Privacy Lost

How Technology Is Endangering Your Privacy

David H. Holtzman

Foreword by Senator Evan Bayh

JOSSEY-BASS
A Wiley Imprint
www.josseybass.com

Privacy Lost

How Technology Is Endangering Your Privacy

David H. Holtzman

Foreword by Senator Evan Bayh

JOSSEY-BASS
A Wiley Imprint
www.josseybass.com

Published by Jossey-Bass
A Wiley Imprint
989 Market Street, San Francisco, CA 94103-1741 www.josseybass.com

Limit of Liability/Disclaimer of Warranty: While the publisher and author have used their best efforts in preparing this book, they make no representations or warranties with respect to the accuracy or completeness of the contents of this book and specifically disclaim any implied warranties of merchantability or fitness for a particular purpose. No warranty may be created or extended by sales representatives or written sales materials. The advice and strategies contained herein may not be suitable for your situation. You should consult with a professional where appropriate. Neither the publisher nor author shall be liable for any loss of profit or any other commercial damages, including but not limited to special, incidental, consequential, or other damages.

Readers should be aware that Internet Web sites offered as citations and/or sources for further information may have changed or disappeared between the time this was written and when it is read.

Jossey-Bass books and products are available through most bookstores. To contact Jossey-Bass directly call our Customer Care Department within the U.S. at 800-956-7739, outside the U.S. at 317-572-3986, or fax 317-572-4002.

Jossey-Bass also publishes its books in a variety of electronic formats. Some content that appears in print may not be available in electronic books.

Library of Congress Cataloging-in-Publication Data

Holtzman, David H., date.
Privacy lost: how technology is endangering your privacy / David H. Holtzman.
p. cm.
Includes bibliographical references and index.
ISBN-13: 978-0-7879-8511-0 (cloth)
ISBN-10: 0-7879-8511-2 (cloth)
1. Privacy, Right of. 2. Information technology—Social aspects. I. Title.
JC596.H64 2006
323.44'8—dc22

2006022977

Printed in the United States of America
FIRST EDITION
HB Printing 10 9 8 7 6 5 4 3 2 1

Contents

Privacy Invasions Hurt

Why Technology Is Key

Privacy in Context

The Technology

The Watchers

What Can Be Done?

Foreword

Privacy is something that most Americans care deeply about, even if they can't always agree on what it means. For some, it means freedom from interruption, like not having their dinner hour invaded by telemarketers. For many Americans, privacy issues hit where it hurts most—the pocketbook; identity theft is the most publicized instance of privacy violation and affects tens of millions of Americans every year. For others, privacy is a principle that they believe to be constantly under assault from corporations, technology, and the government.

This book addresses these issues and more. Although I may not agree with all of David's conclusions, he is doing a public service by launching a discussion on this important issue. Ultimately, public debate is the most basic freedom that we have, and it is critical that we exercise this right loudly and often, especially on important and evolving issues such as privacy. David gets that debate started in a thoughtful way.

Since September 11th, we have taken important steps as a nation to protect the American people from another terrorist attack on our soil. We live in a dangerous world with suicidal terrorists, and we must use information technology to protect our country against those who want to hurt us. However, we must also remain ever vigilant to avoid unnecessary erosion of the basic rights that we are fighting to protect. This book does an excellent job of examining the tension between protecting the United States and protecting our civil rights.

Privacy Lost explores in great detail the force that's driving the privacy debate—technology. Technology can help and harm, depending on how it is used and who is using it. The same computer capabilities that the Transportation Security Administration uses to spot terrorists and stop them before they board airplanes can cause problems for innocent citizens whose profiles happen to match descriptions or names on a security watch list. Senator Edward Kennedy had trouble flying because his name was on a watch list. The solution is not to reject this technology and its ability to protect us from terrorists but to refine it, improve it, and enhance our security by targeting terrorists faster, while at the same time reducing the impact on the innocent.

In addition to the balance of security and privacy that must be managed by the government, there is a growing threat to consumers from data-management companies. *Privacy Lost* explains how advances in technology have enabled these businesses to maintain unprecedented amounts of information on each of us. This profiling makes many people uneasy, because of concerns about privacy in general as well as fear of being incorrectly labeled. An obvious example is credit scoring. These computer systems automatically decide whether we are worthy of credit or too big a risk, without the possibility of appeal or reconsideration, even if the facts are completely wrong. Traditional credit-reporting bureaus come under the Fair Credit Reporting Act, but the credit-scoring companies, whose reports are used to grant most consumer credit, are not regulated at all.

