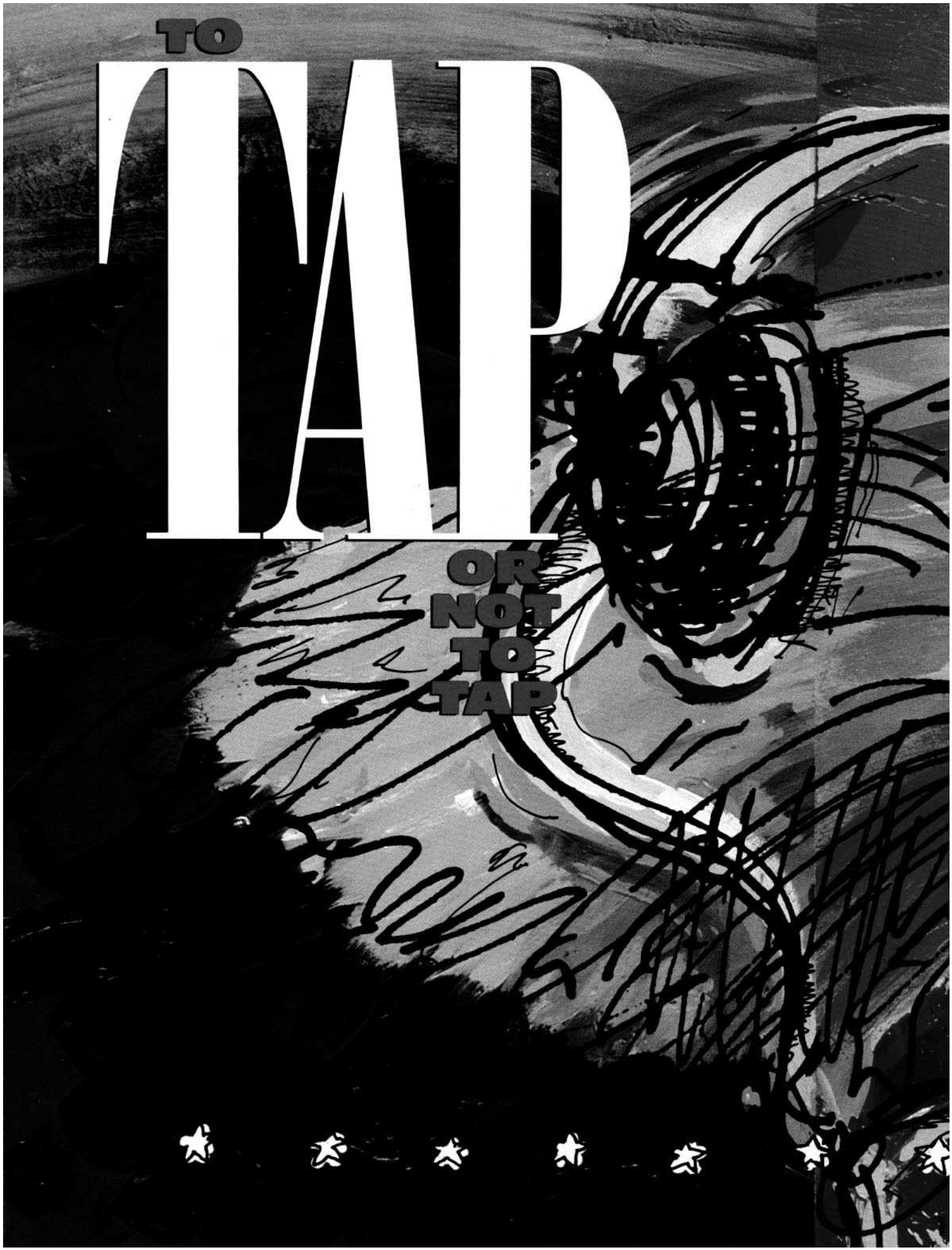
TO
TAP
OR
NOT
TO
TAP

It used to be when the FBI wanted to eavesdrop on suspected criminals they could employ a trusty alligator clip to the appropriate phone line and listen in for incriminating evidence.

Those days are (almost) over.

Advances in telephone technology, particularly digital and fiber optic transmissions, are fast making traditional wiretapping procedures obsolete. New high-capacity lines pack hundreds of conversations in bit streams. Finding that suspicious conversation among the maze takes an expert hand. Indeed, it's reached the point where law enforcement agencies are looking for help.

Last fall the Justice Department proposed legislation that would require U.S. phone companies to give law enforcement officials technical assistance in authorized wiretapping procedures. Moreover, it calls for industry to start designing products with tapability built in.

Not surprisingly, this proposal has ignited fevered debates over protection versus privacy. The FBI says it simply seeks to maintain the tapping power authorized over 25 years ago in federal law. Privacy proponents, however, say giving the government access to untold numbers of innocent conversations will pose a myriad of problems and concerns.

