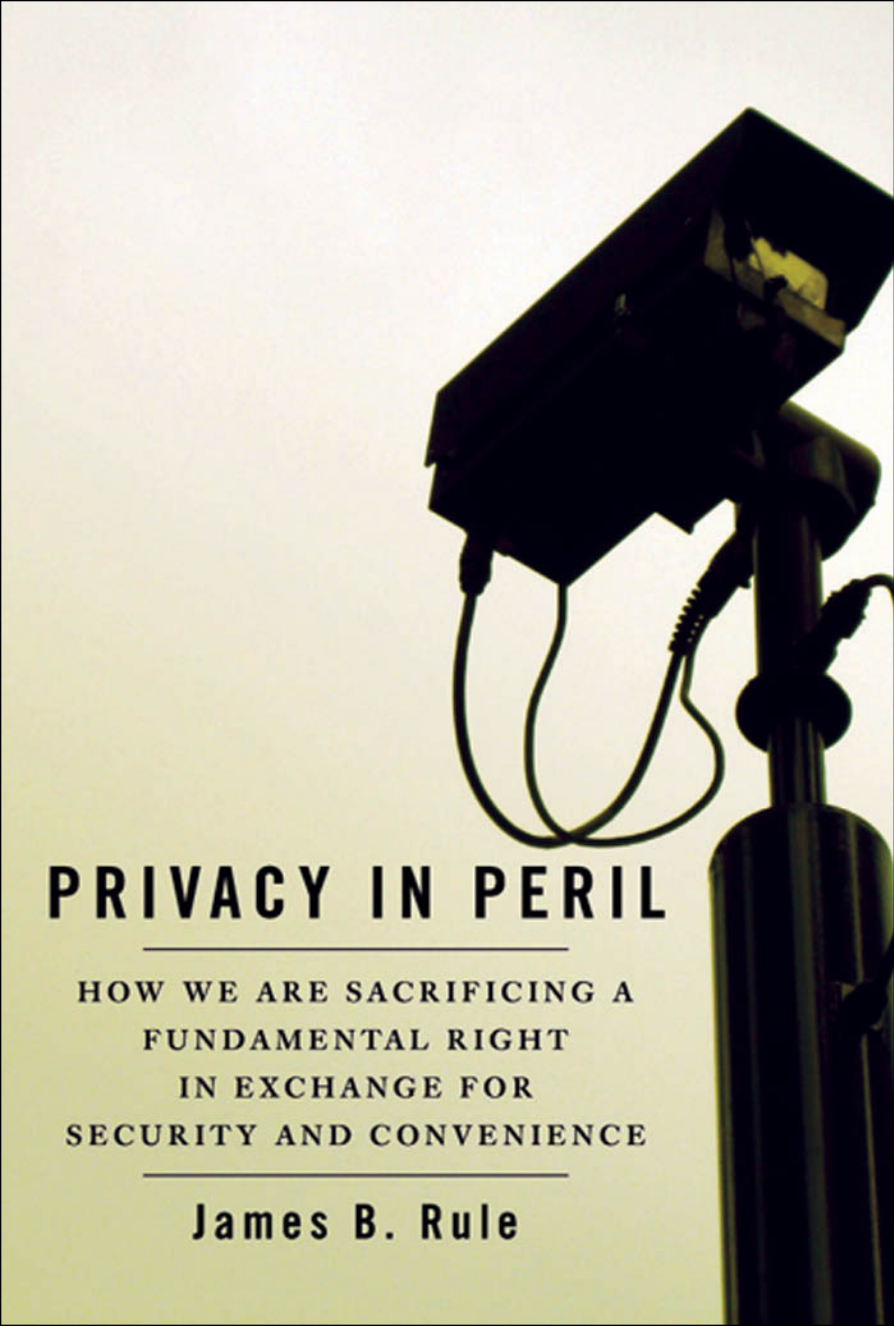

PRIVACY IN PERIL

HOW WE ARE SACRIFICING A FUNDAMENTAL RIGHT IN EXCHANGE FOR SECURITY AND CONVENIENCE

James B. Rule

Privacy in Peril

This page intentionally left blank

Privacy in Peril

James B. Rule

OXFORD
UNIVERSITY PRESS

2007

OXFORD
UNIVERSITY PRESS

Oxford University Press, Inc., publishes works that further
Oxford University's objective of excellence
in research, scholarship, and education.

Oxford New York
Auckland Cape Town Dar es Salaam Hong Kong Karachi
Kuala Lumpur Madrid Melbourne Mexico City Nairobi
New Delhi Shanghai Taipei Toronto

With offices in
Argentina Austria Brazil Chile Czech Republic France Greece
Guatemala Hungary Italy Japan Poland Portugal Singapore
South Korea Switzerland Thailand Turkey Ukraine Vietnam

Published by Oxford University Press, Inc.
198 Madison Avenue, New York, NY 10016

www.oup.com

Library of Congress Cataloging-in-Publication Data
Rule, James B., 1943–
Privacy in peril / by James B. Rule.
p. cm.
ISBN 978-0-19-530783-2
1. Privacy, Right of. 2. Privacy, Right of—United States.
3. Privacy, Right of—Cross-cultural studies. I. Title.
JC596.R85 2007 323.44'80973—dc22 2007018610

9 8 7 6 5 4 3 2 1

Printed in the United States of America
on acid-free paper

To privacy-watchers everywhere

This page intentionally left blank

Contents

Preface ix

■ Part I: The Making of an Issue 1

The Tensions of Privacy and Disclosure 6
Privacy Regimes in Turmoil 13
Blaming Technology 18
The Idea of Privacy Protection 22
Legislating Privacy Protection 28
Spreading Shadows 32
Constraints and Countercurrents 34

■ Part II: Government Surveillance 39

Government Surveillance in America 43
Parallels Abroad 64
The Coalescence of Government Surveillance 82
Conclusion 91

■ Part III: Personal Data in the Marketplace: Credit, Insurance, and Advertising 93

The United States: A Virtually Free Market for Personal Information 97
Markets Abroad: The American Model versus Privacy Constraints 114
Surveillance in Motion 132
Safe Harbor 136
Some Rare Privacy Victories 139
Conclusion 141

■ Part IV: The Future of Privacy 143

Privacy Protection: The Official Response 147
Privacy Codes: A Balance Sheet 150
Origins of the Conflict 156
The Destination 162
Collapsing Resistance? 164
"Needs," "Purposes," and "Consent" 168
Some Uncomfortable Futures 174
Ground to Stand On 182
Conclusion: Where Do We Go from Here? 190

Appendix 203

Notes 205

Bibliography 211

Index 217

Preface

My learned friend—a professor of law—has little patience for worries over the beleaguered state of privacy in today's world. One can hardly expect all worthy values to flourish in all settings, he points out. The right to bear arms may have made sense in a sparsely populated agrarian society, where nature was more dangerous and armaments less destructive. But today's conditions render values of self-reliance in weaponry impossible to realize without intolerable cost. No more do most of us really want to inhabit a world predicated on the values of courtly love or the Sermon on the Mount—much as we may admire these virtues at a distance. In the information society we now inhabit, says my learned friend, privacy has simply become an anachronistic value. Blocking the free flow of personal data, like that of any other information, makes about as much sense today as outlawing steam power during the industrial revolution. For this man, as for many others, the state of privacy in today's world is hopeless—but not really serious.

Other friends, feeling less complacent or more vulnerable, embrace the opposite diagnosis. For them, our steady loss of control over information about ourselves is an evident reality and the value of the losses incalculable. They note—and the first friend would readily agree—that nearly every element of a normal life in today's world leaves its computerized traces somewhere.

Moreover, appropriation and use of the resulting streams of personal data have become basic prerogatives of all sorts of public and private organizations, from law-enforcement agencies to marketing companies. From reliance on the Internet, to access to medical care, to ordinary credit transactions, our lives are documented in detailed and revealing ways, and the resulting troves of personal data are used for purposes not necessarily of our making. Worse, our ability to shape these uses of "our" data often appears minimal if not absent. But as in the complacent version of this story, the forces responsible for these developments appear well beyond anyone's ability to influence. For those who adopt this latter view, the prospects for privacy appear so serious as indeed to be virtually hopeless.

I am writing this book in hopes of improving on these broad-brush, categorical conclusions. Privacy is most certainly under pressure in all sorts of ways. Every day, the news brings a new harvest of horror stories—phone conversations, e-mail messages, and website visits surreptitiously recorded; sensitive medical records disseminated far and wide; consumers' credit charges abruptly raised through automated monitoring of their financial situations; air travelers turned away at departure gates because their names appear on lists whose origins cannot be explained; and on and on. But what is the larger trajectory of the trends at work here, and what can anyone expect to do about it? Any serious response to such questions requires some vision of the social, economic, and technological chemistry fueling pressures on privacy.

It will not do, I argue, simply to blame "technology" for the fact that an ever-increasing array of interested parties now routinely monitors what once would have been bracketed as private information. In fact, the original appetites of public and private organizations for personal information date to well before the advent of computing and other now-familiar technological wonders. Nor should we look to any elegant "technological fix" as an escape route from the resulting dilemmas. What we face instead are uncomfortable and far-reaching choices among conflicting interests and basic social values. Demands for privacy, we need to acknowledge, collide with pervasive pressures for efficiency and control over human affairs. Though nearly everyone agrees that privacy in some sense is a good thing in itself, it is by no means clear that it is good enough to prevail over the values increasingly juxtaposed against it.

The term "privacy" means many different things. This book focuses on privacy issues arising from institutions' reliance on data systems to monitor

the lives of ordinary citizens. These activities, I argue, make up a master social process utterly distinctive to the advanced societies of the late twentieth century and beyond—a process I term *mass surveillance.* Surveillance in this sense has become a pervasive activity among both government and private organizations, as they rely on the details of people's records to shape their dealings precisely to the circumstances of each individual they confront. By the early twenty-first century, mass surveillance has become so basic to everyday life that its extraordinary features pass almost unnoticed.

Over the last several decades, concerns about the privacy-eroding effects of mass surveillance have grown acute in all the world's more prosperous countries. These concerns have made privacy protection a global public issue. By the first decade of the twenty-first century, every liberal democracy has formulated privacy codes to protect citizens from unregulated appropriation of their personal data. These policies, and the developments generating demand for them, make up the subject of this book.

As it happens, this history of privacy as a public issue corresponds with my own involvement with it. As a graduate student in the late 1960s, I grew fascinated with what then seemed novel and revealing forms of social change—the rise of mechanisms like identity cards, credit cards, and other systems for regulating organizations' treatment of people by linking them with their records. These developments seemed to me essential in the rise of a more impersonal, anonymous world dominated by large bureaucracies. The personal record-keeping involved in these systems was then only beginning to be computerized, and it was both qualitatively primitive and quantitatively undeveloped by the standards of today. But as early as four decades ago, one could sense rising tensions between institutions' appetites for more and more personal data, and ordinary people's efforts to exercise some control over such use.

Of course, it would be absurd to suggest that transition to a world shaped by institutional use of computerized personal data necessarily means a *net* loss for privacy—if indeed such summary judgments are meaningful. One reason why institutions come to rely on formal records—from those held by tax authorities to those governing access to consumer credit—is that face-to-face demands on privacy decrease in a world where personal acquaintance matters less. The relatively more mobile, cosmopolitan, impersonal world we now inhabit actually liberates us from privacy demands of family, neighborhood, and community. Most of us would not want to return to a world of relentless, face-to-face local pressures on privacy, even if it were possible to do so.

But the concerns engaged by impersonal, bureaucratic, large-scale demands for personal data underlying today's privacy controversies compel attention in their own right. Do we want to recapitulate the forceful, privacy-invading qualities of small-town life on a national or global scale? Do we want to be monitored by institutions capable of abusing data on literally millions of persons at a time? Can't we find ways of enabling people to maintain a measure of control over information about themselves, while still dealing with the vast government and private-sector institutions that demand so much of that information? If it is indeed *bureaucracies* that foster and profit from these new, impersonal flows of personal information, aren't there ways of forcing them to limit the extent of these attentions?

Such nagging questions ultimately led to the writing of my first book—*Private Lives and Public Surveillance* (1973)—a study of five British and American systems of mass surveillance. As I was preparing that work, friends and colleagues often seemed to find it hard to understand how the study of record-keeping in organizations as diverse as the American credit card industry and the British police added up to a coherent subject matter. But publication of *Private Lives* benefited, ironically, from coinciding with the Watergate debacle, in which the Nixon administration's abuse of personal data from government files provided a major theme. Since then, concerns over large-scale, bureaucratic surveillance have not required much justification or explanation. The salience of privacy concerns has risen and fallen in public opinion. But their status as an authentic public issue has remained unquestioned.

During the years since publication of that first book, my interests turned to other subjects altogether. But like the perpetrators in those hackneyed murder mysteries, I have often found myself returning to the scene of the original action. On each new encounter with the subject, I have been fascinated anew.

To rationalize these intellectual revisits to an earlier obsession, I assured myself that it wasn't *really* the same subject as before. Information technologies, as everyone notices, never cease to evolve. Political climates are transformed, as witnessed by the recent proclamation of the "War on Terror"; new realms of experience as astounding as cyberspace appear. Perhaps even more striking, the fertile imaginations of efficiency-minded government officials and profit-seeking entrepreneurs continue to identify new links between personal data and evolving techniques for dealing with the people concerned. Thus we have prices offered to Internet customers based on their past histories

of Internet purchases; or security scrutiny at airports based on one's record of telephone calls; or insurance rates based on one's credit history. The headlong stream of such transformations conspires to make privacy seem an entirely new ballgame every decade or so.

But these observations, accurate as far as they go, are ultimately evasions. In fact, many of the original questions that drew me to study these processes have only grown more acute over time. How can we characterize the essential forces driving bureaucratic appropriation and use of personal data? What trajectory, in the longest historical view, are these developments following? Do they portend a world of total un-privacy and relentless control or regimentation—either benign or otherwise? How much choice, if any, do we have in reacting to them?

Let us not insist on reassuring news. One possibility, we need to recognize, is that privacy is indeed on the way to becoming an anachronistic value, just as my learned friend would have it. We could be headed toward a world where all personal data of interest to major institutions are recorded as a matter of course and circulated automatically among interested parties. In such a world, citizens might have the right to correct erroneous information about themselves or challenge unwarranted conclusions based on it—but never to interfere with its efficient institutional collection and use. That world could arguably be safe, predictable, and prosperous—just not particularly private.