The biggest privacy problem for citizens comes from a disturbing and growing trend—data breaches. There have been numerous cases of inadvertent disclosures of consumers' personal information. Some of these involved literally millions of personal financial records that included Social Security numbers, credit-card numbers, and bank information. This threat to our privacy is also a threat to our security. In the Digital Age, we are only as safe as our computers. Bad commercial computer practices are potentially just as dangerous as mismanaged government databases.

The importance of a book like this is the light it shines on a growing challenge for our society. David points out that technology moves much faster than most of us can keep up with, but that doesn't mean that we shouldn't try.

I recommend this book to anyone who wants to try to keep up. David explains the implications of privacy in a way that is easily understandable. It's a good read for anyone, not just technologists or lawyers. Privacy is not just a legal concern; it is not just a technical phenomenon; it is an issue for all Americans.

Indianapolis, Indiana Senator Evan Bayh
July 2006

To my children: Lauren, Sam, Ben, Alex, and Becca—
you are my greatest accomplishment

Preface: The Monkey House

I've never looked through a keyhole without finding someone was looking back.

Judy Garland[1]

Technology advances society, but information technology empowers the individual. It certainly did me. Before the Net, I was a bookworm. Books helped me crawl into other people's heads and peer out through their eyes. I was an information junkie and an intellectual voyeur.

Later on, as a young cryptographic analyst in the Navy, I discovered the necessity of using computers when handling huge amounts of information. No human being could sort through the masses of signal intelligence collected during the Cold War, yet those thirty-year-old thinking machines could hear a whisper in a whirlwind, given enough processing time.

Ten years later I discovered the Internet. I was fortunate enough to be at the center of the swirling information industry, the precursor of today's commercial Internet. As waves of computers became "wired," I discovered that I could use networking to reach out to other peoples' computers and see what they saw, know what they knew, sift through their online storehouses. The early information applications like finger, telnet, Archie, and wais could access authoritative sources like the Library of Congress as well as the mundane, like a Coke machine in a computer lab in Boston (to see how many were cold). These hobbyist tools converged into a universal access protocol, http, setting the stage for the World Wide Web. On the web everything that anyone wanted to make public was.

For a junkie like me it was wonderful. The whole world became my zoo, each web site a new and entertaining exhibit. There was a voyeuristic quality about the experience; though information on the nascent web was freely displayed, flashes of the author's private thoughts still showed through, just as in books.

It took ten more years before I realized that I was also on display; I began to see my own bars. I gradually became aware of what was becoming available about me online as I sought information about others. I was divorced, and the documents became public. I was an officer of a public company (Network Solutions), and all kinds of personal information became accessible through Securities and Exchange Commission filings, including my Social Security number. Details of my house purchase popped up. Even my political contributions were searchable. Most of this information was public and had always been available in paper, but two things had changed by the end of the 1990s. The first was the digitization of everything. The second was networking. Material stored on a stand-alone computer required the questioner to be physically present to use the machine. Each separate repository of information had to be interrogated, a task that required expensive and time-consuming travel. Once computers were networked, however, the protective barriers of distance and cost melted away.

I became worried. Not about me, so much. . . . My life was an open book for several reasons. But I became concerned about society in general. The harm from unmanaged access to all this content had the potential to outweigh the benefits. I came to the profound realization that data never disappear. When information is digitized and stored on a networked computer, for all practical purposes it is eternal, even if thought deleted. Historically, privacy has been based on controlling one's own information. However, once someone's life has been sucked into the emerging mesh of interlocked computers, that definition of privacy is impossible.

The rush to digitization was quick and thorough. The analog world disappeared overnight, replaced by an ever-cheapening silicon matrix. Fifteen years of my adult life were completely contained on email. I had entire relationships splayed out on my monitor if I so chose. All my pictures were now digital, my music was MP3, my movies were on DVD, and I can't remember the last time that I wrote a letter. Yet others were collecting information on me too. Between the government and marketing companies, most of my life was being collected—far more than just credit reports and official paperwork. The trend toward centralized, managed health care wrested control of my medical information out of my doctor's hands, for example. My private life was only as secure as my computer. Computer viruses controlled by hackers and spybots managed by businesses swarmed onto every unprotected computer; the creators of these programs no longer caused havoc for kicks but stole personal information for profit.

