FROM
"PRIVACY ON THE LINE"
BY DIFFIE AND LANDAU

10
Conclusion

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 on the phone talking to distant offices or customers. People order goods from dealers on the other side of the continent by dialing 800 numbers. 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 telecommunication 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.

Consider two sets of imaginary events, one taking place in 1945 and the other in 1995. Both take place within major companies with physically separated facilities. The 1945 call is brief, 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. Half a century later, the project review might very well be conducted by conference call, and the associated final report might be sent to all the participants by fax or email.

Now consider the impact of a competitor's intercepting the communications. The 1945 spy has learned only that interesting information will be available at the Pfister Hotel in Milwaukee a few days hence. He knows where to go to get the information he wants, but is still separated from the information by substantial work and risk. On the other hand, the 1995 spy will have all the information handed to her on the same circuit through which she learned about the meeting. All she has to do is keep listening.

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.

It may not be possible to prevent communications from being intercepted, but it is possible to protect them. The 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.[1] 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.[2]

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.[3] 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*.

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 relationships in cryptography. Before public-key technology, cryptography always required centralized facilities to manufacture and distribute equipment and 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 they are communicating with.[4] 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.[5] 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) have 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.

Over roughly a century there evolved in the United States the concept of wiretapping as a form of search that should be controlled by court-issued warrants similar to 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, if not widely employed, police practice. Law enforcement speaks freely of its "right to use court-ordered wiretaps" and appears to think of the use of cryptography as a threat to this right.

There is a clearly discernible difference, however, 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 another problem with the notion of wiretaps as searches. Searches are, 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 confront the householder.[6] Wiretaps, in contrast, are invisible. 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*. Ten years later, 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.[7]

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) have been accompanied by a dramatic expansion of the basic ability to wiretap. The Communications Assistance for Law Enforcement Act of 1994 (CALEA) requires telephone companies make their networks "wiretap ready" so that new features in communications do not interfere with government wiretapping.

The government is attempting to expand its powers of search despite the 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*, and *Katz*), the US Supreme Court expanded the notion of privacy that is implicit, but never given that name, in the Constitution. Though private businesses often intrude upon individual privacy, their intrusions pale beside those of the government. Over the past 50 years, government has invaded individuals' privacy on myriad occasions. Citizens engaged in peaceful political activity (including the Socialist Workers Party, the civil rights movement, and protests against the Vietnam War in the 1950s and the 1960s and the Committee in Solidarity with the People of El Salvador in the 1980s), 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.[8] 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.[9]

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. As even the government will admit, its efforts have succeeded in slowing down cryptography's progress and its use in the public sector. Even were the government's record of using its powers 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 law. Laws, however, 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 could change overnight. The capacity of the telephone system to support wiretaps, by contrast, would not. Although the present-day phone system is quite capable of supporting the 1500 or so wiretaps that now occur each year, it would not be capable of supporting 10 or 100 times as many. But if the FBI has its way, in a decade or two, after the impact of CALEA has been felt, this may no longer be the case. The way will have 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, and any loss of investigative power that results from changes in communications technology seems minuscule in comparison.

The Government's Case

Throughout its history, the National Security Agency has sought to prevent the development of cryptography in the public world. In the 1960s, NSA tried to prevent the publication of David Kahn's popular book *The Codebreakers* (Bamford 1982, pp. 125–126). In the 1970s, its director, Bobby Ray Inman, threatened the academic community with prior restraint. In the early 1980s, it tried to halt other government funding of academic research in cryptography, and it also tried to prevent the publication of James Bamford's history of NSA, *The Puzzle Palace*. In the mid 1980s it succeeding in getting the Reagan administration to promulgate NSDD-145, a directive that sought to expand NSA's authority to include control over the technology for handling "sensitive but unclassified information."

The NSDD-145 effort backfired, and instead increased responsibility for computer security standards (including those for civilian cryptography) being given to the National Institute of Standards and Technology. Unfortunately, the Computer Security Act of 1987, which conferred this responsibility on NIST, was not accompanied by sufficient funding to enable NIST to do the job. The NSA, which had vastly greater resources, forced NIST into a Memorandum of Understanding that shackled NIST's attempt to develop its own cryptography standardization program. The dismal record of the Digital Signature Standard is one example. The Clipper episode, an even more striking example of the misuse of the standards process to further NSA's aims rather than the goals of the law, resulted in the demise of the AT&T TSD 3600, the first mass-market telephone-security device. For over a decade, cryptography policy in the Commerce Department has been dictated by NSA.[10]

Despite its apparent ability to control NIST, NSA has acted like an agency under fire ever since the passage of the Computer Security Act. The law, after all, is quite clear about where responsibilities lie, and a different Congress or a new president might decide that US interests are best served by a liberal policy regarding the use of cryptography. NSA's decision to involve the FBI in the cryptography wars proved astute.

