FINAL THOUGHTS

Dorothy Denning

With an issue as important as wiretapping, it is important we base our actions and decisions on well-grounded assessments rather than opinions, myths, fallacies, and misunderstandings. In what follows, I will challenge the ungrounded assessments and address concerns not covered in my opening statement such as the possibility of government abuse. I will limit my remarks to the wiretapping issues.

The very concept of wiretapping conjures up dystopian images of *1984* and Big Brother, blinding us to the current realities about electronic surveillance. It is common to hear statements such as made by Ron Rivest that many people feel it is better to let a few criminals get away than to put a comprehensive electronic surveillance technology in the hands of the government. Similarly, it is not surprising Marc Rotenberg was able to cite a survey showing the American public opposes wiretapping, especially since the question asked did not include the essential qualifier *when done by law enforcement and authorized by a court order.* Since wiretapping is illegal without a court order, the survey at best tells us Americans oppose unlawful eavesdropping. So does the FBI.

In America, wiretapping is not used for comprehensive electronic surveillance of the general public. Nor is it used against petty criminals. Wiretapping is used against major drug traffickers, organized crime leaders, and terrorists.

Use of the electronic surveillance investigative technique has been sparse (as evidenced by figures found in the Federal Wiretap Report) and is constrained by significant statutory requirements including court orders, minimization, and extensive record keeping. In addition, it is labor intensive and costly (averaging $45,000 per tap in 1991). After a tap has been completed, government attorneys are required to notify the subjects of the electronic surveillance. That so few people even know of anyone who has received such notification shows the myth of comprehensive electronic surveillance of the general public has little do to with reality.

Several commentators expressed a concern about possible wiretap abuses by the government. However, none of the commentators has identified a single act of wiretapping abuse occurring under the current wiretapping statutes, which date back to 1968 (Title III of the Omnibus Crime Control and Safe Streets Act) and 1978 (Foreign Intelligence Surveillance Act), respectively. The American system of government has extensive mechanisms to protect against possible wiretap abuses. These include the illegality of unauthorized wiretapping (criminal and civil actions against violators); the inadmissibility of electronic surveillance evidence obtained without authorization; pretrial motions to discover the use of wiretapping; the availability of the Freedom of Information Act to people to determine if electronic surveillance has been carried out with regard to them; mandatory reporting of electronic surveillance efforts to Congress; Congressional oversight committees and hearings; and the use of the media to expose abuses. Even Rotenberg acknowledges the electronic surveillance law "set[s] out elaborate restrictions on wire surveillance." Thus, the perceived threat of a "pervasive and powerful government" seen by Mike Godwin is, in fact, subject to constant public, Congressional, and judicial scrutiny.

Godwin quotes part of Justice Brandeis's dissenting opinion in *Olmstead vs. United States* and cites the *Katz* decision as support for the view that communications privacy should be deemed sacrosanct and beyond the reach of government ("the whole point of the Bill of Rights was to remove some rights from any balancing act"). Such a position is not sup-

ported by the Constitution, statute, or case law, or even the opinions expressed by Brandeis. Historically, the law has specified that if the government conducts a search—electronic or otherwise—it must be reasonable, and hence it must be pursuant to a warrant or court order. The Fourth Amendment *explicitly* grants authority for searches and seizures when there is *probable cause* and a *warrant* issued, and the Fifth Amendment says that no person shall be deprived of life, liberty, or property *without due process of law.* The Amendments *explicitly* balance individual rights such as privacy with the government's responsibility to protect our liberties by enforcing the laws.

Andrew Grosso says "the burden of carrying out such intrusions [electronic surveillance] has always rested with the agency or person seeking the warrant or tap. This [digital telephony] legislation seeks to change that." Similarly, Lewis and Anne Branscomb claim the existing laws do not require that telecommunications systems be designed to make wiretapping easy. Although partly true, these statements are misleading because they ignore the assistance provisions found in the federal wiretap statutes. These provisions mandate that telecommunication service providers provide law enforcement with "all information, facilities, and technical assistance necessary to accomplish the interception," when served with a court order. Telecommunication service providers who receive numerous such orders over time are clearly on notice of this requirement. The question then becomes should these service providers intentionally design systems to impede or prevent electronic surveillance or, on the other hand, to accommodate this public safety requirement. Legislation is needed to provide the answer.