The following editorial debate examines the many sensitive issues involved in this pending legislation. Dorothy Denning presents the case for the proposed digital telephony plan, exploring the technical possibilities and urging trust in governmental usage. Her article is followed by a collection of comments from noted representatives of industry, government and law who argue points of privacy, competitiveness and technological abuse. This debate concludes with a rejoinder by Denning. ■

DOROTHY E. DENNING

Under current U.S. law, the government is authorized to intercept the wire, electronic, or oral communications of a criminal subject by obtaining a special court order which has been designed by Congress and approved by the Supreme Court. When served with a court order, service providers and operators are obligated under statute to assist in the execution of a court-authorized tap or microphone installation. To obtain this order, Congress and the Supreme Court have specified that law enforcement must demonstrate there is probable cause to believe the subject under investigation is committing some specific, serious felony and communications concerning the offense will be obtained through the intercepts. Before issuing a court order, a judge must review a lengthy affidavit that sets forth all the evidence and agree with the assertions contained therein. The affidavit must also demonstrate other investigative techniques have been tried without success, or won't work, or would be too dangerous. In the decade from 1982 to 1991, state and federal agencies conducted 7,467 taps, leading to 19,259 convictions so far. Convictions resulting from interceptions conducted in the last few years are still accumulating, as trials regarding those subjects are held.

The ability of law enforcement to draw on this investigative tool is now at risk. Methods that have been used to intercept analogue voice communications carried over copper wires do not work with many of the new digital-based technologies and services such as ISDN (Integrated Services Digital Network), fiber optic transmissions, and the increasing number of mobile telecommunication networks and architectures. Although it is technically feasible to intercept digital communications, not all systems have been designed or equipped to meet the intercept requirements of law enforcement. According to the FBI, numerous court orders have not been sought, executed, or fully carried out because of technological problems. To address these problems, the Department of Justice is seeking digital telephony legislation to require the service providers and operators to meet their statutory assistance requirements by maintaining the capability to intercept particular communications, permitting law enforcement to perform its monitoring function at a remote government monitoring facility in real time.

The proposed legislation has stimulated a lively debate. Much of the debate has focused on concerns that the proposal, if enacted, could hold back technology, jeopardize security and privacy, make U.S. products noncompetitive, burden the country with unjustifiable and unnecessary costs, and ultimately fail to meet the stated objectives if criminals encrypt their communications.

This article presents the case for the proposed digital telephony legislation and responds to the preceding concerns. Although the digital telephony proposal does not address encryption, the possibility of regulating cryptography will be discussed following the section on the proposed legislation.

The Digital Telephony Proposal

To ensure law enforcement's continued ability to conduct court-authorized taps, the administration, at the request of the Department of Justice and the FBI, proposed digital telephony legislation [11]. The version submitted to Congress in September 1992 would require providers of electronic communications services and private branch exchange (PBX) operators to ensure that the government's ability to lawfully intercept communications is not curtailed or prevented entirely by the introduction of advanced technology. Service providers would be responsible for providing the government, in real time, the communication signals of the individual(s) named in a court

order so the signals could be transferred to a remote government monitoring facility, without detection by the subject, and without degradation of service. Providers of services within the public switched network would be given 18 months to comply and PBX operators three years. The Attorney General would have the authority to grant exceptions and waivers and seek civil penalties and injunctive relief to enforce the provisions. A fine of up to $10,000 a day could be levied for noncompliance. Government systems would be exempt on the grounds that law enforcement has the necessary cooperation to access the premises. The proposal is strongly supported as a critical public safety measure by state and local law enforcement (who conduct the majority of wiretaps), the National Association of Attorney Generals, the National Association of District Attorneys, and numerous law enforcement associations.

Although the proposed legislation does not expand the authority of the government to lawfully acquire the contents of communications, it arguably places greater constraints and demands on service providers and operators. The current law (Title 18, U.S. Code, Section 2518(4)) states that service providers are required to furnish the responsible law enforcement official with all information, facilities, and technical assistance necessary to perform the intercept unobtrusively and with a minimum of interference. It does not say explicitly that providers must build and use systems that ensure timely interception is possible. This is not surprising, since the emerging technological advances and attendant difficulties would not have been anticipated in 1968 when the legislation was enacted, but it leaves open to interpretation the meaning of the word "assist" and the exact requirements placed on service providers and operators in today's digital world.

When the FBI first encountered the intercept problems, they attempted to educate the telecommunications industry concerning the problems. They sought voluntary cooperation and a commitment to address the problems. But after meeting with industry officials for more than two years, they concluded that industry was not committed to resolving the problems without a mandate and that legislation was necessary to clarify the responsibilities of service providers and operators, to ensure that all providers and operators comply, and to provide a mechanism whereby industry could justify the development costs. Legislation would ensure all service providers remain on the same competitive "level playing field."

