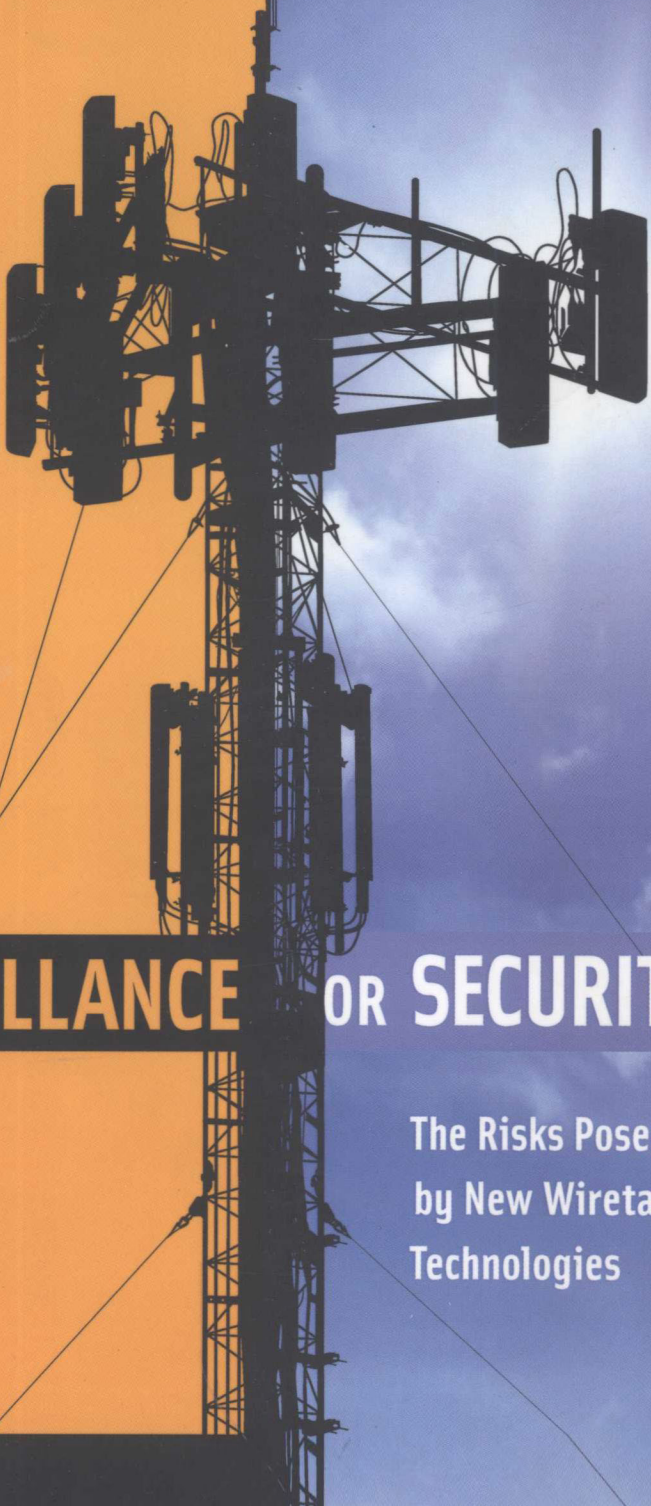
SUSAN LANDAU



SURVEILLANCE OR SECURITY?

The Risks Posed by New Wiretapping Technologies

Surveillance or Security?

Surveillance or Security?

The Risks Posed by New Wiretapping Technologies

Susan Landau

The MIT Press
Cambridge, Massachusetts
London, England

First MIT Press paperback edition, 2013

This book was set in Stone Sans and Stone Serif by Toppan Best-set Premedia Limited. Printed and bound in the United States of America.

Library of Congress Cataloging-in-Publication Data

Landau, Susan Eva.
Surveillance or security? : the risks posed by new wiretapping technologies / Susan Landau.
p. cm.
Includes bibliographical references and index.
ISBN 978-0-262-01530-1 (hardcover : alk. paper)—978-0-262-51874-1 (paperback)
1. Telecommunication—Security measures—United States. 2. Wiretapping—United States. 3. Data encryption (Computer science)—Government policy—United States. 4. Electronic surveillance—Political aspects—United States. 5. Computer crimes—Risk assessment—United States. I. Title.
TK5102.85.L36 2011
363.25'2—dc22

10 9 8 7 6 5 4 3 2

This book is dedicated to Daniel, Emmy, and Ellie.