The proposed legislation does not, as the Branscombs assert, depart from U.S. legal tradition. There is ample precedence for legislation (including fine provisions) that allows the government to establish requirements for the purpose of preserving public safety. Drivers must display license plates on cars, which allow the police to identify them on the road. While such governmental requirements can, in a narrow sense, be seen as impinging on individual liberties, such requirements preserve other liberties (e.g., restricting pollution allows others to breathe clean air). Wiretapping's impingement upon the liberty of a criminal to conceal communications preserves the liberty of honest persons to live in a safe and orderly society.

Godwin claims since there are provisions for a $10,000-a-day fine, the government is seeking new wiretap authority. The fine, if used, does not create authority; it exists to enforce the viability of the basic wiretap authority that has long existed. Further, even under the current law there would be an arguable basis for assessing fines against service providers who refused to provide assistance to law enforcement when served with a court order.

Rotenberg complains that the FBI has failed to disclose the exact details of the technical problems and impedance to electronic surveillance. This complaint is misplaced because it would be inappropriate for the FBI to make such public disclosures. He also complains about the FBI setting technical standards and not disclosing technical alternatives. In fact, the legislation only sets forth *generic* requirements, leaving the technical approaches and details to the service providers. The FBI has stated it has no interest in regulating technology. Yet while challenging the assessments made by FBI experts in wiretap technology and law, he seems willing to accept the often ungrounded assessments of RISKS contributors with much less expertise.

Rivest says the complexity of our telecommunications infrastructure will outpace any systematic attempt to tap it. All the people I have talked with in the telecommunications industry and in the FBI agree that the new technologies *can* be tapped, but that in some cases (e.g., with advanced call forwarding), the taps would have to be effected in ways differently than performed today such as within the networks or switches. Rather than requiring the service providers to design an intercept capability into their telecommunication systems, Godwin seems to prefer the FBI or some local police force "innovate" interceptions on their own. Grosso, who apparently does not object to law enforcement conducting wiretapping within more advanced telecommunications networks, nevertheless argues that the proper remedy is for Congress to finance law enforcement to conduct wiretapping.

Aside from the fact that governmental funding would necessarily be much more expensive than requiring service providers to pay for technology modifications, in many instances this would not be technically feasible for the government or operationally acceptable, either because of a lack of access to the internal workings of the networks, switches, and switch software, or because law enforcement would lack the expertise. Given the complexity of telecommunications networks, I do not believe it would be prudent to require (or for that matter, allow) law enforcement to tinker with highly complicated and intricate telecommunications systems and risk disruption of service.

Rotenberg states that I said the FBI "is not seeking a remote monitoring capability." I never said this. Remote monitoring is a long standing requirement and does not necessitate legislation. The point is that law enforcement is not seeking to use the remote monitoring capability to *dial into* a system, and that law enforcement *would not be able to initiate* a tap from such a facility. Taps could be initiated *only* by service providers.

The Branscombs were unconvinced by my claims that telecommunications switches can be made secure while at the same time affording access for electronic surveillance. I did not mean to suggest they could be made *immune* (in fact, they are not *immune* now), but that the risk could be made acceptably small. More importantly, telecommunications networks security is fundamentally important for reasons of reliability and integrity in general. If someone can gain unauthorized entry into a telecommunications switch and bring a portion of our communications infrastructure down, the consequences would be far worse than if someone

listens in on a few conversations. However, most break-ins occur through sloppy practices (e.g., no passwords or weak passwords, not through holes in the technology). Such break-ins can be avoided through more robust and exacting authentication and access mechanisms

Godwin claims that criminal investigations, for the most part, will be unaffected by the loss of electronic surveillance capabilities occasioned by technological difficulties, arguing that the single most useful resource in criminal investigations is the informant. Similarly, Rotenberg claims the government has not been forthcoming in disclosing the basis for its legislative proposal and whether "other investigative methods [were] considered." First of all, the electronic surveillance statutes specify that if an investigation can be thoroughly and successfully conducted with other normal investigative techniques, such as by using informants, a judge is not permitted to issue an electronic surveillance order. Hence, as a matter of law, if informants were as effective as Godwin asserts, or if other methods were available as Rotenberg suggests, there would never be a need for wiretapping or for the proposed legislation.

