1
Introduction

In the early nineteenth century it took six weeks for the British government to send a message from London to its representative in Delhi. In the late nineteenth century, the telegraph cut this time to days, then to hours. Today, at the dawn of the twenty-first century, the time has been cut to a fraction of a second and the service is available not just to the government but to most of the citizens. In a century and a half, we have gone from a world in which people separated by distance could communicate only through the slow process of sending letters to one in which they can communicate quickly, directly, and interactively—almost as though they were standing face to face. In the near future we may take the next step and move into a world in which computer-mediated interaction may offer such advantages over meeting face to face that it will supplant an even larger part of face-to-face interaction.

The result is that we now conduct more and more of our communications, whether personal, business, or civic, via electronic channels. The availability of telecommunication has transformed government, giving administrators real-time access to their employees and representatives in remote parts of the world. It has transformed commerce, facilitating worldwide enterprises and beginning the internationalization that became the byword of business a decade ago. It has transformed warfare, giving generals the ability to operate from the safety of rear areas and admirals the capacity to control fleets scattered across oceans. It has transformed personal relationships, allowing friends and family to converse with an immediacy that belies the fact they are thousands of miles apart.

These developments in technology have also had a profound impact on privacy. To attempt to function in modern society without employing telecommunication is to be eccentric. Most people use the telephone (including cellphones) daily, and many make constant use of electronic mail and the World Wide Web. These communications are by their essential nature interceptable. A typical telephone call travels over many miles of wire, of which only a few feet are under the control of the people talking. For most of its journey the signal is in the hands of one or more telephone companies, who will give it a reasonable degree of protection, but who can readily listen to it or record it and will from time to time do so. Many a call travels by radio for some part of its journey. The radio link may be at an end, in the form of a cordless, or cellular telephone, or it may be in the middle, in the form of a microwave link or a satellite hop. In either case, the call's vulnerability to interception is increased, and many people, using many kinds of radio equipment, will have the ability to listen in.

The vulnerability of long-distance communication is nothing new; remote communication has always been subject to interception. Couriers have been waylaid, seals have been broken, and letters have been read. But before the electronic era conversing in complete privacy required neither special equipment nor advanced planning. Walking a short distance away from other people and looking around to be sure that no one was hiding nearby was sufficient. Before tape recorders, parabolic microphones, and laser interferometers, it was not possible to intercept a conversation held out of sight and earshot of other people. No matter how much George III might have wanted to learn the contents of Hancock's private conversations with Adams, he had no hope of doing so unless he could induce one or the other to defect to the Crown.

Achieving comparable assurance of privacy in today's world—a world in which many of the most personal and sensitive conversations are carried on by people thousands of miles apart—requires both advanced planning and complex equipment. Most important, privacy in long-distance communication is not something the conversants can achieve on their own. A secure telephone is a complicated device combining a voice digitizer, cryptography, and a modem. Building one is as much beyond the abilities of most potential users as building a television set is beyond the

abilities of most viewers. In general, secure communication facilities are complex and require numerous people, many of whom must be trusted, for their construction and maintenance.

The vulnerability of telephone calls is the vulnerability of something that did not exist before the late 1800s. Unfortunately, holding a conversation face to face is not the guarantee of privacy it once was. The same electronic technologies that have made telecommunication possible have also given us a wide range of listening devices that make finding a private place to talk difficult indeed. Technology has changed the rules for the old game as well as for the new.

Telecommunication and to a lesser extent face-to-face communication suffer from another vulnerability that did not exist when the United States was founded: the possibility that one party to a conversation is recording it without the consent of the others. Before the development of sound recording, even one of the parties to a conversation had limited ability to reveal what had been said. Notes, an outline, or even a transcript would typically be only one person's word against another's. Audio and video recordings have changed the standards of evidence and opened the way for the repetition—sometimes to a very broad audience—of remarks that the utterer did not expect to be repeated.

The result is that privacy of conversation is no longer, as it was 200 years ago, a fact of life. It is now something over which society has a large and ever-increasing measure of control—a privilege that governments can grant or deny rather than a rule of nature over which they have no influence.

