Preface to the Updated and Expanded Edition

It would be difficult to find a more fundamental theme in the contemporary world than the migration of human activity from physical, face-to-face contact into the virtual world of electronic (and digital) telecommunications. Globalization would not be possible without the high-quality, reliable, and inexpensive telephone service that has been made possible by optical fibers and computerized central offices. In the industrialized world and beyond, governments, businesses, universities, and other institutions have made the World Wide Web a centerpiece of their communications with the public.

One of the critical issues raised by this transformation is what effect it will have on privacy and security. The digitization of the world has made the effortless privacy of interpersonal conversations a thing of the past and enabled spying on a global scale never before seen. The decisions we make as we lay the foundations of the new world will have an impact on the structure of human society that transcends that of any previous technological development. If, in designing our new world, we do not take privacy and security into account in a way that reflects the primacy of the individual, our technology will enforce a social order in which the individual is subordinate to the institutions whose interests were put foremost in the design.

The first edition of *Privacy on the Line* was written at a time in which the issue seemed simple. The primary technology for protecting telecommunications privacy was cryptography, and the right to use cryptography for the protection of personal and business privacy seemed in jeopardy. The battle had two fronts, and we set out to explore them both.

The more visible front was chronologically second but stood first in most people's minds. The US government's plan for *key escrow* sought to use its standard-setting power—backed by its substantial purchasing power—to make cryptographic systems with built-in government master keys ubiquitous. Had the plan succeeded, it might plausibly have been extended to outlaw systems that did not have this provision.

The less visible but economically more significant front was export control. Exporting of cryptographic products had been tightly controlled for decades but, until the sudden need for cryptography in commercial uses that followed the opening up of the Internet this had, by and large, only the intended effect of inhibiting the exporting of cryptographic equipment intended for military customers. As low-cost integrated circuits brought high-grade cryptography within the reach of many commercial products, its use expanded steadily. Businesses oriented toward making consumer products now found themselves forced by the export laws to bear the unrewarding expense of producing separate products for export and for domestic consumption.

The first edition was written in the midst of this political struggle over whether individuals and commercial enterprises had a right to protect their communications with cryptography or whether governments had the right to limit its use to prevent possible interference with their law-enforcement and intelligence activities. The preface to that edition gives a flavor of the situation as it stood at that time.

A book written in the midst of events will always become outdated, sometimes quite quickly. Just the short interval between the appearance of the original edition and the first paperbound edition saw a striking sequence of events.

- The existing encryption standard was decisively shown to be inadequate. In an event noteworthy for its neatly orchestrated publicity, the Electronic Frontier Foundation revealed that it had built the often-designed *DES Cracker*—a specialized computer capable of producing DES keys from cipher text in (at worst) just over a week.

- The secret Skipjack algorithm that underlay the key-escrow plan was declassified, apparently in order to allow the Department of

Defense to save money by using software encryption to secure email in the *Military Message System*.

- The National Institute of Standards and Technology's plans for an Advanced Encryption Standard (AES) to replace DES by a cipher with blocks twice as long and a key nearly five times as large made dramatic progress, with fifteen designs accepted for first-round evaluation and presented at a public conference as well as published on the Web.

More dramatic events were to follow shortly. In September 2000, the American export control rules were revised to place less emphasis on the strength of cryptography and more on the end users and the degree of customization provided. Selling off-the-shelf hardware and software to commercial users throughout the industrialized world became relatively easy, while selling customized equipment, particularly to governments, continued to be burdened with a lengthy approval process. The scheme was clever because foreign military organizations—the major target of export control—had well-established cryptographic traditions and usually wanted to employ their own cryptographic algorithms rather than those in common use in the commercial world.

An important ingredient in the demise of export control was the unexpected exposure of a multi-national (though primarily US-controlled) signals intelligence network called Echelon that appeared to be organized for the interception of commercial rather than military traffic. Never mind that the world's military were making ever increasing use of commercial channels; it looked to the Europeans as though they were being spied on. Their response was a new emphasis on secure communications, and one important step was decreased regulation.