The proposed digital telephony legislation was not introduced in the last (1992) session of Congress because time ran out. Meanwhile, the FBI is continuing its discussions with industry through two technical committees, one with representatives from the telecommunications industry, the other with representatives from the computer industry, and many companies are working hard to meet law enforcement's needs.

The following sections address major concerns that have been expressed by some computer scientists, civil libertarians, and people in the telecommunications industry. Many of these concerns are articulated in a white paper [2] issued by the Electronic Frontier Foundation (EFF) on behalf of an *ad hoc* coalition of representatives from industry and public interest groups, including AT&T, IBM, and ACLU.

Technology Advancement

Concern 1: *The proposal would hold back technology and stymie innovation.* Some people are concerned that requiring technology modifications to support taps would prevent full use of new technologies. Janlori Goldman of the ACLU has called this a "dumbing down" and stated that "if the government wants to engage in surveillance, it must bear the burden of keeping pace with new developments" [3].

I see no technological reason why any of the new technologies, including digital technologies, cannot support an intercept capability. In many cases the intercept capability would likely parallel or draw on the maintenance and security features used by the telephone companies to ensure their systems are functioning properly and are not abused. At the very least, the intercept capability can be programmed into the switches where the bit stream for a connection must be isolated anyway so that it can be routed to its correct destination (for interception, a duplicate copy of the bit stream can be routed to a remote government monitoring facility). But whereas this modification would be relatively straightforward for the service providers to make, it would be impossible for the government to do on its own since it lacks access to the switches. Also, because of the complexities of switches and switch software, the government has no desire to engage in self help and interject itself into the arena of networks or central office switching and thereby perhaps inadvertently disrupt service on a widespread basis.

Another reason for not asking the government to implement its own surveillance mechanisms is that the providers can do so surgically, and hence less intrusively. For example, where ISDN or bundled fiber optic transmissions are involved, service providers can isolate an individual communications channel, whereas the government might have to intercept everything traveling over a line or link supporting simultaneous transmission of multiple, commingled communications in order to extract the desired channel. The FBI has stated that law enforcement does not want access to the communications of anyone outside the ambit of the court order.

In short, the digital telephony proposal would not require the communications industry to "dumb down" technology. Rather, it would require industry to use technology to make networks *smarter.*

Security and Privacy

Concern 2: *Providing an intercept capability would jeopardize security and privacy, first because the remote monitoring capability would make the systems vulnerable to attack, and second because the intercept capability itself would introduce a new vulnerability into the systems.*

The first part of this concern relating to the remote monitoring capability

seems to have arisen from a misinterpretation of the requirement for remote monitoring. Sec. 2. (1) of the proposed bill states that "Providers of electronic communication services and private branch exchange operators shall provide . . . the capacity for the government to intercept wire and electronic communications when authorized by law: . . . (4) at a government monitoring facility remote from the target facility and remote from the system of the electronic communication services provider or private branch exchange operator." Some people have mistakenly interpreted this as a requirement for law enforcement to be able to electronically, and independently, enter a computer switch from a remote location to initiate a tap. If this were the case, then an unauthorized person might be able to come in through the connection and tap into a line.

The FBI has made it clear they are not asking for the capability to initiate taps in this fashion, but rather for a tap initiated by the service provider to be routed to a predefined remote location over a leased line. In the specification of the requirements for the government monitoring facility, the proposal states: "Normally, the government leases a line from the electronic communication services provider's or private branch exchange operator's switch to another location owned or operated by the government. . . . The legislation does not establish any independent 'dial-up' authority by which criminal law enforcement agencies could effectuate interceptions without the affirmative assistance of the providers or operators. The providers and operators will continue to make the necessary interconnections or issue the necessary switch program instructions to effectuate an interception." Indeed, the requirement set forth in the legislation memorializes long-standing practice and procedure. Since the connection to a remote government monitoring facility would support an outgoing data stream only, it could not be used to break into a switch and, therefore, does not impose any new or additional danger to the security of the systems and the privacy of the people who rely on them for their communications.

This misinterpretation of the remote monitoring requirement also led to a concern that law enforcement would abuse the wiretapping capability and surreptitiously perform unauthorized taps. Because the only people who would have access to the systems for activating a tap would be employees of the service providers, who have been strict about requiring court orders, the possibility of law enforcement performing unauthorized taps seems even less likely than with present technology.

The second part of the concern, that the intercept capability itself could introduce a new vulnerability, is at least potentially more serious. If the intercept capability is programmed into the switches and an unauthorized person can break into a switch, then that person might be able to eavesdrop on a line or find out if a particular line is being tapped. Indeed, "hackers" have broken into poorly protected computer switches and eavesdropped on lines. But the switches can and must be designed and operated to prevent such break-ins independent of any intercept capabilities. Security is essential not only to protect against unlawful eavesdropping but to ensure reliable service and protect against other types of abuses. The administration, the Department of Justice, and the FBI all are strong advocates for security in telecommunications networks.