It is the appeal of such a world that relentlessly undercuts efforts at meaningful privacy protection. Much as nearly everyone publicly deplores the erosion of privacy, the quest to monitor and control social processes is no less pervasive. We moderns cannot shake the conviction that, by knowing *just a bit more* about this or that realm of social reality, the world will become a better place. It is this conviction that underlies efforts to record new forms of personal information, to share such recorded data more widely, and to use shared data to shape new determinations on the people concerned.

Consider plans announced by the Bush administration in 2004 to centralize and computerize virtually all medical data in America. The aim was to create a single archive of all patients' medical visits, diagnoses, treatments, and prescriptions—a source of vital information that would be available to caregivers at virtually any place or time.

The "needs" for such a system hardly require stating. Even a casual look at current practice reveals massive fragmentation and incommensurability of medical data—with bits of crucial information scattered unpredictably across

places and institutions. The expense of tracking, requesting, and transmitting such data is staggering. Worse, patients often fail to get appropriate treatment—or experience treatments that are actually life-threatening—because their full records are unavailable at a crucial moment. Many of the more than 50,000 deaths each year from medical errors might be avoided, observers speculate, through fuller information. And a truly comprehensive pool of *all* patient histories could lead medical researchers to insights on the origins of diseases that until now defy medical understanding.

But consider the full implications of taking this step. Once a truly comprehensive system of medical information is known to exist, we will have entered a qualitatively new surveillance environment. From that moment, every interested party will be able to assume that *all of every American's medical history is indeed available at a single point.* One's medical record will become like one's tax returns—an authoritative document whose existence is known to everyone. And that will mean that every American institution claiming a "legitimate" interest in Americans' medical situations—or indeed simply their whereabouts—will seek access to that central resource.

Law enforcement agencies will seek such access, to develop evidence on responsibility for unsolved crimes. Data sought here would range from DNA profiles to reports of the whereabouts of suspects when crimes were being committed. Parties to divorce proceedings and other civil actions will demand access to buttress their claims about their partners' movements or sexual habits—or to defend against such claims. Courts and public agencies seeking to enforce child support obligations will crave recourse to the files, to pinpoint the locations of parents avoiding their court-ordered responsibilities. Sellers of medical and life insurance will demand the "consent" of insurance applicants to see their full records, as a condition for entertaining the applications—consent that no applicant will be in a position to deny. Schools and other institutions charged with the care of children will no doubt want to tap any psychiatric records of potential employees, to ensure against hiring anyone who might pose a danger to their charges.

And of course, those prosecuting the so-called War on Terror will demand recourse to any medical data that might, conceivably, identify potential terrorists or their supporters. Remember, this is a measure proposed by an administration that has already mobilized government surveillance to troll through Americans' telephone records, financial transactions, and choices of

reading matter in libraries and bookstores. Would medical data be any less subject to such demand for access?

But let us not imagine that pressures emanating from creation of a system like this one would be attributable solely to the political tendencies of any one administration. In fact, they are ingrained in today's institutions, and in our expectations of them. So long as we regard law enforcement agencies, insurance companies, courts, schools, and other institutions as essentially legitimate in the ends they pursue, it is very difficult to deny them means to pursue those ends more effectively. Yet as more personal information becomes available from more sources, the net impact of their demands for it multiplies. Opting for privacy—that is, precluding access to crucial personal data—appears tantamount to slamming the door on organizations that are simply striving to do what we have always expected them to do.

I want to argue that *there is no natural limit* to the demands for personal data that arise in response to such expectations. That is, no form of personal information is inherently so personal, so intrusive to gather, or so private as to preclude monitoring by government or private institutions. The never-ending stream of innovation in management strategy and information technology ensures as much.

Nor does the fact that institutions already maintain access to vast amounts of such data warrant confidence that the underlying appetites might, finally, be sated. On the contrary, surveillance feeds on itself. The more ways of knowing about people that can be perfected, the more opportune it becomes to know more. The reasons for such self-reinforcing demand for personal data do not lie mainly in conspiratorial intent. They arise instead from deep-seated expectations that organizations will always make the most of available opportunities to master the uncertainties of human affairs.

Thus, I hold, the only limits to endless erosion of privacy are those created by human intervention—that is, by laws and policies that "just say no" to endless extension of institutional surveillance. But does public support for such measures promise to withstand the potent social, political, and economic chemistry generating pressure in the opposite direction?

Any answer to such a question requires a view transcending specific privacy controversies and any one country. Privacy first burst forth as a public issue in the United States. But the issue is now global, and responses to it have evolved somewhat differently across countries. Some forms of surveillance

that have flourished in America have thus far been blocked by strong privacy measures elsewhere. Perhaps other countries' stories provide hope for better solutions than America has yet realized. With an eye to such possibilities, the following pages compare the state of privacy and privacy policy in America to its parallels in Britain, France, Canada, Australia, and other countries.

Essential to these comparisons is assessment of *directions of change* across countries. Pressures on privacy—from government interests in tracking terrorists to commercial desires to track the habits of consumers—are global phenomena. The technological and management strategies available to surveillance interests in one country are eminently exportable to any other. American organizations, it turns out, have labored mightily to promote such export. How successful have been the resulting pressures to extend American-style surveillance to other countries? How resilient have countries with strong privacy measures been in resisting such pressures? Is there a clear alternative to continued erosion of privacy along the most disturbing lines of American practice? Or are all countries ultimately traveling on the same global conveyor belt, headed to a single, privacy-free destination?

In short, have the world's emerging privacy-protection codes made much of a difference? Have they in any significant way stemmed the formidable forces working against privacy? Can we say that privacy is at all better protected than it was, say, in 1973? Or, as one sometimes suspects, have we arrived at a point where we have more extensive privacy codes—but less privacy? And what reasonable alternatives are there to visions of the state of privacy as hopeless-but-not-really-serious and those depicting it as so-serious-as to-be-virtually-hopeless?

In weighing these matters of value and conviction, candor is essential. Like most people who write about privacy, I see it as an endangered value. But it is abundantly clear that other thoughtful observers hold widely differing degrees and forms of concern on these matters. Some—my learned friend the law professor, for example—find competing values so important as to be well worth what I would find intolerable sacrifices in privacy. And indeed, the most earnest privacy advocates themselves often differ on precisely how great a cost ought to be held bearable, to protect individuals' interests in the uses of "their" information. For my part, I have labored mightily to draw careful distinctions between my own preferences—reasoned, I hope—for policy and

action, and matters of fact. Accordingly, I hope that readers who take positions different from mine on these issues will nevertheless find the documentation in this work reliable and thought-provoking.

In fact, underlying differences of conviction actually represent an opportunity for deeper understanding, if only we can be frank about them. One source of conflict on privacy issues, I will argue, is clashes of ultimate value—of irreducible "tastes" for competing visions of a good life. Some of us prefer a more secure, more efficient, less dangerous world, in other words, whereas others prefer more privacy, even at the cost of living less comfortably or more dangerously. Sometimes the best we can do about such often profound differences is to identify them for what they are and be honest about their implications.

But we can often do more, as well. We can carefully trace the implications of pursuing our often differing values through their complex repercussions in today's complex social world. If we prefer more privacy, in other words, what *costs* are we willing to pay to satisfy that need? And if we feel that more efficiency indeed warrants expenditure in the coin of privacy, how much are we ultimately willing to spend? Such assessments need to take account of the fact that more and more of life is coming under the scrutiny of surveillance systems, regardless of how we feel about the matter. If, as I believe, the prevailing direction is toward more intense, more comprehensive, and more multifarious surveillance, we need to weigh how far these trends should go.

At some stage, I hold, nearly anyone would want to call a halt—perhaps even my learned friend. Virtually no one, in other words, really wants to live in a world where *every* private moment, and *every* personal datum, are subject to institutional monitoring. At that point, from nearly any value perspective, surveillance clearly goes too far—even when devoted to the most worthy purposes. But how could informed debate define such a point? And having done so, what practical measures might suffice to make it a reality?

I hope at least that no one will accuse me of having portrayed questions like these as simpler than they are.

More than most works, this study has drawn support from an enormous variety of institutional and individual sources. This support has taken many forms, from academic fellowships and grants through formal interviews and off-the-record conversations, to critical readings of the work in progress. I know that I cannot do justice to all those who have helped, but I must try.

In terms of institutional support, Stony Brook University, my home institution until the end of 2006, granted me sabbatical leave in which much of this writing was completed during the 2005–06 academic year. Early phases of this work received crucial support from the National Science Foundation, Program on Social Dimensions of Engineering, Science and Technology, award number SES9817957. A fellowship at the University of New South Wales Law Faculty in Sydney, Australia, provided a congenial and productive setting for my work there in September 2003. The Remarque Institute at New York University and its director, Tony Judt, furnished a lively intellectual home-away-from-home in the form of a fellowship in the spring of 2004. The Center for Advanced Study in the Behavioral Sciences at Stanford, California, provided the ideal setting for final writing and editing of the text in 2005 and 2006. My special personal gratitude goes to Prof. Doug McAdam and Prof. Claude Steele, the former and current directors, for the invaluable opportunity to work at the Center—and to Tricia Soto and Jason Gonzalez, Center librarians, for unstinting and sophisticated research support.

Perhaps the most crucial institutional debt is to the John D. and Catherine T. MacArthur Foundation for a Research and Writing grant that launched the work in earnest in 2003 and supported it directly and indirectly in the years to follow. There are simply too few fellowships of this kind, that support both serious data-gathering and sustained intellectual reflection aimed at creating statements that go beyond simple research reports.

The research itself has taken a variety of forms, from reliance on websites and other documentary sources; to e-mail exchanges with informed observers and participants in the systems discussed here; to formal interviews with members of record-keeping institutions and countless more casual exchanges with privacy-watchers in many different settings. Particularly crucial has been the willing cooperation of those who have generously taken time out from their busy schedules to help me get a grip on their special areas of expertise.

In the United States, these expansive and thoughtful people include Sheri Alpert, Jerry Berman, James Dempsey, Denise Deneaux, Robert Gellman, Beth Givens, Evan Hendricks, Chris Hoofnagle, Jerry Kang, Cedric Laurant, Steve Nunez, Joel Reidenberg, Priscilla Regan, Marc Rotenberg, Ari Schwartz, Paul Schwartz, Robert Ellis Smith, Peter Swire, Lee Tien, officials of the Department of Homeland Security, and the office of U.S. Senator Charles Schumer.

In Australia, they include Roger Clarke, Chris Connolly, Tim Dixon, Graham Greenleaf, Katherine Lane, Nicola Mckilligan, Nigel Waters, and officials of the Office of the Federal Privacy Commissioner, the Australian Direct Marketing Association, the Australian Finance Conference, and Baycorp Advantage.

In Canada, they include Ann Cavoukian, Philippa Lawson, Stephanie Perrin, Jacques St. Amant, Marie Vallee, and officials of the Canadian Life and Health Insurance Association, the Canadian Marketing Association, Equifax Canada, and the Ontario Information and Privacy Commissioner's Office.

In France, they include Etienne Drouard, Serge Gauthronet, Marie Georges, Celine Hurel, Meryem Marzouki, Andre Vitalis, and officials of the Association Française des Sociétés Financières, the CNIL, Consodata, and the Union Nationale des Associations Familiales.

In Great Britain, they include David Banisar, Casper Bowden, Ian Brown, Tony Bunyan, Louise Ferguson, Benjamin Goold, Ben Hayes, Gus Hosein, Jonathan Kay, Alix Rule, Paul Thornton, Alasdair Warwood, and officials of Equifax, Insurance Database Services, Ltd., Quality Training and Consultancy, and the UK Information Commissioner's office.

Elsewhere in the world, crucial information and insight has come from Diana Alonso-Blas, Rosa Barcelo, Lee Bygrave, Leonardo Cervera Navas, Wolfgang Kilian, Whon-Il Park, Spiros Simitis, and Ivan Szekely.

This listing is far from complete. I am touched to have been on the receiving end of so much conscientious input from supportive privacy-watchers who have done everything possible to help make this work as well informed as possible. This holds particularly where those concerned obviously would not endorse all my conclusions and interpretations but have nevertheless exerted themselves to share their views clearly and thoughtfully.

As always, responsibility for the results lies strictly with the author.

Port Jefferson, New York
December 2006

This page intentionally left blank

Privacy in Peril

This page intentionally left blank

Part I ■ ■ ■ ■ ■

The Making of an Issue

. . . the protection afforded to thoughts, sentiments, and emotions . . . is merely an instance of the enforcement of the more general right of the individual to be let alone. It is like the right not to be assaulted or beaten, the right not to be imprisoned, the right not to be maliciously prosecuted, the right not to be defamed.

—Samuel D. Warren and Louis D. Brandeis, "The Right to Privacy," 1890

The strongest defenders of privacy usually define the individual's right to privacy as the right to control the flow of information about him. A seldom-remarked corollary to a right to misrepresent one's character is that others have a legitimate interest in unmasking the misrepresentation.

—Richard Posner, "An Economic Theory of Privacy," 1978

Lovelace Health Systems, a New Mexico health care provider, takes an aggressive approach to its work. Considered a model of efficiency, it prefers to preempt costly problems before they balloon out of control. In 1997, this approach sparked controversy, when some observers concluded the company was planning to dig too deeply into the lives of those whose health care it managed.

At issue was depression—a debilitating but often hidden mental illness. Depression is known to be associated with many less diffuse, and more expensive, problems. Depressed employees are believed more prone to alcohol and drug abuse, more likely to be hospitalized, and more likely to generate higher bills for prescription medicines. Identifying and treating depression at early stages could forestall big outlays for lost time on the job, psychosomatic illnesses, and self-destructive behavior later on. Lovelace planners apparently calculated that timely intervention, through counseling or drugs like Prozac, could prevent trouble before it occurred. They accordingly conceived a program to identify and treat depressed employees of their client the Sara Lee Corporation at its L'eggs Brand manufacturing plant near Las Cruces.

From there, accounts differ, and the story is disputed. According to the *New York Times* and other publications, employees weren't told that the questionnaires they were asked to complete aimed at diagnosing depression.[1] Many of them would no doubt have objected to having their mental states monitored—or treated—without their consent or knowledge. Like most of us, they might have preferred to keep their moods, their anxieties, and their disappointments to themselves, even if that meant declining "helpful" intervention from others.