Contents

Author's Note

Throughout this book, when I say the *Internet*, I mean the packet-moving layered architecture described in chapter 2. The Internet does not include the applications—the Googles, Facebooks, and so on—that lie above this architecture. Often the public conflates these two. I owe the observation about the confusion to Stefan Savage, who pointed out that engineers and the public have two differing definitions of the Internet. While there are security problems in both Internets, the ones that make securing the Internet extremely difficult are the ones inherent in the packet-moving architecture. This book focuses on these problems.

Preface

Several years before this book was completed, I gave a talk at a company's annual meeting for its technologists. There was nothing particularly unusual about that; I was representing Sun Microsystems to technologists of a major customer. I spoke on new technologies being developed in Sun Labs. Someone from Microsoft also spoke, as did someone from Google, Intel, and so on. The meeting was held at a combination hotel/convention center. That, too, was not surprising. What was odd was the phalanx of hotel security guards who carefully monitored the meeting room as three hundred attendees trooped back and forth between talks, meals, and coffee breaks.

Because outsiders had been invited to attend the sessions, there was no company proprietary information presented at the talks. The hotel was somewhat isolated; it was a large complex on the edge of several four-lane roads. I did not really think much about the security guards until the evening a guard walked into the elevator as I was going up to my room. Except for the United States right after September 11, and traveling in the Soviet Union and China, I could not recall ever having been in a place with so many security personnel, and I commented on the large number of guards I had seen in the hotel.

"That's good," he replied. I thought about this a day later, as the hotel's shuttle service took me back to the airport. The driver had a uniform that included a white shirt with epaulettes. I have taken shuttles in more states of the union and to and from more airports than I care to count. Some shuttle services are more professional than others, but never before had I been driven to the airport by someone who looked like he worked for the military in a third-world dictatorship. That's when I began to reflect on the security guards who had stood before the conference room.

I am sure that the company whose meeting it was did not arrange for the guards. Rather it was the hotel that provided them as part of the service

of running a conference. The service was unnecessary. Any determined "spy"—I say "spy" in quotes because no proprietary information was released during the conference—could have counterfeited a badge and gone to hear the presentations. The guards kept out the hordes on the street, except that the hotel was on an inaccessible four-lane roadway. There was no street and no hordes. The guards were completely superfluous, but they were required by the hotel contract. The money the company was spending on guards' salaries was money it was not spending on training additional security technicians, on upgrading its IT infrastructure, or on improving the security of its products (which included defense information systems sold to the U.S. government). These guards were not providing good security. The situation was even worse. The cost of this "security" prevented this company from protecting what mattered.

The guards provided what Bruce Schneier has called *security theater:* the appearance of security rather than the genuine article. There are thousands of examples of this, from TSA inspections of passengers and X-rays of their hand luggage without accompanying inspection of the parcels that ride in the bellies of the planes, to the ubiquitous closed-circuit TV (CCTV) cameras appearing everywhere with little evidence that their usage actually cuts crime.[1] The cost of CCTVs diverts money from such activities as community policing. As such, their use may actually be counterproductive.

Electronic communication is the lifeblood of modern society. Simultaneously, such communication can be central to how criminals and terrorists conduct their business. Not a day passes without another story of Internet insecurities, critical infrastructure being attacked, attacks from China on U.S. corporations, and Russian hackers targeting U.S. consumers or Estonian government sites. In the decade since the attacks of September 11, in an attempt to keep the nation safe, the U.S. government has embarked on an unprecedented effort to build surveillance capabilities into communication infrastructure.