To protect against possible abuses by employees of the service providers, access to the software for activating an intercept should be minimized and well-protected through appropriate authentication mechanisms and access controls. The intercept control software might be left off the system and installed in an isolated partition only when needed prior to executing an authorized tap. With newer, advanced technology and proper overall security measures, it should be possible to provide greater protection against abuse than is presently provided.

Competitiveness

Concern 3: *Implementing the intercept requirements could harm the competitiveness of U.S. products in the global market.*

This concern, which arose in conjunction with the preceding concerns about holding back technology and security, is based on an assumption that it would take U.S. companies longer to bring their products to market, and other countries would not want to buy products that increased the vulnerability of their systems. However, because the products can be designed to operate with a high level of security and because other governments (many of which run or oversee their nation's telecommunications networks) might desire similar features in their telecommunications systems, the digital telephony proposal would be competition-neutral. In fact, several other countries have expressed an interest in obtaining such products. U.S. companies could have a competitive advantage if they take the lead now, and indeed might be at a disadvantage if they fail to act and companies outside the U.S. do. Under the proposed legislation, foreign communications companies would have to comply with the U.S. law and standards if they seek to provide service in the U.S., thereby preventing any unfair competition in this country.

Cost and Benefits

Concern 4: *The cost could be enormous and is not obviously justifiable by the perceived benefits.*

The cost of compliance is a major concern. The existing law states that service providers and operators shall be compensated for "expenses" incurred in assisting with a tap. The proposed law leaves open who would bear the capital expenses of modifications and engineering costs required to maintain the intercept capability.

The FBI, in consultation with industry, has estimated the cumulative costs for a switched-based software solution to be in the range $150 to $250 million, and the maximum development costs to be $300 million or approximately 1.5% of the telecommunications industry's yearly acquisition budget of $22 billion [11]. These costs, however, are highly speculative and actual costs could be

considerably lower if the service providers pursue a combination non-switch/switch-based solution. In addition, whatever the costs, they likely would be amortized over several years. Some people have suggested the government should pay the costs, but a privately funded approach is more likely to encourage market forces to bring forth the most cost-effective solutions. In either case, this is a societal cost that will be paid for one way or the other by the citizenry to ensure effective law enforcement and the public safety.

The benefits derived from the use of electronic surveillance are difficult to quantify. Because wiretapping has been used infrequently (less than 1,000 taps per year), some people have argued it is not essential—that crimes could be solved by other means that would be less costly. But by law, wiretapping can only be used when normal investigative procedures have been tried and have failed or when they appear unlikely to succeed or too dangerous. Also, according to the FBI, many serious crimes can *only* be solved or prevented by electronic surveillance.

According to the FBI, electronic surveillance has been essential in preventing serious and often violent criminal activities including organized crime, drug trafficking, extortion, terrorism, kidnapping, and murder. While the benefits to society of preventing such crimes and saving human lives are incalculable, the economic benefits alone are estimated to be billions of dollars per year [11]. During the period from 1985 to 1991, court-ordered electronic surveillance conducted just by the FBI led to 7,324 convictions, almost $300 million in fines being levied, over $750 million in recoveries, restitutions, and court-ordered forfeitures, and close to $2 billion in prevented potential economic loss. Since the FBI conducts fewer than one-third of all intercepts, the total benefits derived from electronic surveillance by all law enforcement agencies is considerably higher.

One area where electronic surveillance has played a major role is in combatting organized crime. In 1986, the President's Commission on Organized Crime estimated that organized crime reduces the output of the U.S. economy by $18.2 billion a year (1986 dollars), costs workers 414,000 jobs, raises consumer prices by 0.3%, and lowers per capita personal income by $77.22 (1986 dollars) [6]. Although the impact of law enforcement's successful investigations of organized crime on these losses has not been thoroughly studied, in 1988 David Williams of the Office of Special Investigations, General Accounting Office, testified before U.S. Senate hearings on organized crime that "Evidence gathered through electronic surveillance . . . has had a devastating impact on organized crime." According to the FBI, the hierarchy of organized crime has been neutralized or destabilized through the use of electronic surveillance, and 30 years of successes would be reversed if the ability to conduct court-authorized electronic surveillance was lost.

Almost two-thirds of all court orders for electronic surveillance are used to fight the war on drugs, and electronic surveillance has been critical in identifying and then dismantling major drug trafficking organizations. Although the benefits of these operations are difficult to quantify, their impact on the economy and people's lives is potentially enormous. In 1988, the Public Health Service estimated the health, labor, and crime costs of drug abuse at $58.3 billion [7]. The FBI estimates the war on drugs and its continuing legacy of violent street crime in the form of near daily drive-by murders would be substantially, if not totally, lost if law enforcement were to lose its capability for electronic surveillance.