Stories like this underline a hard truth central to countless privacy dramas: *there is no natural line of separation between the realm of the private and personal matters of legitimate interest to others.* In the Sara Lee case, no one could fault employees for preferring to keep their states of mind—depressed or not—to themselves. Yet it is clear that depressed workers would not be the only ones affected, should their illness become full-blown. Other employees would also suffer, perhaps acutely, if their supervisors, coworkers, or subordinates were disabled in this way. And the savings to the employer and the insurer from early intervention would not benefit the companies alone; all insured persons would stand to gain, if claims from all sources could be reduced.

The very information about ourselves that we experience as most intensely private often stands to affect others in the most direct and compelling ways. Indeed, it is often the most "private" information about ourselves—our health, our political attitudes, or our feelings about those around us—that ultimately holds greatest interest for others. When and whether such interests should be considered legitimate is not somehow given in the nature of things. It is a matter for constant definition and re-definition in public sensibilities.

Let me define privacy as the exercise of an authentic option to withhold information on one's self. This definition has some non-intuitive implications. Not everyone who enjoys options of this kind exercises them so as to experience privacy. A calculating celebrity may have every means of keeping her life to herself but throw privacy to the winds, living flamboyantly in hopes of drawing the attention of curious fans. Conversely, the classic shipwrecked inhabitant of a desert island enjoys no privacy, even though he remains completely out of others' ken, since he exercises no control over information about himself. But privacy is attained by those who, confronted with others' interest in their sex life, their age, their income, or their golf handicap, succeed in keeping such information to themselves.

Tension over privacy is a universal feature of social life. Some societies allegedly have no term for privacy, and no concept of it. The lack of a word translatable as "privacy" is entirely plausible; the absence of concern for it is not. For it is impossible to imagine a social world where people are indifferent to the potential consequences of sharing information about themselves that only they know. That would be a world where people didn't care who knew about their movements, the messages emanating from their viscera, their strengths and weaknesses, their hopes for the future, or whom they love or loathe.

In countless ways, in every social setting, people stand to gain or lose by controlling what others know about them, and certainly by keeping certain "personal" information to themselves. This principle holds true as much in intimate settings as in the most impersonal public forum. Lovers and family members may consider the intimacy that they share as the distinguishing feature of such relationships. But such willing relinquishment of privacy is rarely indiscriminate or total. Every social world entails its distinctive patterns of withholding and disclosure. The bureaucratic, impersonal world that we inhabit at the beginning of the twenty-first century, shaped by institutions like Lovelace Health Systems, embodies its own strange juxtapositions in this connection. It is a world where most of us, willingly or not, share with distant and impersonal organizations information that we would insist on keeping private from intimate acquaintances. Struggles between institutions and individuals over access to and use of such personal data fuel today's far-reaching privacy controversies.

Why do people struggle to protect their privacy? What interests move people to censor or withhold information about themselves?

Often, motives for privacy-seeking are purely strategic or instrumental. In countless situations, the flow of personal information can yield practical advantage or disadvantage. Looking to buy a house or a car, we do not find it advantageous to reveal how urgently we want to make the transaction or the maximum we are willing to pay. No more do we reveal to our bosses, coworkers, or subordinates exactly what we think of them—or our interest in changing jobs, or our efforts to bring about such changes, until they are fulfilled.

But if privacy is often a means to strategic ends, it can also be an end in itself. There are some moments in life that few people choose to share—even though everyone knows that they occur. These range from experiences of sex or excretion to moments of extreme grief, joy, or relief. Most people also recoil from seeing others involuntarily exposed in these ways, sharing their sense of shame or violation when something that seems inherently private is publicized. Similarly, most people would probably prefer not to share with others records of embarrassing medical procedures they have undergone—or perhaps any of their medical files at all—even when everyone understood that the procedures had taken place. At issue in cases like these is not *strategic* advantage or disadvantage, so much as *inherent* satisfaction at keeping certain information and experiences to one's self.

In the real world, these contrasting privacy interests occur in endless permutations and combinations. The proposed centralized archive of all Americans' medical data mentioned in the preface, for example, is apt to trigger concerns on both counts. People would have reason to be anxious that their medical files might be used to their disadvantage in dealings with government agencies or insurance companies, for example. But most of us would also feel uncomfortable simply at the idea of exposing such details to scrutiny by *anyone* with no need to know them.

Most of the big institutional surveillance systems that make up the subject of this book raise strategic concerns. Even if we don't mind other shoppers' seeing our choices at the supermarket checkout, for example, we might well fear disadvantage at the prospect of those selections being shared with direct marketers or the IRS. Tax collectors might plausibly benefit from data on taxpayers' supermarket choices—for example, by identifying taxpayers whose lifestyles appeared to exceed their reported incomes. But most of us probably do not want to confront an IRS endowed with the ability to moni-

tor every consumption choice. For similar reasons, many people recoil at allowing insurance companies access to potential customers' genetic information. Here as elsewhere, the feeling is that *knowing that much* about potential insurance applicants simply places companies at an excessive strategic advantage.

But other privacy values, less strictly instrumental but no less compelling, also matter in today's privacy controversies.

Late in 2004, local officials in the rural California community of Sutter instituted an ingenious new system for taking attendance in the town's public school.[2] All pupils would be required to wear RFID (Radio Frequency Identification) tags while on school premises. These are tiny, unobtrusive chips often attached to or embedded in items, enabling sensors to track their movements—retail goods from warehouse to store shelf; pets, in the event they go missing. Children in Sutter were to don ID badges containing the tags on entering school premises and would be forbidden to remove them until leaving at the end of the day. The intent was to automate tasks of attendance-taking—and also to monitor the whereabouts of pupils when not actually in class. Such well-worn strategies as remaining in restrooms during scheduled activities were obviously destined to become futile under the new regime.

Pupils were disturbed by the requirement, and parents began asking why the measures were necessary. School authorities were unresponsive—and seemingly surprised at the resistance. Organized protests ensued; civil liberties groups and privacy activists entered the fray against the new system. The resulting controversy revealed that the system was a promotional gift to the school from a local company seeking to market it nationally. Stunned by the firestorm of criticism, officials ultimately withdrew the scheme.

"Our children are not inventory," stated the aggrieved parents in a formal complaint. They were articulating, one senses, privacy values of an inherent sort—ones compromised by excessive tracking of young lives, even in the best of practical interests. No doubt many mishaps to children—including even the most heart-wrenching—could be prevented, if *all* children were fitted with RFID tags for use at *all* times. But a world where supervision of children left nothing to chance, where their every moment were accountable, would be a world lacking some of childhood's most valuable moments. Such a world would certainly protect children against many harrowing misadventures—but

would also preclude childhood adventures like those, say, of Huckleberry Finn. And all of this assuming the best intentions of the monitors.

Some of the privacy values implicated here are *holistic,* rather than strictly individual. By this I mean that we often stand to gain or lose from widely experienced gains or losses to privacy, regardless of what happens to information about ourselves individually. If nearly everyone around me feels and acts as though all conversations were being overheard, then something crucial is lost from public life—even if I am convinced that my own conversations are secure. As the jurist Charles Fried put it, a shared sense of privacy creates a kind of "moral capital" whose benefits may be widely shared—by providing context for all sorts of beneficial relationships including love and friendship.[3]

Thus, as with freedom of expression, losses to privacy may not only be experienced by those whose information is appropriated. We all lose in a world where our fellow citizens are intimidated from speaking their minds. And we all lose—in a variety of ways—when those around us sense that anything they do, or perhaps even any inclination to act in the future, is subject to monitoring and corrective action.

The Tensions of Privacy and Disclosure

The Mehinaku are a tiny tribe living near the Xingu River in central Brazil. Their quest for privacy appears as earnest as our own—but in many ways more daunting. They live in close physical proximity to one another, in lightly built houses of natural materials whose walls are permeable to sound. Their village is situated on a flat plain, linked to the outer world by straight trails that render everyone's movements public knowledge. Promiscuity is widespread, but so are curiosity and gossip about one another's sexual exploits. Each member of the tribe has distinctive ways of hunting, fishing, toolmaking, and musical performance—thus advertising his or her presence and occupations, even after the fact. Even people's most intimate activities leave traces easily "read" by their fellow Mehinaku. According to their chronicler Thomas Gregor, "Everyone's footprint is known to all his or her fellow tribesmen. Since the soil . . . is sandy and loose, the barefoot Mehinaku leave visual

records that the rest of the tribe are astonishingly adept at reading. The print of heels or buttocks on the ground may be enough to show that a couple stopped and had sexual relations alongside the path."[4]

These and other pressures on privacy, Gregor speculates, may have something to do with some other distinctive customs that these people observe: long periods of virtual self-ostracism within the community and extended sojourns outside Mehinaku territory.

Like all social settings, Mehinaku life has its distinctive *privacy regime*—its own pattern of facilitation and constraints regarding the flow of personal information. If appetite for privacy in some form is a universal element of human experience, sensitivity to the realities of privacy regimes is no less so. In our world, any socially competent adult quickly comes to understand how privacy expectations in an isolated small town differ from those in a metropolis—just as one immediately senses the contrast in this respect between an intensive-care ward in a hospital and, say, a resort hotel. The same sorts of distinctions are no less evident in relations between citizens and governments. The personal data one expects to share with government agencies in an expansive welfare state like Sweden obviously differ vastly from what one expects as a citizen of the United States.

Few if any privacy regimes are solely products of conscious design. They normally emerge as ad hoc compromises, reflecting prevailing power relations, population densities, technological possibilities, architectural and urban design, and a host of other contingencies. The personal information one expects to yield, in other words, depends on such matters as how often one meets the same people, what technologies and media of communication are in use, the sort of dwelling one inhabits, and other matters that may not figure in anyone's original intents concerning privacy.

Neighbors may ultimately be as curious about those around them in the metropolis as in Sinclair Lewis's archetypal small town, Gopher Prairie. But the physical and social realities of city life make it impossible to impose demands for information in the city that could be made to stick in a small town. Merchants everywhere will want to know how much their customers are prepared to pay for a particular product and where else it might be available to them. But some environments, from small towns to cyberspace, may make such information readily available, whereas the anonymity imposed by other privacy regimes blocks such strategic invasions of privacy.

Debate and soul-searching over the proper claims and counterclaims of privacy and disclosure are essential ingredients of civic life. What personal information should people expect to keep to themselves, and what should the community, the family, or the state expect to know, in any vision of a good society?

Much as domains of privacy are indispensable for a full and decent life, we also rely on the vitality of what one might term the "public sphere"—the realm of actions taken or information offered in public and understood as such by all parties. When we make our way down the public thoroughfare; when we express our opinions in an open meeting or a letter to the editor; when we sprawl on the public beach or step into or out of a tavern—when we do such things, we do so with the understanding that anyone is free to take note. Under such circumstances, everyone adjusts his or her conduct to the public character of the setting. Those incapable of distinguishing between public and private modes of action, and of switching from one to the other at appropriate moments, can never be competent adults.

In noting the distinction between domains of conduct intended to be enacted in public and those intended for the private sphere, I hardly mean to suggest that restrictions should never apply to use of "public" information.[5] But such restrictions have often in the past been unnecessary. Before the rise of special technologies for preserving the unfolding daily "record" of human affairs, personal information generated in public normally had a short half-life, passing unnoticed in the first place, or quickly forgotten. Rather, special steps, from diaries, to social scientists' field notes, to the archives of the daily press, were necessary to preserve it.

Yet whether preserved in human memory or on computer files, the unfolding, publicly accessible "record" of public conduct is crucial for civic life. Events enacted there play an indispensable role in framing public debate and defining the public good. What makes personal information drawn from the public sphere vital is precisely that *no one can altogether know, or control, the interests or mind-sets that will form the context for future "consumption" of that record.* Because public conduct is available to all and sundry, and because no one knows definitively how any element of it will look in light of future events, there is no substitute for it as a basis for future action.

Often this resource serves strictly individual and strategic interests. Throughout life, we constantly predicate dealings with those around us on the cumulative—if unsystematic—record of past acquaintance with them. As the jurist Richard Posner would remind us, such impressions make it possible

to adjust our actions to those who appear as reliable or undependable, restrained or impulsive, honest or devious. It is very difficult to imagine how we could go about everyday life without sufficient "invasion of privacy" to afford some basis for such judgments.

Not just individual strategic advantage, but also the quality of public discourse and deliberation require a measure of access to such information. How did the candidate for public office presenting herself as a champion of women's rights deal with female subordinates before she entered politics? What sorts of environmental practices did the government official now entrusted with environmental protection follow when he was in private industry? What public role did political figures in Eastern Europe who now profess deep commitment to democratic values play, when those values were in eclipse under the Soviet Empire? It is hard to imagine how public life in any pluralistic system could go forward, if no information were available on such matters.

The usefulness of such public information matters not only in regard to specific public figures. In virtually any discussion of public affairs, it is necessary to weigh current stances against "the record" of past events, statements, *prises de position,* and the like. Imagine a situation in which community members rise in collective outrage to oppose construction of a mosque in their neighborhood, claiming it would destroy the neighborhood's strictly residential character. Under such circumstances, the public may well want to know about past responses of the same community to plans for construction of churches or synagogues. When members of an ethnic group organize the defense of one of their own against charges of public misconduct, it is informative to note how the same group reacted when nonmembers were charged under similar circumstances. Here, too, public debate and deliberation depend on knowledge of how people have acted in moments where they could not have anticipated the interest those actions would hold in the future.

One can imagine a fanciful machine that would create a time-delay between social behavior and its "transmission"—the social equivalent of devices used in radio and TV broadcasts. Such a machine would give everyone a few extra seconds or minutes to decide whether any particular bit of social behavior would go "on the record." No doubt everyone would want such a miraculous privacy protection device, and everyone would have occasion to use it. But unless it could be adjusted to censor behavior well into the past, it would still not serve to eliminate all embarrassing or inconvenient information from our "public record." For what anyone might regard as embarrassing

or inconvenient itself depends on unfolding context, such that what appears unremarkable or meritorious in one setting may take on quite another aspect under new social circumstances.