Unlike the TSA and CCTV examples, the issue of who is defending what runs more deeply than the question of whether we are diverting funds from techniques that may provide better security. What are these communication surveillance systems? Who are the guards? Are they really protecting us? Or are they working for someone else? Could these surveillance capabilities be turned by trusted insiders for their own profit, or used by our enemies to access our secrets? The fundamental issue is whether, by housing wiretapping within communication infrastructure, we are creating serious security risks. Understanding whether building wiretapping into communication infrastructure keeps us safe requires that we understand

the technology, economics, law, and policy issues of communication surveillance technologies. That is the point and purpose of this book.

I begin in chapter 1 by laying out the issues of communication and wiretapping within their social and legal contexts. In chapter 2, I discuss the development of communication networks, both the telephone and the Internet, while in chapter 3, I explain how the Internet came to be so insecure. These two chapters are more technical than the rest of the book and less technically trained readers may choose to skim them. I discuss legal aspects of wiretapping in chapter 4, effectiveness of communications surveillance in chapter 5, and evolving communications technologies in chapter 6. In chapter 7, I examine who is intruding on our communications, how they intrude, and what they are seeking. Having built that framework, in chapter 8, I look at the technology risks that arise when wiretapping is embedded within communications infrastructures, while in chapter 9, I look at the policy risks created by wiretapping technologies. In chapter 10, I examine how communication takes place during disasters; this gives different insights into communications security. I conclude in chapter 11 by discussing how we might get communications security and surveillance "right."

Note: Because my focus in this book is on whether widespread communications surveillance enhances or endangers national security, I am not addressing broader policy issues of U.S. national security. In particular, I will discuss only peripherally the role that the concentration of executive power over the last decades, and most particularly under the administration of President George W. Bush, has had in determining current U.S. communications surveillance policy. This issue—which has been the subject of many other publications—is beyond the scope of this book.

Acknowledgments

My thanks, first and foremost, go to my long-term collaborator, Whitfield Diffie, with whom I enjoyed many years of intellectual give-and-take. Much of my thinking on the issues of privacy, security, and surveillance has been influenced by our conversations. The direction my career has taken is no small part due to Whit, and I am very grateful to him.

Sun Microsystems was a great place to work: full of smart people and the ferment of ideas, and I was lucky to be there. I am particularly appreciative of Bob Sproull's strong encouragement and support for writing this book.

Dancing between policy and technology is complicated, and I owe many thanks to friends and colleagues who answered more questions than they imagined existed. I particularly want to thank Steve Bellovin, Matt Blaze, Clint Brooks, Jim Dempsey, Al Gidari, and Brian Snow. I very much appreciate Nancy Snyder's work on the illustrations for the book. I have benefited from meetings organized by Deirdre Mulligan and David Clark, and I would like to thank them for those as well as for many stimulating conversations. The following people generously shared their knowledge, read over sections, and translated text: Steve Babbage, Curt Barker, Jim Bidzos, Danny Cohen, Dennis Costa, Tom Cross, Gary Cutbill, George Danezis, Roger Dingledine, Chris Essid, Dickie George, John Gilmore, Andy Grosso, Ann Harrison, Paul Karger, Eleni Kosta, Leslie Lambert, Herb Lin, Steve Lipner, Nick McKeown, John Morris, John Nagengast, Peter Neumann, Hilarie Orman, Jon Peterson, Phil Reitinger, Jen Rexford, Ed Roback, Greg Rose, Ari Schwartz, Renee Stratulate, Paul Syverson, Lee Tien, and Jonathan Weinberg. I am very grateful to them all. In addition, there are a number of knowledgeable high government and private-sector sources whom I will have to thank anonymously.

Special thanks to Brown Kennedy, who told me to stop revising my outline and start writing. Without her, this book might still be a highly polished outline.

Everyone thanks their spouse or partner, and I am no exception. With great equanimity my husband, Neil Immerman, put up with my intense focus on surveillance, frequent travels to Washington, and a lifelong obsession, at least in pre-Internet days, with finding a copy of today's *New York Times*. He found me texts, read multiple drafts of this book, and even helped with typesetting.

It has been many years since I took a writing course with John McPhee and learned how the fact-checkers at the *New Yorker* insist on the accuracy of even the smallest fact.[1] My debt to John—and the legions of fact-checkers employed by the *New Yorker*—is enormous. I have done my best to apply the many lessons learned. Any errors in this book, however, are my own.