Clearly the courts and Congress haven't "gotten it" yet. The courts have been scrupulously avoiding anything that might slow down Internet growth, and since 9/11, Congress has not shown any inclination to get involved in information protection if it constrained commercial database companies or counterintelligence efforts by the government. There has been media discussion of the legal ramifications of privacy, but the primary agent of change, technology, has largely been ignored.

I am a technologist and a businessman, and it is from that perspective that I wrote this book. Privacy is too important to be left to lawyers. As a starting point, I did a little violating of my own privacy, including running background checks and having my DNA analyzed. In a few days, I was able to put together a comprehensive report on myself from easily accessible sources. I've included a highly abridged version here. The full version was almost embarrassingly complete, with detailed financial and personal information.

Vital statistics

Age:	49
Address:	Herndon, Virginia
Birthplace:	Pittsburgh, Pennsylvania
DOB:	9/30/56
Height:	67”
Weight:	198 lbs
Hair:	Brown
Eyes:	Brown
Travels:	Canada, Italy, Spain, Netherlands, UK, BVI, Japan, Tahiti, France
Education:	BA Philosophy U of Pittsburgh, BS Computer Science U of Maryland
Veteran:	8 years as Cryptographic Interpretive Technician (Russian)
Special:	Qualified in Submarines (SS)
Family:	5 children, divorced
Source:	*Passports and driver’s license,* Who’s Who *entry, resume*

Medical

Blood type:	A+
Genetic variations:	Possible heart complications
Dental work:	Two bridges, three crowns
Marks:	Circumcised, no tattoos, small birthmark left collarbone
Surgery:	Tonsillitis
Physical:	Exercises regularly, doesn’t smoke, social drinker
Other:	Type II diabetes
Source:	*DNA test from a cheek swab, medical records from HMO*

Legal and financial

Felonies:	None
Traffic:	Two speeding tickets since 2000
Credit cards:	Amex, Visa, MC
Debt:	$230,000 mortgage, minor credit-card debt
Voted:	2000 and 2004 general election
Political contribution	$2,000 Wes Clark in 2000
Source:	*Credit reports, opensecrets.org (political-donation tracking)*

Entertainment

Books:	Mysteries, science fiction, thrillers, varied nonfiction
Music:	Jazz, blues, modern rock
Television:	Comedy and news, likes *The Daily Show*
Movies:	Varied, documentaries, comedies, foreign
Source:	*TiVo, Amazon.com records*

Online behavior

News:	*Washington Post, NY Times,* C/Net
Blogs:	Slashdot, Daily Koz, Gizmodo, boing-boing, Wired, thecoolhunter
Personal site:	www.davidholtzman.com
Blog site:	www.globalpov.com
Book site:	www.privacylost.us
Email address:	david@globalpov.com
Daily email load:	250–350 pieces, 75 percent spam
Source:	*Wi-Fi monitoring, packet sniffing*

Personality

Intelligence:	High
Myers-Briggs:	ENTP
Political leanings:	Moderate-Liberal
Source:	*Passive psychological tests, analysis of online behavior*

Threat potential

Online gambling	None
Buys subversive books	Some
Browses counterculture sites	Some
Emails known terrorists	None
Visits known terrorist sites	Never
Travels to suspect countries	Never
Uses encrypted email	Occasionally
Threat risk	Low
Source:	*Overall analysis of behavior patterns, credit reports, emails, travel history*

Welcome to the monkey house. We're the monkeys and the tourists both—the exhibitionist and the voyeur. Each bar in our cage is smelted from the same metal—technology. If you want privacy, pay cash, send postal mail, use a television antenna, and don't travel by airplane or leave the country. That strategy might work right up until the inevitable national ID card is mandated. Of course, you'll give up many of the benefits of our society; renting cars requires a credit card, for example.

Technology is wonderful. It extends our life span, feeds the poor, and helps us thrive in harsh environments like tundra and deserts. Just as the railroads opened up the United States in the nineteenth century, networked smart devices are opening up new business areas in the twenty-first. But there are consequences. Building the railroads killed off the buffalo. What will building the Information Superhighway kill off?

Technology has changed our culture: how we communicate and how we don't. It has affected our ability to control our personal information: who sees it, what they see, what they do with it. Our privacy is already lost, whether we know it or not. Whether we can find it again is still unclear.

Herndon, Virginia David H. Holtzman
July 2006

Acknowledgments

My extremely competent, vivacious, and super-smart assistant, Beth Watson, has helped me in innumerable ways, not least by keeping the home fires burning when I disappeared to write this book. Plus she keeps my cat, Helen, happy when I'm away.