Thus debates over privacy reflect long-running ethical and political tensions between individual prerogatives and claims of larger social units. Aspects of life that can be made known to governments—or communities, families, tribes, or other authorities—can often thereby be subjected to control by these interests. Desires for privacy often map efforts to assert one's own interests or individuality in the face of countervailing claims. The greatest ambivalence surrounds these efforts—and often, the greatest inconsistency. Everyone deplores the invasion of privacy in principle, just as nearly everyone professes to join Warren and Brandeis in deploring media preoccupation with personal matters unrelated to the public interest. But at the same time, we often join Richard Posner in affirming the validity of people's desires to inform themselves on the backgrounds of political figures, potential lovers, or prospective nannies, physicians, or business partners. One person's outrageous invasion of privacy may be another's prudent testing of social waters.

Efforts to adjudicate between privacy claims and public demands for personal information have a long pedigree in Western thought. Indeed, they follow intellectual fault lines laid down centuries ago.

One key tradition is utilitarianism, reckoning the value of personal information (or anything else) in terms of the total utility or pleasure generated by its use. This line of thinking ascribes no special say to anyone regarding the fate of "his" or "her" information. Instead, the best use of personal data is the "highest use," the one commanding the greatest rewards for the largest number of people. Defense of privacy is thus not *inherently* more worthy than its invasion—the fate of personal data properly being decided, in effect, in the marketplace.

Consider privacy in romance. Should someone be able to draw a veil of confidentiality over past relationships in approaching potential new dates or partners? Only if he or she is willing to pay more to conceal such information, a utilitarian might say, than prospective future companions are to discover it. There are no "rights" to privacy, in this view, any more than there are "rights" to discovery. The best allocation of personal information is the one that brings greatest total satisfaction to all interested parties—with satisfaction often

reckoned in terms of the price they are willing (or able) to pay. Thus claims of large numbers of highly motivated seekers of personal information may very well outweigh those of the person seeking to withhold such information.

This mind-set has its precise expression today in the influential privacy doctrines of jurist Richard Posner. He proposes a wholly strategic view of privacy, with treatment of personal data governed by "economic efficiency," specified as: "(1) the protection of trade and business secrets . . . ; (2) generally no protection for facts about people—my ill health, evil temper, even my income would not be facts over which I had property rights although I might be able to prevent their discovery by methods unduly intrusive."[6] In Posner's own terms, it is hard to see what would constitute "unduly intrusive" methods. Intrusion, however understood, should not be too high a price to pay, if the market-reckoned benefits of knowledge so acquired warrant it.

Clearly, utilitarian thinking does not naturally lend itself to support for privacy. It is an utterly democratic doctrine, in which the satisfactions of all concerned command equal consideration—the satisfactions of those who seek to know personal data, as much as of those who seek to conceal it.

The historic counterweight to this position is doctrines of individual *rights* over information about one's self. If Hobbes and Bentham provide the origins of the utilitarian doctrines, notions of privacy rights derive from Immanuel Kant. This line of thinking posits that people must be accorded certain forms of control over "their own" information—much as over their own property, their own bodies, or their own opinions. Claims regarding disclosure or concealment of personal information, in this view, should have nothing to do with the advantages or disadvantages to others, or to society as a whole, of such sharing or withholding. Instead, respect for individuals' right to control certain kinds of personal information forms part of a broader respect for personal dignity and autonomy that every social order must embody. This thinking underlies many of the most articulate defenses of privacy—including defenses against the pressures on privacy from government and private institutions that have arisen in recent decades.

Most of us, I suspect, at least vaguely embrace notions that people have some special rights over disposition of "their" information. We feel that things have gone wrong, somehow, when a health care provider trolls through employee data to identify and even treat depressed staff members without permission or knowledge of the latter. Even if our own depressed state of mind may prove counterproductive for others, we sense that information about

depressed thoughts or moods is *our* information—and nobody else's. Yielding control over such intimate information about ourselves, we may feel, erodes some basic right to be treated differently from an animal, a robot, or a bit of merchandise.

These profoundly contrasting rationales are not just the province of professional philosophers and ethicists. They infuse real-world debate and struggle over privacy among jurists, public officials, activists, and ordinary citizens.

In controversies over law enforcement or national security, for example, many hold that the most personal information may properly be extracted from unwilling individuals, even by stealth or torture, given the high collective benefits of stopping terrorism or curtailing crime. By this logic, a "right" to control access to one's bank or credit card records would make no sense. Those taking this position would argue that openness of such data to commercial scrutiny actually reduces the costs of credit transactions or abets the growth of the economy—thus generating the greatest total satisfaction for all. Here the logic is basically utilitarian.

Against such thinking, the logic of rights would uphold people's ability to maintain control over "their" information, regardless of the profitability or other satisfactions of disclosure. Even where defense of privacy is inconvenient, or even excruciating, to nearly all concerned, the right of privacy must be upheld—just as slavery or baby-selling must be rejected, no matter how expedient, efficient, or profitable. It is of course such a rationale that underlies American constitutional guarantees that people not be required to testify against themselves, as well as other basic civil liberties. Transposed into the commercial realm of consumer credit, advertising, and insurance, such thinking would undermine major industries and highly expedient government practices—as parts II and III of this book show.

But public debate and public policy on privacy issues have produced few if any rigorous purists on either side. Or to put matters less elegantly: few real-world advocates and planners in these matters appeal consistently or exclusively either to utilitarian logic or a logic of rights. Few proponents of utilitarian thinking are willing, at least openly, to assert that people should enjoy *no* special say whatsoever in the fate of data about themselves—that is, that personal data should receive no different treatment from that accorded to just *any* information. And few if any thinkers in the Kantian, rights-oriented tradition would be willing to assert that numbers and costs should *never* matter in adjudicating privacy claims—as though, for example, a person with

a highly communicable disease should never be obligated to share data on his or her health status, even when such sharing might well protect the lives of many others.

In what some scholars consider the most influential law review article ever published, Samuel Warren and Louis Brandeis argued for legal recognition of privacy as a "right to be let alone."[7] But in practice, we hardly ascribe to anyone an *absolute* right to be left alone—any more than most of us would assert that people should have no special say in the fate of information about themselves. Whether as philosophers or ordinary folk, we nearly all view life as a skein of legitimate and illegitimate claims and counterclaims over who may know what about whom. Efforts to weave these disparate threads into a coherent theory of privacy are endlessly tantalizing.

Privacy Regimes in Turmoil

Struggles to draw a bright line between private and public thus have a long, if inconclusive, history in the abstract world of philosophers and ethicists. But real-world developments over the last few decades have injected a jolt of immediacy and urgency to these unresolved tensions—and goaded me to write this book.

No alert observer in the twenty-first century can fail to note these developments. All of us constantly sense that "our" information—data on our movements, our financial affairs, our consumption habits, our physical state, and on our very consumption of information itself—is taking on a life of its own. But obviously data don't literally act in their own right. More precisely, *organizations* are constantly finding new ways of capturing, transmitting, and using personal data, for purposes defined by the organizations rather than by those depicted in the data. Supermarkets track our purchases; government agencies track our travels, transactions, communications, and associations; insurers and employers monitor our medical histories and genetic makeup; retailers monitor our expenditures, our website visits, and our financial situations. In any of the world's "advanced" societies, such lists could be extended at great length—with revealing differences across national boundaries. No less tellingly, we correctly sense that the information harvested in these efforts *matters* for the treatment we receive in settings often far removed from the collection.

How are we to account for these patterns? What larger social forces have propelled them? Most observers probably place responsibility squarely on information technology. It is the computer, they insist, that has created these new transparencies and thereby roiled privacy regimes.

But in fact, these trends have even deeper roots. Routine collection and use of personal data by state and private organizations dates from well before the computer. As long ago as the late nineteenth century, some Western European governments had begun systematic record-keeping on their populations, to support the administration of old-age pensions or passport issuance. By the mid-twentieth century in the United States, credit-reporting agencies probably maintained records on the majority of middle-class families. By that time, income taxation and Social Security in America had given rise to systematic record-keeping that touched the lives of the majority of the economically active population. In Western Europe, welfare state record systems supporting family allowances and pension plans probably antedate their U.S. counterparts by several decades. And all consumer societies soon added comprehensive systems for law enforcement record-keeping, driver licensing, and vehicle registration. All these systems were flourishing well before anyone thought to computerize them.

Such systems share a distinctive and sociologically crucial quality: they not only *collect and record* details of personal information; they also are organized to *provide bases for action toward the people concerned.* Systematically harvested personal information, in other words, furnishes bases for institutions to determine what treatment to mete out to each individual. I call such operations systems of *mass surveillance.*[8] Mass surveillance is a distinctive and consequential feature of our times. Whether carried out by government agencies or private-sector organizations, it shapes the ways we approach major institutions and our treatment at their hands.

Surveillance in this sense does not necessarily entail harmful intent. In one form or another, it is a basic and ubiquitous social process, occurring in settings ranging from the family to state bureaucracies—whenever one party seeks to shape its treatment of the other on the basis of the latter's past performance. What has changed in the last hundred years is the rise of mass, bureaucratic surveillance based on formal record-keeping. Surveillance in this form ranges from the benign to the repressive—from the personal information systems supporting intensive care in hospitals to those mobilized to track and curtail terrorists. And it fuels today's pervasive pressures on privacy.

Expectations of mass surveillance have become ingrained in all of us. We take it for granted that large organizations from tax collectors to credit card companies will deal with us—and everyone else—on the basis of our ubiquitous "records." And the *forms* taken by these surveillance processes are remarkably similar, despite radical differences in the sorts of organizations involved. The purposes may be as varied as the allocation of consumer credit; or identification and tracking of criminals or terrorists; or administration of social welfare benefits; or precise targeting of advertising to the most susceptible consumers; or control of population movements across international (or internal) boundaries—or any number of other familiar bureaucratic aims. In all of these and many more settings, the logic of mass surveillance leads to similar routines of personal-data monitoring and similar patterns of action based on data so collected.

For all surveillance systems, the ultimate aim is discrimination—discrimination in determining precisely what actions are warranted toward each member of large populations. This may mean discrimination as to who is "worthy" of credit, and how much credit should be extended; or discrimination between individuals more or less dangerous to public order, and in what measure; or as to who is liable for tax assessments or social insurance benefits, and to what extent—and on and on. Each resulting decision as to what action to take in turn becomes part of the "record" of the individual concerned. In this way, surveillance systems combine the fine-grained attention to the detail of people's lives characteristic of intimate relationships, with the impersonal, rule-bound action typical of bureaucracies.

Systems like these feed on steady diets of "actionable" personal information—that is, personal data deemed reliable enough to form bases for binding bureaucratic decisions. Most often, actionable data are produced by other bureaucracies. For decisions on consumer credit, actionable data range from details of consumers' current and recent credit accounts to data on assets and liabilities drawn from their tax returns. For law enforcement decisions, relevant data range from someone's criminal history to the details of his or her bank account. For decisions underlying identification and tracking of terrorists, crucial data might be anything from records of telephone conversations with other suspected terrorists to electronic logs of international travel. For decisions about allocation of medical benefits, actionable information would include data on premiums or contributions, as well as medical history and recent claims histories.

A fact of life in the world's "advanced" societies is that more and more junctures produce such actionable information—and hence feed the needs of ever-expanding surveillance. As more and more consumer transactions require use of credit cards, more and more data are generated to support more refined judgments of what *further* credit should be allocated to each consumer—and on what terms. Credit information has now grown so rich, and its use so sophisticated, that every American consumer is now allocated a three-digit credit score, based on a wide range of actionable data. Since the 1990s, credit grantors have succeeded in marketing these scores to insurance companies, as bases for discriminating decisions as to who will receive insurance coverage, and at what cost. Thus the evolution of credit surveillance has given rise to a new form of actionable personal data of great value in another setting altogether. Such ever-emerging symbioses among surveillance systems represent one of their most remarkable features.

Note that a certain conflict of interest between system and individual inheres in mass surveillance, whether the ultimate purposes of the operation are repressive or benign. Even systems supporting allocation of highly sought-after resources still need to distinguish between the deserving and the undeserving. Surveillance systems involved in medical care or social welfare benefits, for example, must concern themselves with the accuracy of information provided by seekers of those allocations. Not everyone seeking social security benefits will be entitled to them under the letter of the law, for example. Nor will all those seeking medical treatment "deserve" exactly the medication or other attention they seek.

Accordingly, surveillance systems constantly seek to generate and maintain their own sources of personal information, beyond the reach of the individuals concerned. They compile histories of contributions to social insurance schemes; or records of medical insurance payments made or medical care received; or data on past tax liabilities and payments—all of which must be mobilized in the determination of what future treatments are warranted for the persons concerned. The latter, of course, have their own interests in what treatment they receive—hence the endemic tendency to "censor" one's own record. When the system in question seeks to address those who prefer to avoid tracking altogether—criminals, credit abusers, or dangerous drivers—the cost of separating information from disinformation grows commensurately greater.

Thus, to support the discriminations they seek, surveillance systems typically require information from outside. The reasons are hardly complex.

In face-to-face relations, one rarely takes people's accounts of themselves altogether at face value, at least if the stakes are high. If someone promises to be trustworthy, for example, one prefers to verify that trustworthiness from those who have extended him or her their trust in the past. If a prospective baby-sitter or nanny professes to love children, one prefers to seek evidence of that attitude from those with independent knowledge. So, too, with bureaucratic surveillance. Given people's universal interest in censoring the flow of information about themselves, surveillance organizations always seek to cultivate data sources not subject to censorship from the persons concerned.

Thus it is axiomatic among credit grantors that credit applicants are more likely to provide data on their "good" credit accounts—those where their record of payment is satisfactory to the seller—than the bad. Similarly, applicants for driver's licenses or auto insurance do not necessarily acknowledge past accidents or citations. For such purposes, organizations sponsoring surveillance systems seek direct lines of reporting from the sources of such negative information.

Continuing refinements in surveillance constantly produce new twists in these symbiotic relationships—including collection and use of information whose relevance for decisions on the people concerned is unintuitive and indirect. Often these symbiotic uses of personal data exploit correlations between behaviors that the systems seek to address or control and predictive cues from utterly different corners of life. In marketing, for example, knowledge that interest in a particular topic—as revealed by website visits, for example—is associated with a tendency to purchase a specific product is enormously valuable as a basis for advertising appeals. Or in the search for terrorists, knowledge (or suspicion) that known terrorists favor a particular brand of toothpaste is apt to focus vast and unfriendly interest on buyers of that brand. The very fact that people have no idea that records of their website visits or product choices might influence treatment that they experience by retailers or federal investigators makes it especially unlikely that they will alter the behavior thus recorded.

