging the legitimacy of communications interception. Outside the country, national intelligence agencies were allowed to intercept whatever foreign communications they could acquire and considered worth recording. Inside the country, interception followed the reasonable search-and-seizure model of law enforcement. Communications could not be intercepted without probable cause, and that probable cause had to be based on legitimately obtained evidence, typically of some other kind. Although 'inside' and 'outside' are not entirely clear, a workable set of rules has been found. Inside is inside. Communications originating or terminating inside the US, even when they originate with foreign companies or foreign embassies or foreign spies, can be monitored only under the court-regulated model

of reasonable searches and seizures. Communications between entities outside the United States can be monitored fairly freely. Moreover, they can be monitored from US territory: the US proper, foreign US military bases, or US embassies.

'Inside' and 'outside' are fairly static notions. A foreign embassy, with its extraterritorial status, may seem to blur the inside-outside distinction, but at least it stays put for years at a time. As travel and communications have become more fluid, determining what is inside and what is outside has become harder. Communications between foreign entities that can be intercepted from antennas at Yakima are unequivocally foreign under the current rules. What about packets entering the United States at the same location and headed for addresses in Europe? Should these be regarded as foreign traffic that happens to have passed close enough to be intercepted—like the radio signals picked up by the antennas—or should they be regarded as domestic traffic because they are traveling over resources provided by US companies and are entitled to protection as invited guests?

Even more provocative are the questions raised by travel. Suppose that intelligence has been monitoring a terrorist traveling abroad and tracks the terrorist onto a flight to New York. Cutting off monitoring at the border would seem particularly foolish if the earlier monitoring showed that the terrorist was on the way to attack a target in the United States. On the other hand, if such emotional cases are allowed to hold sway, we will find ourselves in a world where government can rationalize monitoring anything. Furthermore, if the intelligence model of secrecy about what is being monitored holds sway, as the growing use of FISA rather than Title III wiretaps suggests, the rationale may not have to be explained to very many people.

The task is simple to explain but far harder to achieve. If we do not incorporate adequate security measures in our computer and communications infrastructure, we risk being overwhelmed by external enemies. If we put an externally focused view of security ahead of all other concerns, we risk being overwhelmed by their misuse. We must find a set of rules and a mechanism for overseeing those rules that allows society to defend itself from its genuine enemies while keeping communication surveillance

from stifling dissent, enforcing morality, and invading privacy. If we do not, the right to use privacy-enhancing technology that was won in the the 1990s will be lost again.