My extraordinarily intelligent and articulate researcher, Moya Mason, kept me on the straight and narrow with timely and thorough material as well as encouraging words when I needed them the most, and in the process proved that not everything in Newfoundland is cold.

Dorothy Hearst and Jesse Wiley at Jossey-Bass championed this project, and Jesse spent many weekend hours working with me on the editing.

My agent, Grace Freedson, stuck with me and sold this book, even when prospects were less than rosy. She always cheerfully took a call, even for stupid questions.

Friends of many decades have always been supportive of my writing: Jim and Kathy Carr, Rich and Cindy Burkhart, and Cathy, who supported me early on.

Helpful readers and friends gave me feedback. Mike Sheridan and Rick Garvin offered helpful insight into both privacy and technology. Tim Skinner from SRA was great at reviewing the legal bits. My old friend Hatte Blejer read material, kibitzed, and made some good introductions. Jack Lewis often talked to me about the law and history at diners and helped more than he realized. My lawyerly daughter, Lauren, always made time for me that she didn't have. My lawyer, Max Miller, was always glad to share his opinions and to occasionally listen to mine. Travis Van was very generous with his time and public relations advice.

Tara gave me the great gift of believing in me.

The beautiful Canadian province of Prince Edward Island nurtured me while I wrote, entertained me when I was bored, and challenged me when I got too comfortable.

To curmudgeons everywhere, and you know who you are: keep fighting the good fight.

Introduction

How and Why Our Privacy Is at Risk

> *The Central Intelligence Agency is committed to protecting your privacy and will collect no personal information about you unless you choose to provide that information to us.*
>
> *Central Intelligence Agency*[1]

Privacy is a universally cherished prerogative that isn't much of a right at all. Few laws protect our seclusion, and they weaken every year. Our privacy is shrinking quicker than the polar ice cap; technology is eroding it faster than the legal system can protect it. This trend cannot be reversed in any obvious way. Privacy, as we know it today, is lost.

At its most basic level, privacy is about information control—who owns knowledge about us? The German term *informationelle Selbstbestimmung*, which means "informational self-determination," suggests that we control our own information. But today our information has slipped out of our control, and as a result we have lost our privacy. This loss has been caused by the most significant society-impacting science of our generation—computerized technology. My intention in writing this book is to explain the connection between technology and privacy and to speculate about where things might be headed.

This book is not written just for privacy advocates or for technologists, however. Rather, it's for all who are disturbed about the growing amount of data available on them, about who's doing the collecting, and about what the collectors are going to do with all that personal information. It's also for those who are concerned about the growing number of exceedingly well-publicized privacy violations and who are wondering how many other incidents haven't become public. It's hard not to notice the unending stream of news stories describing one egregious privacy violation after another: companies losing the financial information of millions of customers, a civil servant in the U.S. Department of Veteran's Affairs having a laptop stolen that contained personal information on nearly every American who's ever served in the military, a Boston newspaper wrapping papers in printouts of its customers' credit-card numbers. These stories are all documented and discussed in this book. They are, in themselves, a testament to the effect of technology on our privacy.

Privacy Lost is also for people who get nervous about privacy-hostile government actions like the Patriot Act. These counterterrorist programs give millions of government agents a get-out-of-jail-free card, permitting electronic probing of U.S. citizens on a scale that would have made even J. Edgar Hoover blush. None of these government activities would be possible without the availability of sophisticated information technology like data mining, which is used to sift through the rapidly growing data heaps of our newly digital civilization.

Our data include our emails, photographs, medical results, travels, and purchases. Eventually every transaction will be stored somewhere digitally and therefore will be accessible to a persistent searcher. As a rule of thumb, according to Moore's Law, digital storage devices get twice as powerful every eighteen months for the same price.[2] However, the cost of human labor stays the same. Therefore, it's cheaper to buy additional disks than to figure out what to delete. Digital data never disappear, and searching technology like Google is good enough that all information will be found. Like Poe's raven, our past may come back to haunt us when we least expect it. It's no coincidence that emails have been the key evidence at the center of most political and financial scandals since the mid-1990s. Data last forever. Privacy does not.