The end of the Cold War had diminished the heft that national-security arguments carried, and even that weight had proved insufficient to guarantee NSA the role it sought under the Computer Security Act. It was one thing to bend everything to the will of an intelligence agency in a world where the United States had an enemy that could annihilate it on a day's notice. It was quite another in a world where people were talking about the degree to which intelligence could assist US industry.

In the post-Cold War world, law enforcement was playing a more significant role in national-security issues than ever before. Involvement of the FBI in cryptography policy had the potential to result in a rewriting of the government equation on encryption. In the late 1980s, when the FBI learned about encryption, it asked the Senate Judiciary Committee for a resolution calling on telephone companies to provide the plaintext of any encrypted messages that were encountered during court-authorized wiretapping. The FBI also submitted "digital telephony" bills to Congress.

The FBI's Advanced Telephony Unit studied encryption. In 1992 it warned that by 1995 no more that 40% of Title III wiretaps would be intelligible and that in worst case all might be rendered useless (Advanced Telephony Unit 1992). In 1994, when he testified before Congress in support of the "Digital Telephony" bill (later passed as CALEA), FBI Director Louis Freeh emphasized the importance of wiretaps in solving kidnappings and in preventing terrorist actions (Freeh 1994b).[11] Freeh claimed that the FBI sought only to maintain the status quo given to law enforcement by Title III and to keep up with the new technology. Whatever truth there may be in these statements is hard to find. In 1994 Assistant Attorney General Jo Ann Harris admitted that, a year after the introduction of the Clipper proposal, the FBI had yet to encounter a single instance of encrypted voice communications (Harris 1994).[12] Two years later, the National Research Council panel was also unable to find any FBI Title III surveillances that had encountered problems due to encryption (Dam 1997, p. 3). Freeh had claimed in February 1994 that hundreds of wiretaps had been rendered useless by advanced switching technology, but he cited only 93 instances when he testified to Congress a month later. Even then, not all of the instances Freeh cited were wiretaps; some were electronic bugs, which are not affected by encryption.

FBI Directors have always emphasized the use of wiretaps in kidnapping investigations, and Louis Freeh was no exception. In fact wiretaps were used on average in only two to three kidnapping cases a year in the period 1968–1993.[13] Terrorist actions were likewise cited as an important reason for wiretaps, despite the fact that there were no Title III wiretaps in terrorist cases in the period 1988–1994.

In pressing for various new wiretapping capabilities, FBI Assistant Director James Kallstrom argued: "... just for the FBI alone, we have used court-authorized electronic surveillance to capture terrorists intent on blowing up buildings and tunnels in New York, to detect and capture pedophiles who intended to brutally murder their intended victim, to arrest and convict various organized crime leaders like John Gotti, and to successfully investigate a spy whose espionage cost many their lives" (Kallstrom 1997). However, the Rahman case ("terrorists intent on blowing up buildings and tunnels in New York") turned not on wiretaps, but on other forms of electronic surveillance, including a body wire (which does not require a warrant); the valuable evidence in the Gotti case came from an electronic bug;[14] and the wiretap in the Ames case ("a spy whose espionage cost many their lives") served in a tangential fashion, enabling the government to pressure Ames to reveal information in order that his wife—whose knowledge of his spying activities was revealed on the wiretaps—receive a reduced sentence.[15]

Immediately after the Oklahoma City bombing and the TWA 800 explosion, the FBI called for expanded wiretapping capabilities, even though wiretapping would not have prevented Oklahoma City and the FBI has now acknowledged that TWA 800 appears to have been the result of mechanical failure. The FBI's interpretations of CALEA have included substantial expansions of wiretapping capabilities, and some of the FBI's requests (e.g. in regard to locations of cell phones) were actually in direct contradiction to the law.

NSA was fighting a turf battle with NIST, and was using the cloak of national security to make its arguments. The FBI, on the other hand, stretched the truth and distorted the facts. Few of the government's arguments regarding the criticality of wiretaps in criminal investigations hold up under scrutiny. It seems fair to conclude that the government has not made its case regarding encryption.

Prospects for Intelligence

For thousands of years, a country could strictly limit what other nations could learn about it. 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 communications intelligence just as it served photographic intelligence, allowing giant antennas to be put in orbit where they can catch signals from any nation. However, the growth of technology bodes another change: the development of encryption may cause a steady decline in the amount of intercepted traffic that can be understood.