This, of course, is not the case. For example, as useful as informants may be, they do not provide all the evidence required to prosecute criminals or whole criminal conspiracies, and in some instances their credibility or reliability is at issue. In a talk at EDUCOM '92, Ed Tufte, a leading authority on the visual display of information, explained how organized crime leader John Gotti was acquitted during one state trial because the defense was able to cast doubt on the credibility of the informants by showing a chart listing all their criminal offenses. He was not convicted until in a later Federal trial the FBI was able to produce tapes of Gotti's own conversations obtained through electronic surveillance (in this case, bugs) wherein he was overheard admitting he had a person murdered. In short, law enforcers need wiretapping and other electronic surveillance tools to obtain evidence in those cases where other methods fail. While it is impossible to say how many cases would have remained unsolved without wiretapping, one of the FBI agents who conducted the taps in the military procurement fraud case ("Ill-Wind") said it would have been impossible to get the evidence any other way.

With regard to my comment that technological features which accommodate wiretapping may be attractive to other governments, Rotenberg retorts that such technology would have delighted the old East German Secret Police and the KGB, and that there would be no market at all for such features in Japan since their constitution prohibits wiretapping (in fact, neither the Japanese constitution nor any statute prohibit wiretapping, although this technique is only used rarely). These are extreme examples. The fact is some of our closest democratic allies (the British, Germans, French, Canadians, Australians) have electronic surveillance laws and, like the U.S., will be facing similar technological challenges to their interception capabilities. It is interesting to note that whereas the FBI has been quite successful in fighting and dismantling organized crime families through the use of electronic surveillance, organized crime in Japan (the Yakuza) flourishes and is a substantial problem, often corrupting businesses and political leaders.

While Rivest may be right in his assertion that most Americans feel they have "a basic right to a private conversation," as noted earlier, our laws do not actually grant this right absolutely. Under the Constitution and statutes passed by our Congress and upheld by the Supreme Court, private conversations are subject to court-ordered surveillance. Thus, wiretapping has been part of the established balance between individuals and their government. Hence Rivest's assertion that cryptography restores a balance that was lost with wiretapping is not accurate. It is more accurate to say that the widespread availability of cryptographic products to protect communications from government surveillance will create an unprecedented situation.

Whitfield Diffie pointed this out at the 1992 Conference on Computers, Freedom, and Privacy, provocatively asking whether society as we now know it would exist if the availability of undecipherable communications had existed earlier, thereby allowing for communications without accountability. He proposed a compromise that would guarantee accountability by making communications accessible with a court order, but that would prevent covert access. I agree with Rivest that we must flesh out a "menu" of policies that are technically supportable. I am optimistic we can design products that would allow the government to conduct electronic surveillance when authorized without seriously jeopardizing the ability of industry to protect the privacy and commercial interests of their customers, but further study is clearly needed. The Branscombs claim I am—along with the FBI—inviting us onto a slippery slope with regard to governmental involvement in the area of encryption, but the unrestricted use of encryption and ensuing social unaccountability could prove far more slippery.

The argument for a viable wiretapping capability is not an argument about absolutes. There will always be a potential for government abuse; some clever criminals will on occasion avoid detection; and some systems whose security practices are lax might be compromised. The argument is about fighting society's most serious crime problems, cost-effective law enforcement, and security commensurate with risk. It is time to acknowledge that *1984* was fiction and recognize our extensive system of government checks and balances has worked exceedingly well in preventing and exposing abuses and, when needed, producing needed reforms. Crime is a serious problem in this country. Without a cultural shift that would drastically reduce the level of crime, it would be unwise and unconscionable to knowingly design our communications infrastructure in such a way that would make effective law enforcement more difficult or impossible when we can avert it through proper planning now.