Privacy on the Line

Reviewed by Stewart Baker and Peter G. Neumann

Editor's Note: U.S. cryptography policy has become a highly controversial issue. For this reason the *Notices* intentionally solicited two independent reviews of *Privacy on the Line*. The reviewers were chosen in order to provide two different perspectives on the issues raised in the book.

One of the book's coauthors, Susan Landau, is a member of the *Notices* Editorial Board. To prevent a conflict of interest, she did not participate in the decision to review the book, the choice of reviewers, or any other aspect of the preparation of these reviews.

Privacy on the Line: The Politics of Wiretapping and Encryption
Whitfield Diffie and *Susan Landau*
MIT Press, 1998
342 pages
Hardcover $25.00 (ISBN 0-262-04167-7)

Stewart Baker

I wasn't sure I would like this book, but I knew I had to read it. It's the story of my life—the last several years, anyway.

In the early 1990s I was the general counsel of the National Security Agency (NSA), a job that required me among other things to sell key escrow encryption and the Clipper Chip to the Clinton Administration (mission accomplished) and to the rest of the country (er, the less said about that, the better). I had the chance, too, to work closely with the Federal Bureau of Investigation (FBI), especially on the problem of how to conduct wiretaps in a new and far more demanding environment.

One of the surprising results of breaking up AT&T was to create a slow-motion crisis for law enforcement. So long as communications were controlled by one company—with a heavy stake in demonstrating its good citizenship—planning for and providing wiretap access was easy. AT&T knew what the FBI needed, and it could build those requirements into its products, passing the cost along to consumers. But deregulation put a

(Continued on following page)

Stewart Baker practices law at Steptoe & Johnson in Washington, DC. His e-mail address is `sbaker@steptoe.com`.

Peter G. Neumann

Mathematically, cryptography is an incredibly complex and fascinating subject. However, from many other perspectives—political, legal, diplomatic, social, and economic—cryptography policy is also incredibly complex; as *Privacy on the Line* demonstrates, it is fascinating from these perspectives as well. This book performs an extraordinary service for readers wishing to understand how we got to where we are today with respect to privacy and the uses of cryptography and wiretapping, and what the potential implications are for the future.

Privacy on the Line is beautifully written and makes complex issues readily understandable to the reader who is curious and eager to learn; in some chapters it almost has the appeal of a spy thriller. On the other hand, it is carefully researched and documented with copious references that should whet the appetites of the most intense and knowledgeable readers.

(Continued on page 711)

Peter G. Neumann is principal scientist in the Computer Science Lab at SRI International in Menlo Park, CA. His e-mail address is `Neumann@csl.sri.com`*; Web site:* `http://www.csl.sri.com/neumann/`.

*(**Baker** continued from previous page)*

premium on getting to market quickly, reducing overhead, and building lightweight innovative products. Law enforcement wasn't the customer, and it was increasingly left behind in the explosion of new products and services. Often law enforcement didn't have the technical expertise or the funds to adapt to the new technologies, and sometimes even expertise and money weren't enough.

After several years of trying to jawbone industry into compliance with its requirements, the FBI decided in the early 1990s that it needed a big stick—it needed a law. The law would not try to sort out all the technical problems that industry said were preventing wiretaps. It would solve the problem by fiat, simply requiring that all telecommunications carriers and manufacturers design wiretap capabilities into all their products and services.

Privacy advocates were horrified. The press was hostile. Industry jeered. Not one member of Congress could be found who would introduce the FBI's bill.

The FBI, however, never gave up. They showed up for every debate, they mobilized local police, they lobbied Congress relentlessly.

Three years later the Senate passed the Communications Assistance to Law Enforcement Act (CALEA), with the FBI's requirement, by a voice vote of 98-0.

That was round one. Round two, for the FBI, is encryption. Most of the computer software and hardware industry sat out the fight over CALEA, and those companies haven't grasped how much the CALEA debate shaped the FBI's view of encryption.

Thanks to CALEA, the FBI is undaunted by the technical complexity of building key recovery into encryption, or by the claims of industry that it can't be done. They heard the same thing from telecommunications companies—all of whom are now building wiretap capabilities into their products.

And thanks to CALEA, the FBI is not too troubled by the bad press it's getting over encryption or by the privacy and industry complaints—or even by the congressional harrumphing. They've heard all that before, too. In the CALEA debate it was patience that paid off, and in the end the Bureau believes that Congress will have to mandate crypto controls just as it had to mandate wiretap requirements.

Since leaving government I've advised dozens of companies on how to live not just with encryption controls and key recovery but also with CALEA. I've started to joke that my law practice consists of being the first lawyer to discover that the country's main technology and telecommunications regulatory body is the Federal Bureau of Investigation.

So any book that deals with the politics of wiretapping and encryption is hard to resist. If I took it to the beach to read, I could probably deduct the trip.