The digital universe parallels the one we live in, except it's littered with lost and forgotten information, data, and facts—a silicon twilight zone. Each of us has a twin in this universe, a digital Doppelgänger that reflects our lives and experiences and will be around when we're long gone. This electronic simulacrum shares our birth date and Social Security number and all our specifics: what we've bought, where we've traveled, the state of our health. Even though we may zealously guard our personal information, our double will tell anyone about us because that electronic twin is not under our control.

It's impossible to walk through this modern world without leaving behind indelible footprints in its silicon sand. Most financial activities, for example, leave a digital imprint somewhere because a record of every cashless transaction goes into someone's database. A whole industry has sprung up around selling and storing personal information about our behavior and activities. Each bit seems innocuous, but, in aggregate, this electronic montage provides a frighteningly detailed history of what we do, when and where we do it, and whom we do it with. As you'll read about later in the book, computer software is also beginning to make some good guesses as to what we think. Do we want new laws protecting our privacy from these intrusions, or are we willing to put up with them to have a better shopping experience?

We are also being tracked by our gadgets, such as cell phones (even when they're off) and Geographic Positioning Systems in our cars. A new technology called Radio Frequency Identification enables small chips to be hidden in packages, books, and even clothes. These little devices know essential information about us and can be surreptitiously interrogated from thirty feet away. Soon this technology will be prevalent in our lives. Are we willing to live without our gadgets if we know that they erode our privacy?

In addition, we're under constant observation by computerized sensors. In most modern cities our picture is snapped dozens of times a day by surveillance cameras. License-plate-reading and face-recognition programs are matching these pictures to names. So far, the worst result of this capability is the automatic issuing of speeding tickets, but additional uses will be developed. Will we ever get used to being watched twenty-four hours a day?

Even our bodies are being tagged, analyzed, and stored for future cross-reference. A simple cheek swab or drop of blood is enough to analyze our DNA, which indicates our tendency to inherit certain health problems. Health care providers and employers would naturally like to screen out those of us with genetic problems to keep down the overall cost of medical coverage. As a result, our genetic road map sometimes makes it difficult to get insurance or even a job. Several U.S. states and some nations are also building sweeping databases of citizens' DNA information for future use. Are we as a nation okay with a genetically biased health care system?

Some of these capabilities have been available for years, but weren't threatening because they were too expensive to be widely deployed on a large scale. Unfortunately digital technology is now cheap, very cheap—and it is getting more so every year. The best protection against wholesale privacy abuse has always been the cost. However, this fiscal barrier is effective only against physical, not virtual, items because the economics are different in the digital world. For example, the profitability point for spam (junk email), regardless of the volume, is insanely low compared with the break-even point for postal mail because the incremental cost per item of spam is close to zero. The cost of a postage stamp is a natural brake on the proliferation of junk mail. There's no equivalent friction for email. America Online (AOL) has instituted a program called Good Mail, which purports to cut back on spam by charging mass emailers who want to send to AOL recipients. The theory is that the payments will deter spammers. Are we willing to pay for all our email in the future, or is spam a nuisance that we're willing to put up with for free stuff?

Our lives are represented electronically in databases across the world. The decentralization of this information makes it difficult to regulate. These computerized storehouses are necessary for so many business and governmental purposes that most people do not view them as a threat. And the political climate is not favorable for changing the situation. These information tools are seen as important weapons in our nation's arsenal. We live in a turbulent time. All but the most snugly bundled liberties have been whipped by the wind of fear that has blown through the United States since the attacks on the World Trade Center and the Pentagon in 2001. The natural balance between national security and privacy has tipped precariously toward security. Are we as citizens in a democracy willing to grant our government indefinite powers to anonymously invade our privacy if it makes us safer? What if we only think it makes us safer? Should government be limited in what it can see and do with the information it collects on us?

But it's not just government tracking citizens. Every group that uses computers incrementally erodes the privacy of its constituents when it starts keeping lists. The newspapers are full of privacy-related stories, ranging from abuses of the Patriot Act to President George W. Bush's authorization of possibly illegal domestic surveillance. Every few weeks, we hear about massive data breaches caused by careless data handling by private companies, while others, like Google, are holding enormous amounts of personal information—so much so that the government is trying to forcibly get access to it. The privacy situation in the United States and Canada is at an Orange Alert level and will not be going back to Yellow again in my lifetime.

Information gathering is the new arms race. Superior knowledge gives the knower the ability to predict what's going to happen. And a lot of money can be made from predicting the future. Governments collect personal information to spot subversion. Merchandisers use it to target or persuade consumers. Financial institutions assess creditworthiness. Politicians find donors. Terrorists hatch plots. This fungible information is easily transportable and can be converted into cash in any currency in the world. You often hear the old legend that our body is worth $4.50, stripped for parts. Our digital identity is worth far more than that. Information about us is worth $20–$50 to a business trying to sell us a product and is worth many thousands of dollars to an identity thief.