Electronic surveillance has been used to investigate aggravated governmental fraud and corruption. A recent military-procurement fraud case ("Ill-Wind") involving persons in the Department of Defense and defense contractors has so far led to 59 convictions and nearly $250 million in fines, restitutions, and recoveries ordered.

The use of electronic surveillance has successfully prevented several terrorist attacks, including the bombing of a foreign consulate in the U.S., a rocket attack against a U.S. ally, and the acquisition of a surface-to-air missile that was to be used in an act that likely would have led to numerous deaths. By intercepting voice, fax, and communications on a local bulletin board system, the FBI prevented the proposed kidnapping and murder of a young child for the purpose of making a "snuff murder" film. Wiretapping also has been used to obtain evidence against hackers who broke into computer systems. This case illustrates how wiretapping, which is popularly regarded as an antiprivacy tool, actually helps protect the privacy and proprietary interests of law-abiding citizens by helping to convict those who violate those interests.

Aside from preventing and solving serious crime, wiretapping yields evidence that is considerably more reliable than that obtained by many other methods such as informants, and is less dangerous for law enforcement officials than breaking and entering to install bugs in homes or offices. It is critical in those situa-

I see no reason why any new technologies, including digital technologies, cannot support an intercept capability. In many cases this capability would likely draw on the maintenance and security features used by phone companies to ensure their systems are functioning properly and are not abused.

tions where the crime leaders are not present at the places where the illegal transactions take place, as is the case with major drug cartels directed by distant drug chieftains.

The societal and economic benefits of authorized electronic surveillance will increase as telecommunication services and facilities continue to expand and electronic commerce comes into widespread use, bringing with it more possibilities for fraud and other types of crimes.

Some people are troubled that citizens would have to pay for the wiretapping capability, possibly through their phone bills. In an open letter to several congressional committees, Joseph Truitt wrote: "What an insult—to be forced to pay for the privilege of being tapped!" [9] However, through tax revenues and telephone company security office budgets, law enforcement has always been able to carry out investigations and conduct electronic surveillance, and unless a person is the subject of a court order, that person will not be paying to be intercepted. As citizens, we have always paid for law enforcement, knowing fully well that it will be used against us if we ever engage in criminal activities. This is one of the costs of protecting society from people who do not respect the laws. One could equally say: "What an insult—to be forced to pay for the privilege of being arrested!"

Compliance

Concern 5: *It is unclear who must comply with the proposed legislation and what compliance means.*

The EFF expressed a concern that the proposal was overly broad, covering "just about everyone" including businesses, universities, and other organizations owning local and wide area networks; providers of electronic mail and information services such as Prodigy and Compuserve; operators of networks such as the Internet; and owners of computer bulletin boards [2]. They raised questions about the conditions under which exemptions might be granted and the requirements for compliance. An earlier report published by the General Accounting Office [10] also asked for greater clarity about what is meant by full compliance, for example, response time for executing a court order.

In response, the FBI points out the existing legislation already imposes an assistance obligation on electronic communication service providers that includes all of the foregoing named service entities, and that the reason the requirements are stated in generic terms is because historically these have sufficed and law enforcement's requirements, including those for a timely response, have been met. With respect to exemptions, the proposed legislation states that the attorney general may grant exemptions for whole classes of systems where no serious criminal activity is likely to take place, for example, hospital telephone systems, and grant waivers for providers and operators who cannot comply or need additional time. The FBI has also indicated that interceptions would normally be sought at a point close to the target, such that intranetwork interceptions would be very infrequent generally, and that information networks such as Compuserve and Prodigy would likely be considered for exemption. Although the proposed legislation allows for stiff fines, the legislative history background materials state that "this provision is not expected to be used."

Cryptography

It is now possible to purchase at reasonable cost a telephone security device that encrypts communications and to acquire software that encrypts data transmitted over computer networks. Even if law enforcement retains its capability to intercept communications, this capability ultimately could be diminished if criminals begin to hide their communications through encryption and law enforcement is unable to obtain access to the "plaintext" or unscrambled communications. If encryption becomes cheap and ubiquitous, this could pose a serious threat to effective law enforcement and hence to the public's safety.

The digital telephony proposal does not address encryption, leaving open the question of how best to deal with it. Currently, the use of cryptography in this country is unregulated, though export of the technology is regulated. Cryptography is regulated in some of the major European countries. This section explores the possibility of regulating cryptography use. For an introduction to cryptography and the methods referenced here, see [1].