Still, I had my doubts. Whitfield Diffie is a famous cryptographer, of course, but I knew him first as NSA's single most determined and effective opponent. I can't defend every aspect of the government's current policies on encryption and wiretapping, but I still have a deep reservoir of sympathy for that point of view. Wiretapping is an important criminal investigation tool, particularly when law enforcement is targeting the leaders of organized crime, who usually don't commit crimes so much as order them committed. There is no doubt that a wired society needs ubiquitous encryption, but it's equally true that ubiquitous encryption will give wired criminals new protections from the law.

That's why I still bridle at too-simplistic Silicon Valley retorts to law enforcement concerns—especially those that run along the lines of "We're smart. We're rich. They're not. We win." I wasn't looking forward to reading a self-congratulatory book about clueless cops being outsmarted by liberty-loving technologists.

To my surprise, that's not what Diffie and Landau have written. They've produced something quieter and more useful. Like a handful of others (mostly professional privacy advocates and FBI officials), they see the entire picture—something the high-tech industry has so far only seen in bits and pieces. Ready or not, the FBI is determined to force us all into a debate over how and whether we will shape the direction of technological change.

This book draws together the elements of that story in a fashion that is scholarly, though it's too well written to deserve that adjective. Diffie and Landau don't quite popularize the issue—this is still a book only a policy wonk could love—but they ease the reader gracefully into some remarkably complex material as though it were a warm bath.

The book begins with an admirably simple introduction to cryptography that carries the reader deep into the topic. I have to confess that I never knew how "S-boxes" got their name until I worked my way through Diffie and Landau's description of the Digital Encryption Standard and its historical debt to Vingenere ciphers. (I told you this was a wonk's book.) The authors next march the reader through a history of crypto policy, laying out the interests of the NSA, the public cryptography movement, law enforcement, the National Institute of Standards and Technology, and privacy advocates.

With the groundwork laid, the book then plunges into wiretapping, its history, value, and abuses. It sketches the FBI's five-year fight to enact CALEA. The closing chapter traces the evolution of the encryption debate from a fight between the software industry and the NSA into a fight that pits the FBI against the likes of Americans for Tax Reform and the National Association of Manufacturers.

Throughout this tour, there isn't any doubt where the authors' sympathies lie. They linger almost lovingly over thirty- and forty-year-old stories of how the FBI once abused its wiretap authority. They insist on a long and not entirely persuasive discussion of why wiretaps aren't that useful to law enforcement. Government arguments tend to get much shorter shrift than civil libertarian rebuttals. But it is perhaps a sign of how bitter the encryption battle has become that Diffie and Landau deserve credit for including the government's arguments at all.

They deserve praise as well for avoiding dishonest arguments that support their point of view. Not everyone in this debate is so careful. Lawyers for industry, for example, can still be heard to argue that there's no need for encryption controls because the FBI hasn't offered evidence that it has lost any cases because of good crypto. Of course this is the kind of Catch-22 argument that is hard to resist because the lawyers know it can't lose. If the FBI found a way to read the files, then the industry lawyers can say, "See, crypto wasn't a problem." And if the FBI is truly stymied and can't read the files, then the lawyers can say either, "The defendant was acquitted, and there's no proof the encrypted files were related to a crime," or "The defendant was convicted, so the FBI didn't need to decrypt the files." Unlike some of their allies, Diffie and Landau never insult our intelligence.

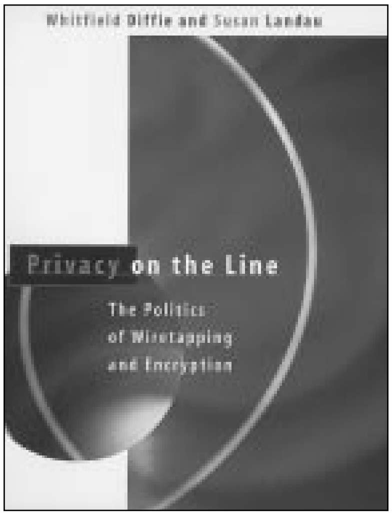
In short, it's hard to imagine a better introduction to an issue that will be with us for years to come.

(*Neumann* *continued from page 709*)

Wiretapping and cryptography are sometimes depicted as a classical conflict between good and evil, depending on which side the supposed protagonist is on. *Privacy on the Line* makes it quite clear that the picture is not quite so simple—indeed, there are also elements of good versus good and evil versus evil. The good news is that crypto can be used for good; the bad news is that it can also be used for evil.

The real question is which of two capabilities is more important: (1) protecting our civilization from widespread losses of privacy and violations of personal integrity that can result when cryptography is applied inadequately or not at all, or (2) guaranteeing the law enforcement and national security communities the power of rapid surreptitious access to essentially all communicated or stored information. Ideally we might believe that there could be a solution that does both; however, that appears to be wishful thinking, especially because the key-recovery technology is likely to be inherently vulnerable to misuse. The debate to date seems to suggest that there is no easy middle ground and that any solution will be a tenuous one at best.

The first nine chapters are rather well balanced, presenting with equal care the viewpoints of national security, law enforcement, and ordinary citizens. However, the final chapter comes down strongly on the side of humanity and comes to grips with the question posed above. The answers given in the book make sound sense if you have read the first nine chapters and thus understand the basis for the reasoning given in the last chapter.