Our ethical sense is not yet fine-tuned to the changes brought about in the privacy arena by technology. Nor is our legal system. Western society views the universe through the lens of science. In this model, technological progress is ideologically pure and apolitical. Information is just data, just facts. We find it hard to accept the idea that knowledge can be dangerous. We don't have a cultural perspective that supports this idea, unlike people living under repressive regimes, who know that information, true or not, can get them jailed or even killed. This intellectual blind spot, refusing to believe that control of information should be regulated, is one of the major reasons why the United States has no comprehensive privacy laws today.

This book is different from other books about privacy because it's centered on technology, not the law. In this century, technology moves fast and sets the pace for social issues, leaving the law lagging behind. Legislation works best when fixing a problem that has clearly definable boundaries. However, information technology itself and the ways in which it's harvested and sold are developing at such a rapid rate that new laws are likely to address technology that industry has already abandoned. Congress has historically done a miserable job at providing protection against future problems, even the slow-moving ones. These kinds of problems cannot be resolved in Congress, just as they cannot be fixed solely in the courts. The law will always lag behind the technology.

Privacy legislation has also been difficult to enact because the damages from privacy loss are not clearly understood. To many people, privacy issues are linked to immediate annoyances, like telemarketing phone calls. Because the consequences are not directly apparent, the hardest situations to regulate in a democratic society are those, like smoking or environmental protection or control of information, that cause long-term damages.

Privacy Lost is divided into six parts. The first part is about the damages caused by the loss, including what I call the Seven Sins Against Privacy. The second part reviews some of the history behind our concept of privacy, how related technology has evolved, and how new technology leads to new invasions of privacy. The third part discusses the context of privacy; it includes a chapter on the legal basis in the United States, another on how privacy relates to identity, and a third on how the idea of privacy varies culturally. The fourth part deals with the mechanics of snooping, databases, surveillance, and networking technologies. The fifth part describes the snoopers themselves, the marketing companies and the government. The last part suggests some ways you can slow or staunch your loss of privacy. The Recommended Reading list at the end of the book provides suggestions for further reading on the topics covered.

Throughout the book you'll find numerous stories and examples, culled from newspapers, magazines, and the Internet, about how privacy invasions hurt people. Although privacy violations happen to celebrities more often they affect normal people, the ones who mistakenly think that the government or the law is protecting them. If you take one idea away from reading this book, it should be that you have the right to control information about yourself. Even if the law doesn't recognize this right, you should. Privacy is, in a legal and practical sense, based on our expectations. Even though Americans have no explicit constitutional right to privacy, most think that we do. People are constantly surprised that there is no mention of privacy in the Constitution. Government is, in fact, powerless to regulate the availability and flow of personal information; even more dangerously it believes that it can. This book discusses some steps individuals can take to protect themselves instead of relying on the government.

Polls indicate that people are willing to give up their privacy in exchange for safety. However, the damage caused by the loss of privacy could reach into other areas of our lives as well. For instance, the ability to keep our thoughts and opinions to ourselves gives us the freedom to exercise our other rights without fear of retribution. Privacy allows us to peacefully exercise other rights such as freedom of speech and religion and the right to bear arms. The answer to the question of who controls information about us touches many other areas such as intellectual property and genetic engineering. It may be the most important domestic policy question of this century.

A long-term danger to society resulting from a total loss of privacy protection is that our creative and freethinking culture could be replaced by one that rewards fear-driven mediocrity. It happened on a smaller scale in Hollywood after the Senator Joseph McCarthy hearings and was part of daily life in the Puritan colonies. Those who know that they're watched don't call attention to themselves, and thus they disappear. The economic might of Western innovation cannot be sustained by a nation of ghosts.

Part I

Privacy Invasions Hurt

Many, maybe most, people aren't worried about their privacy. Isn't it our right, already protected in the Constitution? The short answer is no. This part explains privacy by describing what happens when it gets violated: how privacy violations affect our culture, our government, and, most important, us. Chapter One breaks privacy violations into seven categories and provides accompanying "commandments" for improvement. Real examples of privacy problems are included to help explain each sin. Chapter Two describes how a lack of privacy can harm civilization in general and a country specifically.