Society's response to these developments has been both to exploit them for various ends and to regulate them. It has tried to replace the fact of inviolably private communications with a "right to communicate privately." In the process, however, society has stopped short of creating an absolute right comparable to the reality of a former day. Society has placed controls on the use of technology to violate privacy by either the government or the citizens, but has also allowed it under many circumstances. Police employ wiretapping in criminal investigations, and intelligence agencies intercept foreign, and occasionally domestic, communications on a grand scale. Both regard their activities as a natural prerogative of the state, necessary for an orderly society. Many who are

not spies or police have a different perception of electronic surveillance. They see wiretapping not as a tool for law and order but as an instrument of the police state.

The ill ease that many people (including a number who were members of Congress at the time the federal wiretapping law was passed) feel when contemplating police use of wiretaps is rooted in awareness of the abuses to which wiretapping can be put. Unlike a search, the fact of whose occurrence is usually obvious, a wiretap is intrusive precisely because its invisibility to its victim undermines accountability. Totalitarian regimes have given us abundant evidence that the use of wiretaps and even the fear of their use can stifle free speech. Nor is the political use of electronic surveillance a particularly remote problem—the Watergate scandal is only the most recent example in contemporary American history of its use by the party in power in its attempts to stay in power.[1]

The fundamental similarity between the government's power to intercept communications and its ability to search physical premises has long been recognized. The Fourth Amendment to the US Constitution takes this ability for granted and places controls on the government's power of search. Similar controls have subsequently been placed by law on the use of wiretaps. There is, however, no suggestion in the Fourth Amendment of a guarantee that government searchers will find what they seek. Just as people have always been free to protect the things they consider private by hiding them or storing them with friends, they have been free to protect their conversations from being overheard.

Today, a new development in communication technology promises —or threatens, depending on your point of view—to restore some of the privacy lost to earlier technical advances. This development is electronic cryptography, a collection of practical and inexpensive techniques for encoding communications so that they can be understood only by their intended recipients. Modern cryptography also serves to provide anonymity to certain transactions.

Technology rarely exists in a vacuum, however. The rise of cryptography has been accompanied, and often driven, by a host of other phenomena.

Ease of communication, electronic as well as physical, has ushered in an era of international markets and multinational corporations. Today's

business is characterized by an unprecedented freedom of movement for both people and goods. More than one-fourth of the gross national product of the United States, for example, comes from either foreign trade or return on foreign investment (Dam and Lin 1996, p. 28). When foreign sales rival or exceed domestic ones, corporations open new divisions in proximity to markets, materials, or labor.

Security of electronic communication is as essential in this environment as security of transportation and storage have been to businesses throughout history. The communication system must ensure that orders for goods and services are genuine, guarantee that payments are credited to the proper accounts, and protect the privacy of business plans and personal information. These needs are all the more pressing today because, as governments have come to view the economic battlefield as an extension of the military one, industry has become a direct target of foreign espionage (Dam and Lin 1996, p. 33; Schweizer 1993, pp. 15–20; Williams 1992).

The rising importance of intellectual property has expanded the role of electronic communications in business. The communication systems with which we have been familiar all our lives—the telephone and the mail on one hand, ships, trains, trucks, and airplanes on the other—serve quite different sorts of business needs. The business function of the former has lain primarily in negotiation of commercial transactions, that of the latter in delivery of goods and services.[2] Today these distinctions are blurring. A larger and larger fraction of our commerce is commerce in information, so delivery of goods and services by electronic media is becoming more and more common. To support this delivery, the media themselves are becoming more unified. These phenomena are commonly referred to as the development of a "Global Information Infrastructure."

Both the negotiation and the delivery aspects of commercial communications have long required security. In the pre-electronic world, the validity of letters was established by seals, letterheads, and signatures; that of negotiators was established by personal recognition or letters of reference. Goods were typically protected by less subtle mechanisms. In past centuries, merchant ships carried cannon, and port cities were fortified. Today, warehouses are locked, airports are guarded, and roads are patrolled.