By comparison with export regulation, key escrow merely faded from view without being officially withdrawn or renounced. When the National Institute of Standards and Technology began the process of replacing the quarter-century-old Data Encryption Standard with a new system, it placed a high level of security at the top of its requirements. The resulting *Advanced Encryption Standard* was adopted in late 2001 and has since been approved for national-security applications as well as civilian ones.

Even as these events were under way, it was clear to observers that the underlying issues had not been resolved and that other, non-cryptographic, aspects of communications privacy were evolving in a different direction. Although regulatory jockeying and lawsuits delayed its full implementation, the Communications Assistance for Law Enforcement Act was, for the first time, forcing the major telecommunications companies to build wiretapping into the infrastructure of the American communications system. In a disquieting parallel development, the FBI had begun demanding the right to implement wiretap orders by installing its own hardware on the premises of Internet Service Providers rather than presenting the order to the ISPs and allowing them to comply using their own technology. Critics feared that the new technique would lift a layer of scrutiny from the wiretap process. If the ISP were not doing the monitoring, they would not know what was being monitored, and would be unable to challenge overbroad interception.

Cryptography, free from oppressive regulations, was going nowhere fast. Although SSL (the Secure Socket Layer protocol used to protect Internet commerce) is perhaps the most widely deployed cryptographic mechanism of all time, the application of cryptography to protecting Internet communications—and electronic communications overall—is spotty. Some Web transactions and most VPN connections are encrypted, but only a small fraction of email, voice, or video communications, or even Web browsing, is protected.

There are many proximate causes of the changed aspect of communications privacy. In the late 1990s, the world, particularly the United States, was in the midst of a massive economic boom. The collapse of the Soviet Union had given America the sense that it had no real enemies, and, despite vicious civil wars in Africa and Eastern Europe, the world seemed more peaceful than it had been in decades.

The September 2001 attack on the United States ended that sense of peace and initiated an era of widespread fear, fear that inclined the population toward accepting greater encroachment on their liberties and supporting more ambitious intelligence programs. At the time of this writing, the activities of the intelligence community (what they are and what they should be) have become a subject of debate in the courts, the Congress, and the press.

The debate has moved beyond the attempt to suppress access to strong cryptography. In the United States such access is now supported, in principle, by government policy. In Britain, a state right to access encrypted information was included in the Regulation of Investigatory Powers Act. The law authorizes expanded surveillance, and one clause requires individuals to divulge cryptographic keys on demand.

The political battle in the United States now focuses on decline of the once-rigid wall separating foreign intelligence from domestic law enforcement. There is acceptance of the increasing use of facilities originally built for spying on other countries to spy on targets inside the United States. Along with the shift in policy comes a steady push to extend the built-in wiretapping approach of the Communications Assistance for Law Enforcement Act from the conventional telephone system to the Internet.

In an effort to provide supporting material for the conduct of the new debate, we have brought out this updated and expanded edition, adding two new chapters and changing the existing ones in varying degrees to reflect new developments.

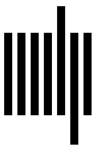
Privacy on the Line

The Politics of Wiretapping and Encryption

By: Whitfield Diffie, Susan Landau

Citation:

Privacy on the Line: The Politics of Wiretapping and Encryption
By: Whitfield Diffie, Susan Landau
DOI: 10.7551/mitpress/5572.001.0001
ISBN (electronic): 9780262256018
Publisher: The MIT Press
Published: 2010



The MIT Press

Composed in LaTeX 2ε by the authors.
Set in Sabon by Loyola Graphics of San Bruno, California.
Printed and bound in the United States of America.

Library of Congress Cataloging-in-Publication Data

Diffie, Whitfield.
Privacy on the line : the politics of wiretapping and encryption / Whitfield Diffie, Susan Landau. — Updated and expanded ed.
p. cm.
Includes bibliographical references and index.
ISBN 978-0-262-04240-6 (hardcover : alk. paper)

1. Electronic intelligence—United States. 2. Wiretapping—United States. 3. Data encryption (Computer science)—Law and legislation—United States. 4. Electronic surveillance—United States—Political aspects. 5. Telecommunication—Political aspects—United States. 6. Privacy, Right of—United States. I. Landau, Susan Eva. II. Title. III. Title: Politics of wiretapping and encryption.

UB256.U6D54 2007
342.7308'58—dc22 2006035514