Possible Approaches

In order to assess whether cryptography can or should be regulated, we need some idea of how it might be done. Our knowledge of available options is quite limited, however, since the possibility of regulating cryptography in the U.S. has thus far received little public discussion. The following three possibilities are offered as a starting point for discussion:

Weak Cryptography. This approach would require cryptographic systems to be sufficiently weak so that the government could break them, preferably in real time since timeliness is crucial for preventing many crimes such as murder and terrorist attacks. While weak cryptography would offer adequate protection against most eavesdropping when the conse-

By law, wiretapping can only be used when normal investigative procedures have failed or when they appear unlikely to succeed or are too dangerous. According to the FBI, many serious crimes can only be solved or prevented by electronic surveillance.

quences of disclosure are not particularly damaging, it could be unacceptable in many contexts such as protecting corporate communications that are seriously threatened by industrial espionage.

However, it is worth noting the general migration from analog to digital communications *itself* provides a high level of protection in the area of telecommunications, since such communications are only understandable with the aid of very sophisticated technology unlike the relative ease with which eavesdroppers can understand analog intercepts. Thus, it is not obvious that most individuals and organizations would either need or demand strong encryption, especially since most do not use any form of encryption at present. However, since history shows that methods which are secure today may be blown apart tomorrow, this may not be a dependable long-term solution.

Escrowed Private Keys. Ron Rivest has proposed using high-security encryption with "escrowed secret keys" [8]. Each user would be required to register his or her secret key with an independent trustee, and cryptographic products would be designed to operate only with keys that are certified as being properly escrowed. The trustee could be some neutral entity such as the U.S. Postal Service, a bank, or the clerks of the federal courts. It would be extremely difficult to subvert the system since someone would need the cooperation of the telecommunications provider (to get the communication stream) and the trustee (to get the key), both of which would require a court order.

Additional protection can be obtained by distributing the power of the trustee. For example, two trustees could be used, and the keys could be stored with the first trustee encrypted under a key known only to the second. Alternatively, using Silvio Micali's "fair public-key cryptography," each user's private key could be split into, say, five pieces, and each piece given to a different trustee [4]. The splitting is done in such a way that all five pieces are required to reconstruct the original key, but each one can be independently verified, and the set of five can be verified as a whole without putting them all together.

In order to implement an approach based on escrowed keys, methods would be needed for registering and changing keys that belong to individuals and organizations and for gaining access to the transient "session keys" that are used to encrypt actual communications. Key registration might be incorporated into the sale and licensing of cryptographic products. To facilitate law enforcement's access to session keys, the protocols used to distribute or negotiate session keys during the start of a communications could be standardized. Once law enforcement has acquired the private keys on a given line, they would then be able to acquire the session keys by intercepting the key initialization protocol.

One drawback to this approach is the overhead and bureaucracy associated with key registration. Another is that it is limited to cryptographic systems that require more-or-less permanent private keys. Although some such as the RSA public-key cryptosystem fit this description, others do not.

Direct Access to Session Keys. Ultimately a session key is needed to decrypt a communications stream, and this approach would give the service provider direct access to the session key when an intercept has been established in response to a court order. The service provider can then make the session key available to law enforcement along with the communications stream.

One way of making the session key available to the provider is for the provider to participate in the protocol used to set up the key. For example, the following three-way extension of the Diffie-Hellman public-key distribution protocol could be used to establish a session key that would be known only to the two communicants and the service provider: Each party independently generates a random exponent x and computes $y = g^x \bmod p$ for a given g and prime p. All three parties then pass their value of y to the right (imagine they are in a circle). Next, using the received value of y, they compute $z = y^x \bmod p$ and pass it to the right. Finally, using the received value of z, they compute the shared session key $k = z^x \bmod p$, which will be the value g raised to all three exponents. An eavesdropper, who sees only the values of y and z, cannot compute k because he or she will lack the requisite exponent.

If a court order has been issued and an intercept activated, the component or module operating on behalf of the service provider would pass the key on to the remote government monitoring facility before destroying it. Obviously, this component would have to be designed with great care in order to ensure that keys are not improperly disclosed and they are immediately destroyed when no intercept has been activated.

This approach has the advantage over the preceding ones of allowing the use of a strong cryptosystem while not requiring the use and registration of permanent keys. It has the disadvantage of requiring the service provider to be brought into the loop during the key negotiation protocol, which might also be difficult or costly to implement.

The cost of regulating the use of cryptography following either of these last two approaches is unknown. A feasibility study would be needed to examine the requirements in greater detail and estimate the costs.

Protecting Privacy and Proprietary Interests

The last two approaches suggest that it is possible to regulate cryptography without compromising the privacy and proprietary interests of the citizens. Some people have argued, however, that the citizens have a right to *absolute* communications secrecy from everyone, including the government, under all circumstances, and that requiring people to make the plaintext of their encrypted communications available to the government directly or indirectly would be tantamount to forbidding them from having a private conversation in a secret place or using an obscure foreign language, or making them

carry a microphone. These absolutist positions, however, contort the concept of privacy and do not represent valid analogies.