As we have stated before, the principal effect of advancing communication technology on communications intelligence is to bring more and more valuable traffic into telecommunications channels. By comparison with the explosive expansion in the use of telecommunications, the application of protective measures will turn out to lie somewhere between "less important" and "insignificant." Losses due to encryption will be mitigated by many factors, and communications intelligence will be with us for as long as people communicate.

That is not so say that communications intelligence will be untouched or unchanged by the spread of cryptography. It seems likely, indeed, that the character of the COMINT product will change, 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 will not be surprising if 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[16] 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.

Tactical communications intelligence will probably improve despite the prevalence of encryption. Cryptography is much less successful at concealing patterns of communication than at concealing the contents of messages. In many environments, addresses (and, equally important, precedences) must be left in 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.[17]
- 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.[18]

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.[19] 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 where, 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.

Yet 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.[20]

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.[21]

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.

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 industry they support, it seems realistic to accept them. The best we can hope to do is to regulate their use in a way that protects individual privacy.

On the other hand, perhaps the compilation of databases—born of the need for billing and credit verification, but later put to numerous intrusive marketing uses—can be avoided by means of another technology. One strong theme in electronic commerce is a return to the anonymity of money. If you have funds in your electronic wallet, you can spend them, and merchants have no need to know who you are or how good your credit is. In such an environment, the desire of marketers to keep records on customers could well give way to the customers' desire for privacy.

The area in which technology can most clearly make a positive contribution to privacy is encryption. If we assert the individual's right to private conversation and take measures in the construction of our communication systems to protect that right, we may remove the danger that surveillance will grow to unprecedented proportions and become an oppressive mechanism of social control. Fortunately, the fight for cryptographic freedom, unlike the fight against credit databases, is a fight in which privacy and commerce are on the same side.

The great vision of electronic commerce is an orgy of buying and selling over the Internet, and the vastness of the Internet is essential to this vision.

This vastness is less a function of the tens of thousands of miles over which it spreads or of the millions of computers connected to it (though this comes closer) than of the diversity of those computers—a diversity of hardware, a diversity of protocols, a diversity of tasks, a diversity of ownership, a diversity of businesses, a diversity of regulatory environments, and a diversity of objectives.[22] What is required in this environment is what public-key cryptography has made possible: secure communication between parties with minimal trust. Requiring key escrow, which came to seem natural to the military mind as a result of decades of a key management system that amounted to escrow, would cripple cryptography's contribution to secure worldwide communication.

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.

The discussion of which this book is part has focused on whether cryptography should be allowed to develop in response to commercial and technical influences or whether it should be regulated by governments. This narrow question excludes consideration of many possibilities —technical and otherwise—that address the larger social issues on which communications privacy bears.

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.[23]

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 conspiracy 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,[24] 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.

What Is Possible?

Cryptography, once an arcane art, is now inseparable from mainstream computing technology. Cryptographic equipment is neither difficult to build nor demanding in its computing requirements. Any attempt to control the deployment of cryptography must contend with this fact. Attempting to control cryptography is more like the notoriously unsuccessful attempt to outlaw alcohol than it is like the control of guns, the manufacture of which is beyond the capabilities of the typical home shop.

Furthermore, antisocial uses of cryptography are less demanding than socially beneficial uses. A group of conspirators trying to rob a bank, blow up a building, or commit fraud is typically small, rarely more than a dozen people. On the other hand, the use of cryptography in electronic commerce will require providing millions of people with interoperable cryptographic devices and a steady supply of supporting electronic credentials. In short, the latter is probably controllable; the former probably is not. In pursuing policies that limit the use of cryptography for business purposes, out of fear that it will be used for criminal ones, we deny ourselves one benefit without achieving the other.

It has been argued that it is important to prevent the ubiquitous use of cryptography in order not to lose the ability to monitor communications between criminals and non-criminals. Arranging any substantial crime, from a bank heist to a bombing, is likely to entail commonplace actions such as renting cars, booking hotel rooms, or buying airplane tickets. If the police can monitor the phone calls in which criminals transact the ordinary part of their business, they will have a very good idea of what the criminals are up to, even if all the calls from criminal to criminal are encrypted. On the other hand, since the signaling information will tell the police what legitimate businesses the suspects are calling, the police will be able to approach the businesses and make enquiries.