The growth of an information economy merges the channels used for business negotiation with those used to deliver goods and services. Much of what is now bought and sold is information, such as computer programs and knowledge about consumers' buying habits. The security of information has become an end in itself rather than just a means for ensuring the security of people and property.

In parallel with the growth of a commerce in information, there is a development that makes security harder to achieve: the rising demand for mobility in communication. Traveling executives sit down at workstations they have never seen before and expect the same environment that is on the desks in their offices. They carry cellular telephones and communicate constantly by radio. They haul out laptop computers and connect to the Internet from locations around the globe. With each such action they expose their information to threats of eavesdropping and falsification barely known until the 1990s. It is the lack of security for these increasingly common activities that we encounter when we hear that most cellular telephone calls in major metropolitan areas are overheard or even recorded by eavesdroppers with scanners, that a new virus is destroying data on the disks of personal computers, or that industrial spies have broken into a database half a world away.

The growing awareness of security, particularly in regard to Internet communications, has given rise to an explosion in the market for cryptography and in the development of products to satisfy that market. Software examples include Lotus Notes, the Netscape browser, and the seamless encryption interface in the popular Skype VoIP service. Hardware encryption is used in satellite TV decoders, in automatic teller machines, in point-of-sale terminals, and in smart cards. One researcher estimates that the commercial market for cryptography—still in its infancy—has already outstripped the military market.[3]

Cryptography's good fortune has not been to everybody's liking. Its detractors see its potential use by criminals, terrorists, and unfriendly foreign countries as outweighing its benefits to commerce and privacy. Two groups in particular have emerged in opposition to the easy availability of strong cryptography: the national-security community and the law-enforcement community.

The Allies' ability to understand German and Japanese communica-

tions, even when they were encoded with the enemies' best cryptographic systems, is widely seen as having been crucial to the course of World War II. Since that time, the practice of communications intelligence has grown steadily. Today it accounts for one of the largest slices of the US intelligence budget.[4]

The availability of wiretaps—legal or otherwise—for more than a lifetime has given us generations of police who cannot imagine a world without them. Confronted with even the suggestion of losing this tool, they respond in the same way one would expect of a modern doctor faced with the prospect of returning to a world without MRIs, CT scans, blood panels, and the numerous other diagnostic tests that characterize modern medicine.

The US government's initial response was a series of programs designed to maintain its eavesdropping capabilities. The centerpiece of those efforts, initially called *key escrow* and later *key recovery*, is a scheme that provides the users of cryptographic equipment with protection against most intruders but guarantees that the government is always in possession of a set of "spare keys" with which it can read the communications if it wishes. The effect is very much like that of the little keyhole in the back of the combination locks used on the lockers of schoolchildren. The children open the locks with the combinations, which is supposed to keep the other children out, but the teachers can always look in the lockers by using the key.

The first of these "spare keys" was the Clipper program, which made the term Clipper virtually synonymous with key escrow. The program was made public on Friday, April 16, 1993, on the front page of the *New York Times* and in press releases from the White House and other organizations. The proposal was to adopt a new federal standard for protecting communications. It called for the use of a cryptographic system embodying a "back door" that would allow the government to decrypt messages for law-enforcement and national-security purposes. Subsequently adopted over virtually unanimous opposition, the "Escrowed Encryption Standard" did not prove popular; most of the equipment implementing it was bought by the government in an unsuccessful attempt to seed the market.

Business objected to the Clipper scheme on every possible ground. First

of all, its workings were secret. This meant that the algorithm had to be implemented in tamper-resistant hardware, which was unappealing not only to the software industry but also to hardware manufacturers. Because of the secrecy and the tamper resistance, the Clipper chip's functions could not readily be integrated into other chips. And the scheme entailed the cost of adding a chip to each product—typically several times the cost of the chip itself.

Perhaps most important was the fact that Clipper's back door was accessible to the US government and only to the US government. This made it unlikely that Clipper products would appeal to foreign customers and undercut one of its major selling points. The Clipper chip, unlike most cryptographic equipment, was supposed to be exportable.