Our laws, as embodied in the Constitution and Bill of Rights, common law, tort law, and legislation, reflect a *social contract* that strikes a balance between our rights to privacy and to an orderly society. This contract does not grant us absolute privacy in all areas. For example, whereas we are protected against *unreasonable* searches and seizures by the Fourth Amendment, we are not immune from searches and seizures when there is probable cause we have committed a crime and a judge has issued a warrant. When Congress enacted wiretapping legislation and the Supreme Court ruled that wiretapping with a warrant was permitted, law enforcement was empowered to intercept communications, whether they were encrypted or not. Now that encryption is becoming an issue, it would seem appropriate for Congress to set an encryption policy.

Viewed narrowly, cryptography offers the possibility for absolute communications protection or privacy that is not available to us in any other area of our lives. Our physical beings are constantly at risk, and our premises, cars, safes, and lockers can be illegally broken into or lawfully searched. We live with this risk and indeed benefit from it whenever we lock ourselves out of our homes, cars, and so forth. It is unclear that we need an absolute level of protection or privacy for our communications surpassing the levels in other areas of our lives. Indeed, our speech in many regards and areas is already subject to balanced regulation (e.g., slander, libel, obscenity, falsely yelling "fire" in a theater).

Although illegal eavesdropping poses a threat to corporate security, the communications network is not the weak link. Employees and former employees have posed a bigger threat. If companies themselves do not regulate cryptography, their employees would have a means of transmitting company secrets outside the company with impunity and without detection. The military-procurement fraud case mentioned earlier was solved only because law enforcement was able to tap the communications of a Pentagon employee. Thus, corporate security is not necessarily best served by an encryption system that offers absolute secrecy to its employees.

Competitiveness

Some people have argued that regulating cryptography in this country would harm the competitiveness of U.S. products overseas. No other country would want to buy products based on weak encryption algorithms or with built-in mechanisms for registering private keys or making session keys available to the service providers.

As with the basic intercept capability issue, it is not only conceivable but likely that other countries will be interested in products that allow their governments to decrypt communications when authorized by law. Foreign governments, for example, would be loathe to see terrorists operate and communicate in their country with impunity behind the shield of absolutely secure cryptographic devices. U.S. companies could take the lead in developing products that meet the security needs of customers and the legitimate needs of law enforcement and governments abroad.

Enforcing Cryptography Regulation

Many people have voiced a concern that criminals would violate cryptography regulations and use cryptosystems that the government could not decrypt, thereby also obtaining an absolute privacy beyond that of law-abiding citizens. This is typically expressed as "if encryption is outlawed, only outlaws will have encryption." Because products are being designed, sold, and given away in the absence of any regulation, this outcome is indeed possible.

Cryptography can be embedded in a device such as a secure phone or security device attached to a standard phone that encrypts communications transmitted between phones (or fax machines), or it can be embedded in software packages or modules that run on computers and encrypt the communications transmitted over computer networks. It seems easier to regulate and control telephone encryption devices than software. For example, if an approach based on escrowed keys is adopted, then the keys embedded in the products could be given to one or more trustees at the time of sale, and the products could be designed so the keys could not be changed without bringing the product in for service or negotiating a new key with a trustee online. Similarly, if an approach based on direct access to session keys is adopted, a suitable key negotiation protocol could be built into the products. Although criminals could develop their own noncompliant products, it is likely that most criminals would use commercial off-the-shelf products rather than developing their own.

Software encryption, performed on personal computers or servers, could be much more difficult to regulate, especially since strong cryptographic methods have been distributed through networks such as the Internet and cryptographic algorithms can be implemented by any competent programmer. But enforcing cryptography regulations on software may be less critical for law enforcement since electronic surveillance has typically focused on telephone calls or conversations. Thus, it would be a mistake to make the difficulty of controlling software encryption an excuse for not regulating cryptography.

Although it would be practically impossible to prevent the use of noncompliant products, the work factor required to acquire and use these products may be sufficiently high to deter their use. But even if they are used, if there is probable cause that a person is involved with some serious crime and a warrant is issued for that person's communications, then legislation could also provide grounds for arresting that person if he or she violated the laws governing cryptography as a separate offense. However, it would be important to not lose sight of the purpose of cryptography regulation and to not expend resources enforcing it for its own sake.

If private encryption is allowed to proceed without some reasonable

accommodation, it will logically lead to situations in which someone is arrested outright when probable cause for a criminal act is demonstrated. This could lead to premature cessation of investigations where critical evidence would not be obtained.