This is how computing, while hardly the original cause of rising demand for personal data, has vastly facilitated the satisfaction of such demand. It's not just that new information technologies have drastically reduced the costs of storing and recalling personal data. Perhaps more crucially, computing has rendered it possible to produce countless "markers" of information from the most disparate moments of social life—and to bring such otherwise far-flung data to bear where they matter most to quite different surveillance systems.

To be sure, surveillance systems have always in some sense "needed" the benefits of supplementary or symbiotic information. But in earlier privacy regimes, vast amounts of such data have routinely been "wasted," forgotten as soon as they came to life, if they were ever noticed at all—permanently out of the reach of institutions that might need them. Computing has changed all that.

Thus the logic—perhaps one should say, *socio*-logic—of surveillance systems is to grow. Given that efficient pursuit of discrimination among persons is their raison d'etre, we should hardly be surprised that they tend to grow *in depth*—that is, in the total amount of information collected on the average individual with whom they deal. But surveillance systems also tend to grow *laterally*—to broaden the *variety* of sources of personal data that they rely on in making those discriminations, especially through symbiotic exchanges with similar systems.

It is not just the sheer volume of data accumulated that gives these systems their power to shape people's lives. Nor is it the "sensitivity" of these data in themselves, so much as their interactive quality. What information matters most, in terms of impact on individuals' lives, is often an utterly contextual matter. The knowledge that a visitor to a particular website is also drawing a particular prescription at the pharmacy may suggest something about that person's sexual orientation or HIV status—matters of great dollars-and-cents value to sellers of insurance and credit. Knowledge that a particular foreign national has changed his address with the post office to a location adjacent to that frequented by another foreign national may have great significance to police or national security services.

The resulting pressures for surveillance systems to link and exchange give great pause to privacy-watchers.

Blaming Technology

What are we to make of the long-term trajectory of these changes? Is the evident impetus of surveillance systems to grow and fuse with one another bound to end in utter elimination of private life?

At least one line of scholarly thinking would credit this view. This is the doctrine that technological change is driven by "imperatives" somehow inherent in technologies themselves.[9] In its pure form, this theory holds that

human intent has little bearing on the ultimate repercussions of technology. Technologies thus somehow develop according to their own inner logic, sweeping human values and intentions in their path. Applied to information technologies, this doctrine would suggest that destruction of privacy is inevitable, simply because it is possible—that the capacities of computing systems to absorb, analyze, transmit, and use personal data are bound gradually to find their ultimate expression, until no personal data is safe from incorporation.

This view is certainly provocative—indeed, usefully provocative. At the very least, it compels recognition that the actual social repercussions of any new technology are likely to include consequences remote from anyone's intent in introducing them. But notions of technology as an "autonomous" force in human affairs are surely misleading in their extreme form. With information technologies, one can readily point to forms and uses of the technologies that are scarcely dictated by the technologies themselves. The "same" technologies, in other words, can be imagined sustaining very different privacy regimes and very different social relations.

Consider consumer credit reporting in America, the industry concerned with collecting and selling data relating to consumers' attractiveness as credit customers to prospective credit grantors. Well before computerization, American retailers had developed sophisticated data systems for monitoring and reporting the credit status of ordinary consumers. By the 1960s, the credit reporting industry in America had enabled retailers to achieve a striking and economically rewarding goal—judging the "credit worthiness" of potential customers in a matter of minutes, before the latter had the opportunity to leave the auto showroom or appliance department and perhaps shop elsewhere or reconsider the transaction altogether. In short, credit reporting was now able to provide virtually an instant fix on the value and susceptibilities of any potential credit customer. With significant increases of speed and sophistication, the surveillance system constituted by this industry today continues to govern access to everything from employment to mortgages to credit cards.

But note that there exists no comparable intelligence system to inform U.S. *consumers* on matters of symmetrically vital interest to them in such transactions—the average length of time before major repairs are necessary for cars, appliances, or other prospective purchases; or the numbers of deaths or injuries reported from the use of such items; or indeed the rates of satisfaction reported by previous consumers of the product or by customers of the establishment selling it. In other words: there is a striking disparity between the

information afforded by technologies of surveillance over consumers *versus* technologies to inform consumers about products.

Thus we should hardly blame "technology" or "the computer" for the loss of consumers' control over information on their consumption patterns. There is no "imperative" requiring information technology to serve the interests of retailers rather than those of consumers. Indeed, the strictly technical demands of keeping track of hundreds of millions of idiosyncratic, mobile American consumers are surely more daunting than those of reporting on smaller, more standardized numbers of products and retailers. The reason why one set of systems is strong—and erosive of privacy—and the other relatively weak, has to do with social and political *sponsorship* of the two forms of information use, not with anything inherent in the technology itself. Far from being "autonomous" in this connection, information technology has supported the interests of retailers in accessing personal information about consumers, rather than interests of consumers in accessing information about retailers and products, because one group is simply stronger and better-organized than the other.

Consider, then, an alternative to visions of technological autonomy. One might view the potentials of any new technology as open-ended "resources"—social or economic goods that are "up for grabs" and subject to exploitation by whatever existing social interests are strongest. Thus one would expect the particular forms taken by information technologies to be dictated by the established interests of institutions already claiming public support or acceptance for their activities.

This picture, I submit, fits fairly closely the evolution of mass surveillance up to the early twenty-first century. It is very difficult to point to interests promoted by such systems that were not already well established before the crucial technological changes supporting them began to gather steam. The imposing surveillance systems we see around us in the world's advanced societies aim at reinforcing policing and other forms of state authority; or motivating consumers and regulating their use of credit; or enabling sellers of insurance to reduce their risks and maximize profits; or keeping bad drivers off the roads—in short, an array of long-standing administrative purposes pursued by the organizations involved well before the availability of computing to abet them. By contrast, it is hard to identify insurgent or previously unorganized social interests that have managed to shape any system of mass surveillance. Large-scale recourse to record-keeping on people has grown up to serve institutions that began with the best resources for investing in it.

This broad trend, however, draws upon something basic in public expectations of institutions—expectations of appropriateness or *justice* in treatment of individuals on the bases of their full records. All of us share these expectations, and they play an enormous role in fueling growth in surveillance. We expect governments to extract taxes from their people not capriciously but according to the letter of the laws defining tax liability. We expect to have the benefit of all the consumer credit that "our record" entitles us to. We expect state authorities to act against dangerous aliens and welfare cheats. We expect sellers of auto insurance to recognize our claims to rates that reflect our good driving histories. We expect to be protected from criminals and terrorists—and from those whose actions foster suspicion in these directions. For government and private-sector record-keeping alike, publics expect performances that demand just and authoritative discrimination—discrimination that in turn drives demand for recourse to systematic record-keeping.

Thus it would be a serious mistake to imagine that extension of mass surveillance, and concomitant pressures on privacy, simply entail institutional impositions on passive publics. That notion is as misleading as the notion of its being guided by some "autonomous" techno-logic. Instead, popular desires for efficient processing of personal information, and for just discrimination based on such processing, play an enormous role. Accordingly, nearly all systems of mass surveillance can rely on significant support in public opinion, however anxious people may be about demands made on their own information. Efficiency is a cardinal value throughout the world's "advanced" societies. And it has come to be axiomatic in these societies that efficient processing of human affairs demands satisfaction of institutions' "needs" for personal information.

Feeding such "needs" promises to intensify pressures on privacy—threatening what public opinion studies show is a strongly held value. But if there is one thing we know for sure about public opinion, it is that it obeys no requirement of consistency.

These conclusions can only lead to the sobering realization that has propelled me to write this book. *There is no "natural limit" to the incorporation of personal information in systems of mass surveillance.* By this I mean, for one thing, that no form of personal data is inherently too personal, too intimate, or too "private" to furnish a valuable basis for efficient decision making by organizations. Indeed, even casual examination of these systems shows that the most "private" or "personal" data may provide the very clues or associations most highly sought after for purposes of efficient discrimination.

These are often data available only through *symbiosis* among surveillance organizations. Thus information from medical encounters may well be relevant to determinations made by law enforcement organizations; or data from one's bank and credit card accounts may be highly attractive to suppliers of insurance; or information on website visits may hold the greatest value for prospective employers or state anti-terrorist operations. The potential for personal data to serve the purposes of efficient discrimination, on behalf of organizations with significant public mandate for their actions, is simply limitless. What may today strike us as outlandishly intrusive or fantastically inappropriate demands for personal information may readily be redefined as basic exchanges in tomorrow's information society. Think of the intrusions that air travelers have recently learned to accept as routine and inevitable.

Such a view of the spread of mass surveillance requires no assumption of arcane technological imperatives. More plausibly, and less mysteriously, the open-ended, ever-expanding monitoring of people's lives by government and private institutions stems from their attempts to "do better"—often at tasks widely commended in public opinion. If there are indeed no natural limits to growth in surveillance, serious efforts to protect privacy can only proceed via limits self-consciously created by human invention. But principles that might serve to guide such limits have proved to be anything but easy to define.

The Idea of Privacy Protection

Privacy as an issue for legislation and policy is a relatively recent arrival in the public forum. As early as the 1950s in the United States, acute social commentators began to single out personal record-keeping as a legitimate matter for public attention and action.[10] The year 1967 saw the publication of Alan Westin's *Privacy and Freedom,* probably the most influential writing on privacy since Warren and Brandeis's famous law review article. Westin could not have chosen a better moment in American consciousness. In a period when all established institutions were coming in for public skepticism and scrutiny, those involved in collecting and using vast amounts of personal data could hardly have avoided attention. No one could deny that these systems *mattered* to the lives of the people concerned, or that their existence had long been kept

as much out of the public eye as possible. The conclusion became inescapable: the workings of personal data systems were simply too important to be left solely to the discretion of the organizations holding the data. Some form of state action—legislation, policy, institution-building—was necessary.

But what form should such action take? More specifically, what practices stood to be corrected? And what principles required defense? What were the essential evils of invasion of privacy, and how should we define the essential aims of its protection? No one could fault vague declarations of basic "rights to privacy" of the sort affirmed in the United Nations Universal Declaration of Human Rights of 1948: "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence. . . ." But what concrete claims do such rights translate into, when juxtaposed against institutional demands for personal data? When are institutional appetites for personal information simply routine administrative requirements—and when do they amount to intolerable invasion of privacy? Many people, then and now, seem to identify that point according to the same principle by which they identify pornography: *I know it when I see it.* The trouble is that, in both cases, not all observers make the same sense of what they see.

By the mid-1960s in America, commentators were struggling with these questions—prodded by the realization that computerization was only making them more pressing. Perhaps the first official effort anywhere to propound general principles for privacy protection in the face of institutional surveillance came in *Records, Computers and the Rights of Citizens,* a report by the U.S. Department of Health, Education and Welfare published in 1973. In a declaration of far-reaching consequence in worldwide thinking on privacy, the report authors recommended five basic "Fair Information Practices":

> There must be no personal data record-keeping systems whose very existence is secret.
>
> There must be a way for an individual to find out what information about him is in a record and how it is used.
>
> There must be a way for an individual to prevent information about him obtained for one purpose from being used or made available for other purposes without his consent.
>
> There must be a way for individuals to correct or amend a record of identifiable information about him.

> Any organization creating, maintaining, using, or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take reasonable precautions to prevent misuse of the data.[11]

The term "fair information practices" seems to have been modeled after the notion of "fair labor practices"—ground rules, in both cases, for mediating between interests that are bound often to conflict.

It would be hard to overestimate the repercussions these recommendations have had in subsequent privacy debate and policy. Other key statements of principle on these same issues subsequently adopted around the globe have closely paralleled these. But like its successors, this influential statement leaves critical questions unanswered.

One is just how broadly these "fair information practices" are supposed to apply. Clearly many organizations—law enforcement and intelligence agencies, most obviously—would zealously insist that *their* record-keeping must remain secret and unaccountable to those targeted in it. The HEW authors nod to such claims, distinguishing between *administrative records, intelligence records,* and *statistical records.* "[B]y and large," they delicately aver, "administrative records are considered public; intelligence records, secret; and statistical records, anonymous," and they go on to comment: "The three types of records . . . should be held separately, and each should only be used for its nominal purpose. The transfer of data from one type of record to another should take place only under controlled conditions."[12] Thus they skirt the question of what safeguards or constraints should apply to record-keeping carried out by law enforcement and intelligence agencies—to which they evidently do not expect the above principles to apply. One can only speculate what they would make of the voracious appetites of intelligence agencies today for data compiled by private-sector record-keepers like credit and insurance reporters.

Another conspicuous absence in the HEW principles is any statement on the acceptable raison d'etre for record-keeping in the first place. What purposes, what interests warrant creating and maintaining surveillance systems? When should anyone be able to "just say no" to inclusion in such systems? When should government or private organizations be expected to conduct their business without recourse to record systems? What forms of data, if any, should be held unsuitable for inclusion in such systems? These questions obviously matter for privacy interests in all sorts of ways. The authors pred-

icate a key recommendation on the "intended use" of personal data, and the importance of preventing data "obtained for one purpose from being used for other purposes" without permission. But questions of who specifies the purposes for which data are collected or what constitutes its intended use get no attention. It is as though personal data systems arose through some nonhuman process, like earthquakes or sunspots. The HEW authors seem content simply to deal with them, once they come into existence.

Nevertheless, the HEW principles do clearly define and defend certain nontrivial privacy interests. Above all, they seek to open surveillance systems to public cognizance and attention, acknowledging personal record-keeping as a legitimate public issue. They envisage regular processes through which individuals can scrutinize their records and challenge inadequacies in their contents or injustices in their use. They propose to hold managers of record systems responsible for keeping their workings fair and accurate, and their contents secure. And they envisage limits on what can be done with personal information, so that individuals who yield their data to one system for one purpose should not ipso facto have to renounce control over further uses.

These may strike the reader as minimalist, even commonsense articulations of basic privacy values. But the subsequent evolution of surveillance has rendered some of them—particularly the injunction against unauthorized sharing of data—controversial, if not radical, in relation to twenty-first-century practice.