Another area in which cryptography is said to be interfering with police work is the protection of stored data. One view holds that searches and seizures of computer media are far more important to police than wiretaps, and that cryptography may make them ineffective. The precise importance of seized computer media is hard to judge. The FBI has a central laboratory for processing those that cannot be adequately examined by field offices.[25] This lab handled about 400 cases in 1994, of which it estimated that 2% involved cryptography. This does not mean that the FBI was unable to read the files; in any case, it is probably a generous estimate that counts anything that could possibly be called cryptography.[26]

The protection of storage—particularly as it might be applied to protecting the records of a criminal group—appears to be a less complex phenomenon than the protection of communications. In the former case the decrypting can be done by the person who did the encrypting, reducing problems of key management. In view of the fact that the desire to protect the information in readily stealable laptop computers provides widespread motivation to use encrypted storage, it appears unlikely that any law would be effective in preventing the encryption of stored data in non-escrowed systems.

It is also appropriate to ask what is legally sustainable. The Constitution has a strong principle of freedom of speech that is generally interpreted as encompassing the freedom to write and publish. It is the US government's current position that publication of programs on the Internet is not protected free speech and can legitimately be regulated as export. This view has been challenged by the mathematician Daniel Bernstein, who has asserted a free-speech right to publish the code of a cryptographic algorithm electronically. Bernstein has won the first round. In June 1996, US District Court Judge Marilyn Hall Patel ruled that computer programs are a form of speech and thus subject to First Amendment protection.[27] In a stinging opinion issued later that year (*Daniel Bernstein v. United States Department of State,* 945 F. Supp. 1279. (N.D. Cal. 1996)), Patel held that the government's action was an unconstitutional prior restraint on free speech, but the issue will not be effectively decided until the case makes its way to the Supreme Court.[28] If free speech prevails, export control may be entirely bypassed. This will likely be true even if the government's narrower position—that executable computer programs are not protected—is upheld. If technical papers and standards and other non-executable information can circulate freely, compatible cryptographic system can simply be implemented locally, and no exports or imports need actually occur.

Suppose We Were to Make a Mistake?

Suppose we were to allow the unfettered development of cryptography and later decide that government access to communications is necessary?

Suppose we were to build surveillance into our communications although none is needed? Which would be the more serious error?

It is generally accepted that rights are not absolute. If private access to high-grade encryption presented a clear and present danger to society, there would be little political opposition to controlling it. The reason there is so much disagreement is that there is so little evidence of a problem.

If allowing or even encouraging wide dissemination of high-grade cryptography proves to be a mistake, it will be a correctable mistake. Generations of electronic equipment follow one another very quickly. If cryptography comes to present such a problem that there is popular consensus for regulating it, regulation will be just as possible in a decade as it is today. The laws will change, strong cryptography will not be made part of new products, and the ready availability that government claims to fear will decline quite quickly. If, on the other hand, we set the precedent of building government surveillance capabilities into our security equipment, we risk the very survival of democracy.

Control of cryptography is being promoted on the grounds that it will protect our sources of foreign intelligence and protect the ability of police to use wiretaps to investigate criminals. None of the current plans seems to offer much hope in either direction.

Key escrow would protect our ability to collect intelligence against other countries only if we could persuade them to escrow their keys in the United States. Had the Clipper system had any chance of achieving worldwide deployment, it might have served this function; its escrow agents appear capable of providing keys in real time,[29] which would allow intercept equipment to make use of them in deciding whether traffic was worth recording. More recent proposals appear to recognize the infeasibility of persuading countries to accept extra-territorial escrow and to acknowledge that key escrow will function under the laws of the countries in which it operates. We have argued that cryptography can be implemented by a startup programmer. It can probably be implemented by any industrialized nation. If the United States is to have any hope of selling crypto-capable systems outside its own borders, it will have to accept the national sovereignty of the countries with which it trades.

There may be more hope of controlling the use of cryptography within a national population, but even here it seems difficult to achieve any worthwhile result. If cryptography is regulated by law, most businesses and most citizens will comply and will thereby be deprived of some of their ability to protect their privacy. Anyone who is engaged in serious criminal activity and who believes that cryptography would further that activity is unlikely to be deterred from using home-grown or underground products. One class of criminals in particular, state-sponsored terrorists, can be expected to be able to turn to foreign supporters for cryptographic support.

The availability of cryptography for criminal uses may not turn out to matter all that much. Cryptography is a tool well suited to legitimate activities of people who can openly say "I have secrets and I have a right to keep them private." It is not well suited to an activity that will be unable to defend itself if discovered and is trying to remain invisible. Criminals today make far more use of covert means of communication (most notably cloned cell phones) rather than of overtly secure means. Expanding bandwidth offers plenty of opportunity for covert communication (Anderson 1996b), and, this, rather than cryptography, will probably prove to be the major communications-related concern of police in the future.

Whatever the truth of the arguments, government efforts to keep honest citizens from using cryptography to protect their privacy continue. Such efforts are unlikely to achieve what governments claim to want, but very likely to cause serious damage to both business and democracy in the process.