Conclusions

Granger Morgan has observed that controversy over the proposed digital telephony legislation is symbolic of a broader set of conflicts arising from several competing national interests: individual privacy, security for organizations, effective domestic law enforcement, effective international intelligence-gathering, and secure worldwide reliable communications [5]. Because the balance among these becomes hardwired into the design of our telecommunications system, it is difficult to adjust the balance in response to changing world conditions and changing values. Technology has been drifting in a direction that could shift the balance away from effective law enforcement and intelligence-gathering toward absolute individual privacy and corporate security. Since the consequences of doing so would pose a serious threat to society, I am not content to let this happen without careful consideration and public discussion.

With respect to wiretapping, we can take the steps necessary to ensure law enforcement's continued ability to intercept and interpret electronic communications when authorized by court order, or let this capability gradually fade away as new technologies are deployed and cryptographic products become widely available. The consequence of this choice will affect our personal safety, our right to live in a society where lawlessness is not tolerated, and the ability of law enforcement to prevent serious and often violent criminal activity.

While the societal and economic benefits that would come from the proposed digital telephony legislation are difficult to quantify, the economic benefits of maintaining effective law enforcement through its capability of conducting authorized intercepts are estimated to be in the billions and many lives would likely be saved. These benefits are likely to increase with the growth in telecommunications. By comparison, the cumulative costs of complying with the proposed digital telephony legislation are roughly estimated to be in the range of $150 to $250 million. Although the benefits might not be fully realized if the intercept capability would, as has been suggested, thwart technological progress, compromise security and privacy, or harm competitiveness, these are unlikely outcomes as discussed in this article. Indeed, effective law enforcement is crucial for protecting the privacy of law-abiding citizens and the business interests of companies.

If we fail to enact legislation that will ensure a continued capability for court-ordered electronic surveillance, we cannot be guaranteed that all service providers will provide this capability voluntarily. Systems fielded without an adequate provision for court-ordered intercepts would become sanctuaries for criminality wherein organized crime leaders, drug dealers, terrorists, and other criminals could conspire and act with impunity. Eventually, we could find ourselves with an increase in major crimes against society, a greatly diminished capacity to fight them, and no timely solution.

Less is known about the implications of regulating cryptography since no specific legislative or other proposal has been seriously considered. Although government regulation of cryptography may be somewhat cumbersome and subject to evasion, we should give it full consideration. Regulated encryption would provide considerably greater security and privacy than no encryption, which has been the norm for most personal and corporate communications. We must balance our competing interests in a way that ensures effective law enforcement and intelligence gathering, while protecting individual privacy and corporate security.

Acknowledgements

I am deeply grateful to the following people for providing constructive comments on earlier versions of this article, for helpful discussions, and for their willingness to debate those points with which they disagreed: William A. Bayse, Kier Boyd, Julia Dederer, Peter Denning, Jack Edwards, Carl Ellison, Mike Godwin, Lance Hoffman, Phil Karn, Bruce Koball, Steve Lipner, Alan McDonald, Donn Parker, Ron Rivest, Marc Rotenberg, Jeff Smith, James Sylvester, and Willis Ware. ■

References

1. Denning, D.E. *Cryptography and Data Security.* Addison-Wesley, Reading, Mass., 1982.
2. Electronic Frontier Foundations. Analysis of the FBI proposal regarding digital telephony. Sept. 17, 1992.
3. Goldman, J. Why cater to luddites. *Wash. Times* (May 24, 1992).
4. Micali, S. Fair public-key cryptosystems. Lab. for Computer Sci., MIT, Aug. 21, 1992.
5. Morgan, M.G. Viewpoint, *The Institute* (IEEE, Nov. 1992).
6. President's Commission on Organized Crime. The Impact: Organized Crime Today. 1986.
7. Rice, D. et al. The economic cost of alcohol and drug abuse and mental illness: 1985. U.S. Dept. of Health and Human Services, Table 1, p. 2, 1990.
8. Rivest, R.L. Response to NIST's proposal, *Commun. ACM*, 35, 7, (July 1992), 41–47.
9. Truitt, J. Open letter of Sept. 17, 1992 to Congress protesting proposed FBI digital telephony bill. *Comput. Priv. Digest 1*, 081 (Sept. 23, 1992).
10. United States General Accounting Office. FBI Advanced Communications Technologies Pose Wiretapping Challenges. Briefing report to the chairman, Subcommittee on Telecommunications and Finance, Committee on Energy and Commerce, House of Representatives, GAO/IMTEC-92-68BR, July 1992.
11. United States Department of Justice, Federal Bureau of Investigation. Digital Telephony. 1992.

DOROTHY DENNING is professor and chair of computer science at Georgetown University. She is the author of *Cryptography and Data Security.*

Author's Present Address: Georgetown University, Computer Science Department, 225 Reiss Science Building, Washington, D.C. 20057. Denning@cs.georgetown.edu.