The White House saw the objections, which came from almost every quarter, as falling into two classes: those concerned with privacy and civil liberties and those concerned with business. In subsequent proposals, it attempted to address the business objections while flatly rejecting the civil-liberties position and maintaining the view that the government has the right not only to intercept citizens' communications but also to ensure that it will be able to understand the intercepted material. In all these proposals the executive branch attempted to use export controls—the only significant controls it had over cryptography under US law—to pressure industry to accommodate its desires.

The explosion in cryptography and the US government's attempts to control it gave rise to a debate between those who hail the new technology's contribution to privacy, business, and security and those who fear both its interference with the work of police and its adverse effect on the collection of intelligence. Positions have often been extreme. The advocates of unfettered cryptography maintain that a free society depends on privacy to protect freedom of association, artistic creativity, and political discussion. The advocates of control hold that there will be no freedom at all unless we can protect ourselves from criminals, terrorists, and foreign threats. Many have tried to present themselves as seeking to maintain or restore the status quo. For the police, the status quo is the continued ability to wiretap. For civil libertarians, it is the ready availability of conversational privacy that prevailed at the time of the country's founding. The fact that if cryptography has the potential to interfere with police

investigations it also has the potential to prevent crimes and thus make society more secure was often overlooked.

At the turn of the century, the argument seemed to have been won by the civil-liberties and business interests. Export controls were relaxed and revised, moving their focus away from the strength of security systems and toward a regime that preferred allowed commercial sales while restricting government ones. The new regime encouraged uniform *retail* offerings while discouraging customized products that could accommodate the needs of organizations that already had an installed base of cryptographic equipment.

The argument was won, in no small part, because the national-security establishment decided that the widespread use of strong encryption, difficult though it make certain aspects of intelligence, was, in the end, ultimately in the nation's interest.

The attempt to push key escrow was quietly dropped. Skipjack, the secret cryptographic algorithm underlying the Escrowed Encryption Standard, was declassified. More significantly, the aging Data Encryption Standard was replaced not with Skipjack but with a new algorithm of seemingly unbounded security.

Sober minds knew that the victory could not be so complete as it appeared. Police and intelligence agencies had begun to realize that their eavesdropping problem was not so much one of overcoming the protection of communications as of acquiring the data in the first place. The exploding diversity of communications technologies as well as the explosion in the volume of communications had the interceptors running to keep up. The interceptors' response was to offload the difficulty onto the communications carriers by applying a law adopted in the early 1990s to areas beyond those originally intended. These moves have reinvigorated—and fundamentally changed—the privacy-versus-intelligence argument, moving it, at least for the moment, away from cryptography and toward the expansion of interception technology. Should current law-enforcement efforts be successful, however, the issue of restrictions on the use of cryptography is sure to recur.

Had telecommunication merely given us a new option, the fact that the new medium lacked privacy would be at most regrettable—similar, perhaps, to the fact that telecommunication cannot provide physi-

cal contact, either friendly or hostile.[5] The problem arises from the fact that telecommunication has transformed society. It has made possible long-distance relationships between people who rarely or never meet in person. Without secure telecommunication, these people are effectively denied the possibility of private conversation.

The issues are not cut and dried, and no amount of calling a tail a leg will make telecommunication equivalent to face-to-face communication. Any attempt to force such an equivalence and establish an absolute right of private conversation is doomed to failure. The interceptability of communications is as much a fact of life in the electronic era as the inviolability of private conversation was in the pre-electronic. On the other hand, if we deny the fact that telecommunication, whatever its new properties, is rooted in face-to-face conversation and shares much of its social function, we will doom ourselves to a world in which truly private conversation is a rarity—a perquisite belonging exclusively to the well-traveled rich.

Ultimately, to make good policy we must consider the sort of world in which we want to live and what effects our actions will, indeed can, have in bringing about such a world. Such consideration depends on awareness of many factors, including the technology of cryptography and electronic surveillance, the aims and practices of intelligence and law enforcement, and the history of society's attempts to deal with similar problems over more than a century.