The HEW Report's "Fair Information Practices" constitute a historic marker in the evolution of privacy as a public issue—the first of a small handful of influential statements seeking to define privacy protection versus the claims of personal data systems *in general.* In the years to follow, four more statements of comparable breadth and influence have come to share that stage: the Organization for Economic Co-operation and Development (OECD) Guidelines of 1980; the Council of Europe Convention (C of E, 1981); the Australian Privacy Charter (APC, 1992); and the Canadian Standards Association Model Code (CSA, 1996). None of these statements represents law; they are simply recommendations emanating from diverse institutional sources. But no privacy-watcher would deny that they have had great influence on many, if not most, of the national codes that have grown up in the decades following publication of the American recommendations in 1973.

The principles set down in the statements show remarkable continuity with the HEW principles and commonality with one another. These common

themes are apparent in the Composite Portrait of Fair Information Practices presented in the following list—my own rephrasing of the precepts that appear in a majority of the statements.

1. The keeper of any system of personal records is responsible for the safety, security, and integrity of the data so stored.—HEW, OECD, CSA, APC, C of E
2. The existence, purposes, and workings of such systems should be readily accessible to public understanding.—HEW, OECD, CSA, APC, C of E
3. A single figure (a "privacy officer" or "data controller") should be identified publicly as responsible for safeguarding the privacy interests affected by the working of each such system.—OECD, CSA, APC, C of E
4. Information held in such systems must be collected legally and fairly.—OECD, CSA, APC, C of E
5. Individuals must be able to review the content of information held on them in such systems and the uses and disclosures of such information; individuals must be able to obtain redress for inaccurate and inappropriate uses and disclosures of such data.—HEW, OECD, CSA, APC, C of E
6. Personal data should only be collected in the form and to the extent necessary to fulfill the purposes of the system.—OECD, CSA, APC
7. Information held in file should be as accurate and up-to-date as necessary to fulfill the purposes of the system.—OECD, CSA, APC, C of E
8. Information collected for one purpose should not be used or released for other purposes, except under legal requirement or with permission of the individual.—HEW, OECD, CSA, APC
9. Information held in file should be collected with the knowledge or consent of the person concerned.—OECD, CSA, APC

Like any composite portrait, this one blurs detail. Most of the five codes propose at least a few precepts not found in the others. Principle 10 of the Australian Privacy Charter, for example, stipulates that "People should have the option of not identifying themselves when entering transactions." Or,

article 6 of the Council of Europe Convention specifies that data on "racial origin, political opinions or religious or other beliefs, as well as personal data concerning health or sexual life, may not be processed automatically unless domestic law provides appropriate safeguards," and goes on to extend this same principle to criminal convictions. The composite portrait omits these singletons. At the same time, the nine principles emphasize parallels at the expense of detail. They omit, for example, many qualifications and equivocations in the five statements—for example, statements that the principles should be observed "where possible."

But over all, the commonalities are striking. The various statements of principle aim above all to make the workings of personal data systems open, accountable, and subject to known rules of due process. They seek to create a role for individuals in the uses of data on themselves, while implicitly ratifying the right of the institutions involved to carry out these uses. They proscribe capricious, negligent, or inefficient uses of personal data—while basically accepting the activities of the institutions that give rise to such use in the first place.

What they do not do is address the central ethical issue implicated in the extension of surveillance: the tension between an essentially utilitarian logic of *efficiency* and a Kantian logic of *rights.* There can be no doubt that widening surveillance is efficient for all sorts of institutional purposes—that it helps allocate credit, collect taxes more productively, track would-be terrorists and other wrongdoers, crack down on unlicensed or uninsured drivers, direct advertising to just the most susceptible consumers, and on and on. Were it not for these attractive efficiencies, government and private organizations would never bother to invest the vast sums needed to create the systems. But whether the growth of these systems is compatible with values of individual autonomy and choice over "one's own" information is another matter entirely.

In short, principles like these help surveillance systems to achieve their intended ends more fairly and openly. But they do not help us decide what ends actually justify the demands of such systems for personal information in the first place. They do not, in other words, help us decide when institutional appetites for personal information simply *go too far.* It is as though environmentalists were to propose codes for environmentally responsible development of pristine lands without specifying when such expansion, however responsible, simply claims too much hitherto-unaltered space.

Almost certainly, such reflections were far from the thoughts of the policymakers who first struggled to frame these basic principles. Their concerns were no doubt much less abstract: how to reconcile people's evident interest in the fate of their data with the fact that the data-systems themselves were obviously crucial to operations of major institutions. Under the circumstances, planners were probably bound to search for areas of consensus, ignoring conflicts of interest that could only complicate creation of a common code.

One of the earliest of American controversies on this subject set a far-reaching pattern. This was American consumers' growing realization in the 1960s of the far-reaching impact of credit reporting on their lives. Credit reporting companies, then as now, made their way by collecting information on Americans' financial situations, including their consumption patterns, debt levels, and past payment of credit accounts. For decades, this industry had flourished virtually without legal restraint, successfully keeping its activities out of the public eye—on the theory, within the industry, that consumers could not object to practices that remained invisible to them. When commentators began to publicize the role of these practices in shaping access to everything from mortgages to credit cards to employment, many Americans were outraged that such privacy-eroding activities could be subject to such limited legal constraint.

But what would count as a reasonable response to the situation? On one side of the controversy, there was a diffuse population of consumers aggrieved or alarmed at the collection and use of "their" information. On the other was arrayed a major industry, for whom those very data represented an indispensable "raw material." The political chemistry of the situation must have given any public official pause.

The result, as in many another privacy controversy, was to focus public debate on that limited range of events on which almost anyone could agree things had gone badly wrong—"horror stories" where the systems had served neither individual consumers nor the ultimate aims of the industry. Here credit reporting presented rich possibilities. Stories abounded of the wrong consumer's data going into someone's file, or credit information being garbled in transmission, or exculpating information being ignored. The opaque workings of the system, it became clear, often made it impossible to correct such malfunctions, as consumers and retailers alike suffered from the denial

of credit relationships that should have gone forward, if only reporting had functioned more efficiently.

The upshot of these controversies in America was the Fair Credit Reporting Act of 1970—arguably the first national-level legislation addressing surveillance issues, and a presage of the principles embodied a few years later in *Records, Computers and the Rights of Citizens.* It opened the workings of credit reporting to public knowledge and to scrutiny; enabled individuals to see and challenge their records; and required retailers to notify consumers as to the role played by credit reporting in the fate of their credit applications. At the same time, it effectively ratified most of the essential practices of the industry regarding the forms of personal data-gathering permitted and purposes for which reports could be sold. Like later principles and legislation, it challenged no surveillance practices that were basic to this established industry. Nor did it provide individuals with an option to "just say no" to having their financial affairs subjected to reporting.

With the decline of Watergate-era protest in the United States, policy action on privacy shifted from the United States to Europe. There Sweden enacted the first national privacy code in 1973.[13] Since then, virtually every prosperous liberal democracy around the world has enacted one or more national privacy codes—often one each for government and private-sector record-keeping. Table 1 shows the spreading adoption of these measures.

Adoption of some of the measures noted in table 1 stemmed from dramatic explosions of public indignation—as in Australia and South Korea, where government efforts to impose national identity cards ignited privacy revolts resembling that of America's Watergate era. But elsewhere, initiatives to establish privacy protection seem to have arisen more as elite concern—official efforts to join the growing "privacy club" of nations addressing a globally recognized, emerging issue for government action.

To a striking degree, the measures shown in table 1 followed the broad principles summarized in the composite portrait. America's Privacy Act of 1974, for example, draws particularly from the principles of this country's HEW Report. Likewise, the suggestive role of the OECD Guidelines in the European Union's 1995 Privacy Directive is unmistakable, as is the role of the Canadian Standards Association's Model Code in Canada's 2000 private-sector legislation. With the passing years, common principles underlying most

Table 1. Dates of First Adoption of National Privacy Codes Applying to Public Sector Systems, Private Sector Systems, and All Personal Data Systems

Countries	Public & Private Sectors	Public Sector Only	Private Sector Only
Argentina	2001		
Australia		1988	2000
Belgium	1992		
Brazil			1990
Bulgaria	2001		
Canada		1982	2000
Czech Republic	2000		
Denmark		1978	1978
Estonia	1996		
Finland	1987		
France	1978		
Germany	1977		
Greece	1997		
Hong Kong	1996		
Hungary	1992		
Iceland	1989		
Ireland	1988		
Israel	1981		
Italy	1996		
Japan	2003		
Latvia	2000		
Lithuania		1996	1998
Luxembourg	2002		
Malta	2001		
Netherlands	1998		
New Zealand	1993		
Norway	1978		
Poland	1998		
Portugal	1991		
Slovak Republic	1999		
South Korea		1994	
Spain	1992		
Sweden	1973		
Switzerland	1992		
Taiwan	1995		
Thailand		1997	
United Kingdom	1998		
USA		1974	

N.B. These dates mark adoption of laws establishing rights and responsibilities over broad categories of personal records. Not listed here are dates of legislation applying only to specific forms of personal data, such as credit reporting or medical records.

Source: *Privacy and Human Rights 2004: An International Survey of Privacy Laws and Developments*. Washington, D.C.: Electronic Privacy Information Center.

nations' privacy measures have cross-fertilized one another. Yet the United States remains an outlier on most of these dimensions—most conspicuously for its absence of privacy rights covering broad categories of personal data held in the private sector, and for its lack of a national privacy protection ombudsman.

True, the *mechanisms* established in the earliest legislation differed considerably—in terms of the institutions created, procedures established, and legal principles invoked.[14] Some early European measures, for example, sought to license or register every personal data system—an aim that became increasingly impractical, as the sheer numbers of such systems grew. Countries also differ in the powers accorded to privacy commissioners—for example as to whether this official has the right to investigate data systems or to introduce bills for parliamentary consideration. But the years since the 1980s have seen broad pressures toward harmonization. National codes have grown by almost any standard more similar to each other at the beginning of the twenty-first century than when the first laws were framed—the United States remaining, as always, the exception.

The most significant privacy protection legislation since the 1970s is the European Community's 1995 Directive. This measure sets standards for privacy protection to be incorporated by all current and future members of the European Community in their national legal codes. Closely following the OECD Guidelines summarized in the composite portrait, the EC Directive requires that personal data be "processed fairly and lawfully"; it limits the purposes for which personal data may be used to situations where the individual has given consent or where use is required by law; it seeks to ensure the openness of data systems to scrutiny and challenge by data subjects; requires confidentiality and security in the processing of data; and requires that all member states create an independent "supervisory authority"—a privacy commissioner, in effect—to monitor the application of the Directive. It also proscribes export of personal data to countries outside Europe that fail to provide "adequate" privacy protections for such data in their own right.

The effects of the Directive have been sweeping. For one thing, countries around the world have sought to adopt compatible codes, so as not to jeopardize international business relationships by threatening the flow of personal information from Europe. Authoritarian Singapore, for example, has sought

to develop privacy codes that the EU will judge "adequate" to permit export of personal data for processing there. Lately, even mainland China seems to be moving in this same direction.

But whether such developments give assurance that privacy values are ultimately better protected than before is a matter for judgment. For one thing—as the following sections will show—provisions of the Directive have been interpreted very differently in different countries. Still more important, the Directive leaves open the same questions raised by other codes of "fair information practices"—notably, just how much of life should be subjected to mass surveillance. Certainly principles of openness and fairness in treatment of personal information represent a step up from situations like credit reporting in the United States until the 1960s—where the uses made of people's data were subject to no regulation whatever and largely concealed from public scrutiny by the users. But the rise of regulation over surveillance has rarely stopped its spread altogether; in many settings, regulation has apparently inoculated surveillance institutions against public indignation.

Spreading Shadows

Imagine social life as a vast and comprehensive tapestry or map, formed by a nearly infinite number of bright dots. Each dot would be a distinctive, repeatable social moment or transaction in an individual's daily life: a conversation with neighbors; a visit to the doctor; arrival at work; boarding a bus or an airplane; shopping at the market; a conversation between spouses at the end of a day—and on and on. The dots would obviously vary enormously in terms of the sort of information they generated and the parties to such information.

Now imagine the same map, with a difference. Superimposed on many dots would be a darker dot. These darker dots would mark where an encounter or moment is monitored by a system of mass surveillance. Some of the darker dots would obviously apply to points the parties would consider private; others would map actions occurring in public.

One hundred years ago, in even the most "advanced" societies, one would need to search energetically to locate the darker dots. In some of the United States—not all, in the early twentieth century—most births, deaths, and marriages would be so marked, as would be some financial accounts and perhaps

a few retail accounts. In other countries, most dark dots from a century ago would mark social insurance enrollments, military service, or passport issuance. But still, in any comprehensive reckoning, the dark dots on the social map of the early twentieth century would be few and far between—even in the most "advanced," most prosperous societies.

With the passing decades, areas shaded by dark dots have steadily grown. Today they would overshadow broad domains of social life—though not quite the same spaces in all countries. In the United States, I suspect, the darkened areas of the map would occupy larger portions of the total canvas than other societies. A very large percentage of all retail transactions would be incorporated, as would almost all access to credit. Virtually all employment relations would be dense with dark dots, as would all international travel. Most telephone conversations leave traceable, bureaucratically recorded dots, as would one's physical movements as monitored by airline security, toll road travel, cell phone usage, and a host of other markers. Regions involving medical care and Internet use would resemble swarms of insects at mating season.

Do some parts of the map remain untouched by the spreading shadows? A walk on a deserted beach or a backpacking expedition in the woods, perhaps—if the parties' cell phones remained off. Conversations with one's psychotherapist—but only if no third-party payers were involved. A visit to one's bookstore or library—assuming, in the United States, that the Patriot Act's prerogatives for monitoring those activities were not invoked. But the historical trend is unmistakable. Whether one regards particular categories of dark dots as benign or threatening, it would be hard to deny that their spread is changing both our experience of daily living and the participation of state and private organizations in our conduct.

Again, there is no reason to ascribe this spreading sway of mass surveillance to mysterious "imperatives" of information technology. Nor does it necessarily result from conspiracies by surveillance organizations. Instead, the spread of bureaucratic surveillance stems from a reflexive public expectation in modern social orders—that organizations dealing with people always make the very "best" decision possible about each individual, in light of all available information.