Whitfield Diffie and Susan Landau
Privacy on the Line
The Politics of Wiretapping and Encryption

Several quotes from Chapter 10 are worth noting here:

"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." (page 242)

"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." (page 244)

"The availability of cryptography for criminal uses may not turn out to matter all that much. ... Criminals today make far more use of covert means of communication (most notably cloned cell phones) rather than of overtly secure means." (page 245)

Much of the controversy in the past few years centers on cryptographic techniques (known as key-recovery or key-escrow schemes) that contain intentional trapdoors whose purpose is to permit law enforcement and national security personnel to gain surreptitious access to encrypted communications and stored information. Given the inherent security weaknesses in our computer and communication infrastructures (which in the past have been separate, but which are rapidly converging), such trapdoors could easily lead to misuse. In addition, proponents of such systems that permit stealthy access to keys have made little if any effort to examine the long-term costs and risks of creating and operating the infrastructures necessary to enable almost immediate surreptitious access. William Reinsch of the U.S. Commerce Department has enumerated several reasons why law enforcement itself is reluctant to use key-recovery crypto[1], although he carefully skirted discussion of the inherent security risks arising from trapdoor access. Also, serious questions remain unanswered about whether the actual needs for such capabilities are justified by existing conditions. Furthermore, there could be serious risks for electronic commerce and for misuse of information about innocent individuals; very few of these risks have been considered in any detail. My own book (*Computer-Related Risks*, Addison-Wesley, 1995) suggests that many of the risks of misapplying computer-communication technology are simply not avoidable in practice, even in the presence of great perseverance.

It is clear that law enforcement needs to explore some other approaches. The book does a good job in exploring some of the alternatives to wiretaps and trapdoor encryption schemes that could avoid many of the risks that might otherwise arise. Such alternatives include pen registers and trap-and-trace devices for telephony, radio communications, video cameras, computer systems themselves, tracking of credit card usage, materials transport, etc. A section on electronic surveillance concludes with this sentence: "On balance, the impact of technology is so weighted on the side of law enforcement as to make it remarkable that crime has survived at all." Although that comment might seem facetious, it perhaps suggests that law enforcement has not taken optimal advantage of the tools at its disposal.

Potential misuse by government employees is also a serious concern. Chapters 6 ("Privacy: Protections and Threats") and 7 ("Wiretapping") include numerous examples of misuse that have occurred in the past and that must be addressed honestly in future policy considerations. Perhaps most prescient is a 1928 quote from Justice Louis Brandeis:

"'In the application of a constitution, our contemplation cannot be only of what has been but of what may be.' The progress of science in furnishing the government with means of espionage is not likely to stop with wiretapping. Ways may some day be developed by which the government, without removing papers from secret drawers, can reproduce them in court, and by which it will be enabled to expose to a jury the most intimate occurrences of the home. ... Can it be that the Constitution affords no protection against such invasions of individual security?" (pages 148–149)

The credentials of the authors are impeccable. Whitfield Diffie is the coinventor of public key cryptography (with Martin Hellman and Ralph Merkle), extraordinarily knowledgeable on the total history of unclassified manifestations of cryptography and an articulate spokesman for noncompromisable strong cryptography. Susan Landau was the responsible author for the 1994 ACM (Association for Computing Machinery) report, "Codes, Keys, and Conflicts: Issues in U.S. Crypto Policy", finding common ground among a diverse study group that included Diffie and this reviewer as well as representatives of NSA and the Department of Justice. That report clearly laid out the basic questions. (Landau has also written about cryptography policy for the *Notices*, beginning in 1983.) Diffie and Landau each briefed the National Research Council (NRC) cryptography study panel that produced the unclassified 1996 National Academy Press report, "Cryptography's Role in Securing the Information Infrastructure (CRISIS)". (The NRC group operated under high-level U.S. Government clearances and included several distinguished former government officials.) *Privacy on the Line* provides in-depth background that goes beyond what can be found in the ACM and NRC reports. Its fundamental conclusions begin in essence where the NRC study left off. The CRISIS report concluded that the "debate over national cryptography policy can be carried out in a reasonable manner on an unclassified basis." The conclusions of the final chapter of *Privacy on the Line* are even stronger and, in my opinion, are well supported by the first nine chapters of the book.

Cryptographic policy is an international issue. The debate in the U.S. and elsewhere is likely to go on for a long time, even if it is seemingly legislated one way or the other. But deeper understanding of the issues is urgently needed before any policy is invoked. *Privacy on the Line* is a major step in that direction.

My view is that noncompromisable strong cryptography will become widely available around the world irrespective of intended controls, and that is, on balance, in the best interests of national and world stability. Instead of seeking restrictive cryptographic policies and potentially dangerous trapdoors, law enforcement and intelligence communities urgently need to pursue some of the alternatives—which may turn out to be more cost effective anyway. (My own extremely mixed metaphor on the subject is that Pandora's cat is out of the barn, and the genie won't go back in the closet.)

[1] *"Non-Key Recovery Exports after Two Years", memo to Deputies Subgroup on Cryptography, November 25, 1996, obtained by the Electronic Privacy Information Center under the Freedom of Information Act.*