Such efficiencies are of course coveted by the organizations involved—but also in varying degrees by the broad publics that grant these organizations legitimacy, or at least acquiescence. No one could deny that these constituencies

indeed seek convenient telephone communications, easy availability of goods and services, pursuit of dangerous criminals and terrorists (and potential criminals and terrorists). And if access to the fullest possible array of personal data is held necessary for efficient delivery of these performances—well, in the world we inhabit, efficiency is a hard value to trump.

Thus it does not take too much imagination to picture a world where these trends have run their course—where the dark dots have suffused the entire map, and every social juncture generates its own bureaucratically actionable record. This would be a world where all cell phones would be on all the time and where everyone was required to have one. It would be a world where every life juncture of interest to future medical care providers, from supermarket purchases to sexual activity, were recorded for those purposes. It would be a world where tax authorities had full and automatic access to all income and expenditures of all citizens; where credit grantors could predict better than consumers themselves when the latter would find themselves short of funds; where the police and other forces of order had on-line, real time records of the whereabouts of every citizen and resident—and on and on. And where organizations like these found it useful to avail themselves of personal data collected by other surveillance organizations, such information would be shared without question. This could be the safe, orderly, compliant, and efficient world envisaged in the preface—provided of course that one trusted the organizations concerned. But it would certainly not be a private one.

Constraints and Countercurrents

Again, I see no "natural limit" to the evolution of mass surveillance into a world of this kind. The underlying logic of these trends—I might say, their *socio*-logic—is to extend without limit the intake and sharing of new forms of personal data. As the Lovelace Health Systems quest for hints of depression among its insurees demonstrates, no amount of such information, no *category* of personal data, is somehow *too* personal, intimate, or private to serve constantly emerging "needs" of organizations. On the contrary, it is often just that information that we experience as most strictly and intimately "ours" that proves most attractive for such purposes.

The only possible defenses against endless loss of privacy to institutional surveillance are of human design—purposeful limitations in the scope and

extent of surveillance. The impulse to fashion such constraints obviously underlies worldwide privacy protection efforts.

But do such measures in fact promise a serious brake against the inexorable spread of "dark spots" across the social map imagined above? The answer to this question is not obvious. One can argue that privacy protection as it has developed in the world's liberal democracies works more to *enhance* the extension and effectiveness of surveillance than to constrain it. Making the workings of surveillance systems more open and more accountable; providing individuals the opportunity to contest the appropriateness and accuracy of "their" information held in file; and ensuring that decision making based on the information is "fair," one might well hold, simply disarms public objections and streamlines acceptance of the underlying practices. More, one might argue, by establishing that any institutional "purpose" or "need" for personal information justifies such monitoring, privacy codes hold open the floodgates for unlimited extension of surveillance. Thus, a perplexing picture indeed: official measures on behalf of "privacy protection" ultimately serve to smooth the bumps and brush aside obstacles en route to a vastly less private world.

But matters are not quite so simple as this. The consensus principles that have shaped so much of the world's privacy protection measures are actually multifarious and even contradictory in their implications for policy and action. True, they implicitly legitimize the "needs" of institutions for ever-greater amounts of actionable data on people. But they also imply some far-reaching heresies within the church of surveillance.

Above all, notions that personal data provided for one purpose ought not to be released for other purposes without an individual's consent collide with the logic of surveillance. In such systems, *it is precisely personal information compiled by and obtained from sources independent of the individual that best fuels the fine discriminations that surveillance aims to support.* Credit grantors always prefer to seek data on applicants' financial situations directly from other financial institutions—rather than from credit applicants. Tax collectors always seek data on taxpayers' incomes directly from the sources of that income—rather than from the taxpayers. State security agents always seek data on suspected terrorists' movements from other state agencies—rather than from the travelers themselves. But such access to untainted information on people under surveillance requires precisely the transmission of personal data collected for one purpose to users pursuing quite different purposes. If

the people concerned could effectively censor such transmission—if their meaningful consent were indeed required for its release—the essential logic of surveillance would be subverted.

Thus the tension between this privacy-protection principle and the gathering pressures on personal data. The history of privacy over the last four decades consists of one collision after another between privacy-oriented efforts to *compartmentalize* personal data and gathering pressures to share such data directly among interested parties—without consent or even knowledge of the persons concerned. In the United States, these conflicts have often involved efforts of government and private interests to gain access to IRS and Social Security files. In France, they have involved efforts of tax authorities to use welfare state agencies to track reluctant taxpayers. In Canada and the UK, they have involved the efforts of credit reporting agencies to access consumers' account data, regardless of the latter's interest in permitting such access. Universally, the appetites of large institutions to triangulate their dealings with people by relying on data collected by other institutions for other purposes grow more acute as they become easier to satisfy.

The question is, can privacy measures be expected to withstand such pressures? Or is my learned friend correct, when he urges us to regard privacy as a quaint but anachronistic yearning in a world that runs on information?

These questions are not new. Among other commentators, my coauthors and I raised similar concerns in *The Politics of Privacy,* published in 1980. But twenty-five years of subsequent experience now provide much richer possibilities for answering them. Privacy protection efforts now have several decades of history behind them—including a steady stream of confrontation between privacy protection principles and constantly expanding demands of institutions to increase use of personal data. How have the principles fared in these tugs-of-war?

More bluntly: have legislation, court decisions, or institutions created to protect privacy succeeded *at any point* in resisting the full force of institutional demands for personal information? Can one point to *any* cases in which privacy measures have blocked exploitation of personal data of capital interest to an established government agency or private-sector organization? If so, what conditions have permitted privacy strictures to succeed against the

prevailing flow of personal information to the most resourceful interests? And if not, what hope can there be for other privacy guarantees?

Of course, the American story is not the only one in these respects. Indeed, privacy-watchers around the world have come to regard the United States as the bad boy on the block in matters of privacy protection.[15] Other major democracies, most would agree, have made more serious efforts to protect citizens' interests in the fate of their personal data than has America. Nearly all the others have created national agencies dedicated to privacy protection, and nearly all have at least somewhat more restrictive laws as to what can be done with personal data.

The pages to follow compare the state of privacy and its protection in America to those prevailing in Australia, Canada, the UK, and France. Each of these countries furnishes at least a bit of heartening privacy news compared to the American situation. And direct comparisons are eminently possible: the pressures on privacy evident in the United States are felt worldwide—arising from efforts to pursue terrorists, curtail crime, collect taxes, allocate credit, regulate drivers and driving, sell insurance, and on and on. Moreover, the technologies and management strategies for exploiting personal information to these ends are now globally available. What can be accomplished in one country can equally well be done elsewhere—at least, from a technical viewpoint. Thus the question: how have these other democracies fared in the enforcement of privacy protections? Where and how have their political and legal strictures withstood the pressures for appropriation and use of personal data that have flourished so abundantly in the United States? Are their commitments to privacy indeed more deep-going and forceful? Or—in a darker interpretation—are they simply less far along on a global conveyor belt that ultimately promises to make America the world's model for the fate of personal information?

At least we live in the most interesting of times in these respects. The upwelling of new pressures on privacy over the last forty years could hardly have been more dramatic. The rise of cyberspace, mobile telephony, and nearly universal reliance on credit and debit cards has created cornucopias of actionable personal data to tempt the surveillance appetites of institutions. And on the demand side, the flourishing of consumer economies and the events of

September 11, 2001, have whetted institutional appetites for more and more personal information. In response, privacy advocates have often assumed defensive stances, hard-pressed to justify any limits on access to data that could, in principle, make the difference between economic growth and stagnation, or life and death.

If privacy indeed has a future, we should be able to read it in the global response to these challenges.

Part II ■ ■ ■ ■ ■

Government Surveillance

We have a very definite rule in the bureau that any employee engaged in wiretapping will be dismissed from the service of the bureau. . . . While it may not be illegal, I think it is unethical, and it is not permitted under the regulations by the Attorney General.

—J. Edgar Hoover in 1931,
responding to Congressional queries on FBI policy

Governments may seem to come in as many varieties as humanity itself. Yet there are a handful of things that nearly all governments strive to do.

They seek to control territory, demanding compliance with government writ, ukase, law, or decree, while fending off competing demands from foreign powers or domestic usurpers. Governments offer protection from random fraud and violence—at least to their compliant subjects. Governments extract resources—taxes, tribute, and military service, among other things—from the governed. And they redirect those resources into policies and projects—from social security schemes to pyramid-building—that inevitably favor some interests at the expense of others.

Beyond this short list, universal features of governments are scarce. Over the ages and in different parts of the world, governments take the most disparate forms and play the most varied roles in social life. Some remain remote from the everyday lives of most of their subjects. Others—particularly

in today's "advanced" societies—cultivate intimate involvement in their affairs.

These differences are often linked with matters of *information,* especially personal information. What governments can know about their people—about their family situations, their wealth or lack of it, their political inclinations, or indeed their whereabouts—has everything to do with what laws can be upheld, what revenues can be extracted, and what forms of compliance will be forthcoming from the governed.

The options available to Henry VIII in sixteenth-century England were sweeping for his time. He could disestablish the Catholic Church, plundering its monasteries and executing its active defenders when it made trouble over his marital strategies. He could enact the Treasons Act of 1534, making refusal to recognize his headship of the newly established Church of England punishable by death. But he and his government could only keep track of a small minority of the governed—that is, the most vocal and visible—at once. The state could hardly "reach down" into the masses bent on avoiding official attention to identify who favored state policies at the grass roots and who did not.

By twentieth-century standards, Henry was a blind giant. Modern regimes maintain much more comprehensive, precise, and discriminating lines of contact with, and influence over, the governed. In the raising of armies, the monitoring of political support, the control of people's movements, and collection of revenues, modern regimes extend their influence more deeply and directly throughout their populations. They know who nearly every one of their people is, and a good deal about what they've been up to—including how to make life uncomfortable for those who don't play by the rules of the state. Compared to the regime of Henry VIII, the control exercised by modern states is like microsurgery versus the ministrations of a sledgehammer-armed gorilla.

Consider how far we have come from a not-so-ancient mode of revenue collection, *tax farming.* Until a few centuries ago, rulers of any large territory faced intractable problems in extracting taxes from their people. Even if government power were in principle absolute, the challenge of separating uncooperative subjects from their wealth was daunting. Central powers often could not determine who had resources to squeeze; when they did, they often lacked local muscle and savoir faire to do so.

Their response was simply to sell the concession to collect taxes to a local or regional enforcer—the tax farmer—often the meanest baron or most

intimidating magnate on the block. The tax farmer would wring what the traffic would bear from the governed and keep the change. For the local population, these arrangements meant a steady stream of offers they could not refuse, with considerations of justice and equity secondary at best. Tax farming was about as inspiring to contemplate as the making of sausage. But for centuries it worked better than any alternative.

We citizens of modern states do not expect public revenue to be collected this way. Disputes between tax collectors and taxpayers are of course endemic, but the latter need not contend with the whims of profit-seeking tax-collecting entrepreneurs. Tax obligations are legally defined. Each person's liability is based on fine detail of his or her income, financial obligations, dependency status, and a host of other circumstances—all these considerations requiring recourse to authoritative personal records. To be sure, modern governments can and do mobilize their tax systems to make life miserable for political opponents. But there are legally prescribed limits—limits both to what the system can exact from any one taxpayer, and limits to the ability of any taxpayer to evade or ignore the system.

Getting over tax farming was not easy. Many new institutions and mindsets had to be in place before modern revenue systems were even thinkable. One prerequisite was creation of a corps of professional government administrators—a bureaucracy that could be trusted to collect the regime's revenues by the rules, without helping themselves first. But another, obviously, was the development of personal information systems—sources of actionable personal data that would enable officials to know the identities of the citizenry, their whereabouts, their resources, and their circumstances. In the words of Yale political scientist James Scott, populations had to become "legible" to their rulers—identified, enumerated, and located so that demands for tax compliance could be precisely targeted.[1]

There is a lot to say for modernity. Offered the chance, most of us would never opt for having our taxes farmed—just as we would probably prefer modern forms of law enforcement, social welfare provision, and other state services based on precise determinations of our personal situations.

Indeed, we often demand just such discriminating treatment. We don't like paying taxes, and we readily invoke "the record" to show how our particular circumstances limit what we owe. Simultaneously, we are apt to insist that our government vigorously prosecute tax evaders and cheats—so that we pay no more than our fair share. We also insist, with greater or less passion, on

protection from criminals, dangerous drivers, welfare cheats, undocumented immigrants, and other unwelcome visitors from abroad—all of which performances fuel new demands to collect and use personal information. As we insist on these things, we rarely reflect what a remarkable or recent thing it is, to live under governments capable of such discriminating enforcement.

But the twentieth century also amply demonstrated that what governments can do for their populations, they can also do *against* them. Totalitarianism, many have pointed out, is a distinctly modern phenomenon. Henry VIII's England—or the Roman Empire or Louis XIV's France—were massively oppressive and unjust. But the distance between those regimes and their ordinary citizens provided shock absorbers not available under Hitler and Stalin. As governments have come to track the lives of individual citizens more closely, and deal with each one more directly, all sorts of destructive possibilities arise, along with attractive ones.

Surveillance systems created for the most banal or even benevolent purposes can readily serve as instruments of oppression. A classic example occurred in the German occupation of Holland during the Second World War. The Nazi forces discovered that Dutch census registries included data on people's religious preferences—information that took on sinister significance to a regime bent on deporting Jews to death camps. Attempts to block exploitation of this eminently modern information source for purposes of human extermination took drastic form. As one eye-witness account recalls, "Attacks by resistance fighters against population record offices were heroic feats to save people, as was the precision air raid carried out on 11 April 1944 by the 63rd RAF Squadron . . . as a result of which 250,000 personal records were destroyed. The author vividly remembers this spectacular act of 'international data protection.' "[2]

No doubt these same administrative records might have served, under different historical circumstances, all sorts of beneficent purposes. But incidents like this remind us that surveillance capabilities are morally neutral—that systems for orienting state power to individual lives can serve any purpose that prevailing political climates dictate, life-giving or the opposite.

Such realizations clearly weighed heavily in the impetus toward privacy protection measures in Europe. Perhaps because of living memories of atrocities like the one cited above, Northern European countries were the first to enact privacy codes in the 1970s. As the year 1984 approached, and as computing became an everyday tool of government, the warnings in George

Orwell's classic work helped inspire privacy legislation in virtually every prosperous democracy. Underlying these many national privacy codes were the principles of fair information practices shown in table 1 in part I—intended to safeguard citizens against excessive attentions from their governments, as much as from the private sector.

What has come of these efforts? How have those precepts fared in competition with other urgent aims of governments? Has the application of fair information practices over nearly forty years made a significant dent in the broad advance of mass surveillance? The "War on Terror" has obviously tested privacy restraints all around the world—often with the United States leading demands to dismantle them. But in response to these obvious pressures on privacy, have there been significant national differences? Or are those countries providing better privacy protection at this moment simply taking a different route to a common, privacy-unfriendly destination?

Government Surveillance in America

Of course, tensions between governments' efforts to monitor the governed and efforts of the latter to resist are not new, in any democracy. In the United States, anxieties about government penetration into private life led to adoption of the Bill of Rights in 1791. These first amendments to the Constitution were intended to reassure the anxious, newly born republic that the powers of the federal government would be circumscribed. The first amendment, guaranteeing freedom of expression and opinion, aims to provide protection from repression of publicly unpopular or politically repugnant views. The fifth amendment affords protection from government requirements that people produce information against themselves.

The fourth amendment, perhaps most centrally, aims at security of people's "persons, houses, papers and effects" against "unreasonable searches and seizures." And in a final effort at reassurance, amendments nine and ten specify that the naming of these and other rights does not grant the government rights that are not so specified, which "are reserved to the states . . . or the people." So it is true, as often noted, that the Constitution recognizes no right of privacy by name. But with the Bill of Rights included, it clearly does seek

to protect an array of what twenty-first-century Americans would readily bracket as privacy interests.

Of course, those who penned the Bill of Rights hardly anticipated the world in which present-day Americans struggle to apply these principles. They could not have imagined what we take for granted: a kind of dual universe, where events, transactions, statuses, and relationships that define everyday life have their shadow counterparts in written and electronic markers captured and maintained by large institutions. This documentary reflection of reality-as-we-experience-it increasingly shapes our real-world existence—in ways that challenge any principled limitation of state power. When, where, and how should state agencies be empowered to delve into this parallel world?

We can thus think of the government surveillance in America as reflecting two quite different dynamics—one fully anticipated by the authors of the Bill of Rights, the other not at all. First is the fluctuation in political climates, between those favoring stronger state monitoring of the lives of Americans and those favoring individual rights over and against government claims. Second is the unfolding of the parallel world of written and electronic representations of Americans' lives—and the technological and management expertise for manipulating them. The former swings back and forth with a certain regularity in American history. But the latter forms a unidirectional trend—toward more actionable information, more ingenuity in accessing and interpreting such information, and more use of such data to gain compliance from the governed.

Documenting the American People

At the founding of the republic, few people's lives left much of an enduring trace beyond local reputation. Americans' births, weddings, and deaths were documented in parish records. Local governments recorded property ownership and taxes levied on that property. But other records of individuals' lives must have been very rare—and occasions for state action based on them even rarer. True, the federal government issued passports to those who requested them. But Washington did not consistently require their use by Americans entering or leaving this country until the twentieth century. In its early decades, the American state simply had few claims upon individual citizens, or obligations to them, that would have required documentation of their circumstances.

The growth of such relationships began slowly. Veterans of the Civil War had the right to pensions, as did their widows. But claims for these pensions seem to have been supported by affidavits based on attestations of service made after the fact. The age had not yet come in which military life automatically generated a steady stream of personal records documenting the facts of service. Still, expectations that *everyone's* life would be recorded in ways subject to state monitoring and action were aborning.

In 1903 Congress passed legislation urging states to establish a universal and uniform system of birth and death registration. It was not until the 1930s that most states were in compliance with this legislation. Another pressure toward universal documentation came with the need to administer the income tax—instated, after two contentious false starts, in 1913. Obviously any effort to enforce this tax required state monitoring of private incomes; not surprisingly, government steps in this direction initially met with indignant resistance.[3] Initially, though, only a minority had incomes high enough to be taxed. Immediately before World War II, about six and a half million Americans were paying income tax; by wartime, that figure swelled to forty-eight million, or about 60 percent of the adult population.[4]

Social Security was the second system to bring the American population close to total coverage under mass surveillance. Founded in 1936, Social Security issued unique numbers to, and instituted records on, some forty-five million Americans in its first year.[5] Those steps brought about a surge in IRS activity, since payroll taxes for Social Security were collected by that agency. At its inception, Social Security numbering triggered considerable anxiety from labor interests fearing that employers would use the number to identify and blacklist union sympathizers. Elaborate assurances were offered that Social Security numbers would be used only for social security purposes and that personal information documented in that system would not be disseminated outside of it. By the end of the twentieth century, of course, Social Security numbers were used for a vast array of purposes, from student registration in schools and universities to consumer credit and medical care delivery. For tax purposes, parents are now required to obtain Social Security numbers for newborns within weeks of their birth.

By the middle of the twentieth century, these pervasive and interacting developments had brought about a sea change in the role of personal documentation in American life. In this new order, existence of government documentation on every American has become the default condition. Somewhere,

an authoritative record of key life junctures *has to exist* on virtually every American. Any adult today claiming to be a native-born U.S. national yet lacking such documentation must be assumed to have lived a very peculiar life—or to be concealing something.

Increasingly, government agencies can search passport records, domestic flight lists, and countless other databases designed to bring crucial information to bear on decisions on the persons concerned. Moreover, systems like Social Security and income taxation embody two features greatly strengthening government surveillance. One is that they regularly generate new actionable information on the finances and activities of each wage earner. Another is that these systems make each citizen available for government attention and action through his or her place of work. Implications for government agencies' ability to reach down into the population and enforce their claims are far-reaching.

Consider America's "Parent Locator Service" (PLS). This system, dating from 1976, aims at tracking parents who abscond from child-support obligations and enforcing those claims. It was founded in response to demands by custodial parents and—perhaps more significantly—from public welfare agencies burdened with supporting the children of absent parents. These politically potent influences easily overrode privacy concerns—and earlier expectations that record-keeping powers of Social Security and the IRS would be used only for their original purposes. Once located through the PLS, absconders can be served with orders for payment or their salaries garnisheed. Where that does not suffice, the system can also authorize denial of passports to those seeking to flee its attentions. Gleeful Congressional supporters of the legislation in the 1970s dubbed it the "runaway daddies act."

But the default condition of universal coverage by government surveillance has effects well beyond government activity, narrowly speaking. It is now an axiom of American life that virtually every consumer must file income tax returns—and these returns must document full and accurate details of one's financial situation under force of law. This knowledge makes it attractive—actually, irresistible—to nongovernmental interests to "piggy-back" their surveillance activities on those of the state. Applicants for everything from mortgages to employment to college scholarships are accordingly expected to furnish authentic copies of their tax returns. People are always free to decline such requests—much as they are free not to provide personal documen-

tation to support applications for credit cards, passports, or access to air travel. The results of exercising such freedom of course are foregone. In a world where everyone knows that everyone's economic affairs are authoritatively documented, refusal to produce such documentation is tantamount to declaring that one has something to hide.

Imagine that the 2004 Bush administration plan to create a central archive of all Americans' medical information succeeds. The resulting pressures to share one's official medical files would be identical to those pressing for access to, or release of, one's tax returns.

Today strategists for American government agencies, like those in other modern states, can assume that all those they deal with are documented in certain highly predictable, and highly useful, ways. We have made the fateful transition from a world where documentation of life events, if needed, had to be generated after the fact—by active search of parish registers, for example, or by attestations of witnesses—to one where records of key life junctures can be assumed to exist and to be available quickly and cheaply.

Constitutional Privacy Protections

The fourth amendment to the American Constitution famously protects the sanctity of "personal papers" from government seizure without court warrant. But when are papers "personal" in this sense—as distinct from personal information that might be found in the daily press, court or parish registers, or in the hands of banks or business associates? The language of the Constitution itself gives little guidance on these questions, leaving subsequent courts to decide.

For decades prevailing legal doctrine had it that fourth-amendment protections extended only to the physical limits of one's home. "Papers" and other personal information held in safety deposit boxes, merchants' records, medical repositories, or one's place of business could be accessed without court orders. In the 1928 *Olmstead* decision, the Supreme Court applied that doctrine to eavesdropping, holding that unauthorized monitoring of phone conversations did not violate fourth amendment guarantees, unless it involved physical intrusion into the target's premises. Thus only wiretapping accomplished by physically inserting something inside a dwelling—a microphone affixed to an exterior wall of a house by a spike, for example—required a court

order. In a world where lives were already coming to be recorded in countless far-flung locations outside the home, and where telephone communication was becoming universal, this was not a privacy-friendly doctrine.

Thus today, records held by banks, credit card companies, telephone companies, and many other providers of accounts and services are not considered "personal papers" in the sense protected by the fourth amendment. Since at least 1970, all checks processed by all American banks have been required to be microfilmed, with the records held for future inspection by the IRS and other law enforcement agencies. Access to these records by government investigators requires no court order and need not be revealed to the individual targeted.[6] Of course, a privacy-minded citizen could protect access to his or her information by avoiding banks, credit card companies, and telephone connections—paying only in cash, perhaps, and relying only on public phones and public library e-mail connections, for the sake of relative anonymity. But the result would be a life so atypical as to attract attention.

In the 1967 *Katz* decision, the Supreme Court reversed itself on some of these points. Raising a principle of potentially far-reaching significance, it held that fourth-amendment protections extended to telephone communications, where there was a "reasonable expectation of privacy" among the parties. Courts have interpreted this doctrine to protect the *contents* of phone and e-mail communications, while leaving what specialists call "connection information"—details of phone numbers called or e-mail addresses sent to, or the durations of the communications—much less protected. In practice, this has meant that police or other investigators could monitor such connection information largely at their own discretion. By contrast, monitoring of contents of calls and e-mails, in criminal investigations, requires a court order.

The doctrine of "reasonable expectations of privacy" is beset with ambiguity, not to say logical confusion, both in theory and application. What rationale warrants the conclusion that phone users have no reasonable expectation of privacy regarding the identities of those with whom they communicate? Other interpretations are still more far-fetched. As privacy scholars Paul Schwartz and Joel Reidenberg point out, the courts have ruled that observations of marijuana growing carried out from low-flying helicopters did not violate "reasonable expectations of privacy."[7]

But if the doctrine is anomalous when applied to established privacy regimes, it breaks down completely when confronted by qualitatively new

forms of personal data—those from website visits, text messaging, cell phone use, or other novel activities. Here expectations, reasonable or not, have hardly had the chance to arise. What expectations of privacy do people have in their use of ATM machines, the Internet, cellular phones, or automated toll roads and bridges? Other areas of law, it is true, also predicate crucial distinctions on the experience of ordinary actors—for example, prevailing community standards for defining pornography. But such possibilities soon reach their limit. Beyond that point, courts and legislatures must *prescribe* boundaries—in this case, between public and private personal data.

But while courts puzzled over questions like these, political realities supervened. By the middle of the twentieth century, the United States was preoccupied with the Communist threat. Not long after, agitation for racial justice and against American nuclear policies spawned movements that many regarded as no less threatening. Under these conditions, the FBI turned 180 degrees from the disapproving stance of J. Edgar Hoover in the quotation above, launching massive campaigns of unauthorized wiretapping and other illegal forms of surveillance.

The targets were mostly suspected Communists, Civil Rights workers, and other opponents of mainstream political directions. Often, as in the FBI's infamous COINTELPRO program, activities extended beyond mere surveillance to include use of data collected in earlier investigations to embarrass individual activists or disrupt cooperation among them. Many of these activities were widely understood in government circles to be illegal. But the FBI correctly assumed that, under the climate of the times, they would be tolerated.[8] Thus it is probable that the FBI and other federal investigative agencies effectively had free rein of the growing array of files held on virtually all Americans by public and private institutions—from the IRS and Social Security Administration to banks and telephone companies.

Watergate and Post-Watergate: The Reform of Surveillance

By the mid-1960s, anxieties over domestic subversion were losing their grip on public opinion. Spurred by the Civil Rights movement, opposition to the nuclear arms race, and—eventually—protest against the Vietnam War, many Americans withdrew their blanket confidence in the country's elites. All forms of established authority found themselves subjected to new skepticism. These trends culminated in the Watergate scandals—triggered in large measure by

revelations that the Nixon administration had sought personal data held by federal agencies to track and harass political enemies.

By that point, Americans were only too willing to believe that knowledge granted power in matters of personal data and that Washington had abused precisely that form of power. Eventually, even Richard Nixon realized that he had struck a tender nerve and sought to redeem himself by creating a national task force on privacy protection. But the gesture came too late. Nixon was swept from office in a tide of public indignation over illegal federal data gathering—both in the Watergate offices of the Democratic Party and on ordinary Americans. In retrospect the Watergate scandal, and the public mood it triggered, represent the high-water mark of privacy concern in American public opinion.

Privacy forces, led by Professor Alan Westin among others, pressed their advantage by passing the Privacy Act of 1974—still the most important federal legislation on privacy in the United States. This victory was hardly complete. The Privacy Act applies only to "administrative" data held by federal agencies, excluding investigative activities like those of the FBI. The original draft legislation would have applied to the private sector as well as to government record-keeping and would have established a permanent privacy protection agency of the kind now universal in nearly all other advanced democracies.[9] But the Ford administration managed to deflect these provisions by referring them to a study commission—apparently on the shrewd calculation that privacy fervor would have subsided by the time any commission could formulate its recommendations.

As a result, the Privacy Act of 1974 remains to this day America's closest approximation to *omnibus* federal legislation—that is, to law like that prevailing in other democracies. Other federal privacy legislation targets particular industries or practices. It regulates treatment of personal data in settings like consumer credit or medical care but establishes no broad rights for treatment of personal data in all settings.

The Privacy Act follows principles first laid out in America's Fair Credit Reporting Act (1970) and the influential government report *Records, Computers and Rights of Citizens* (1973). It requires that federal agencies maintaining personal record systems publicize that fact; it stipulates that such records may be kept only as necessary to achieve agency goals; and it creates procedures for individuals to challenge the relevance, completeness, and accuracy of data held on themselves. These precepts are of course consistent with

the consensus principles that have subsequently guided privacy protection measures around the world. And the Privacy Act also contains another potentially far-reaching injunction: that records held by federal agencies must not be released "to another agency, except . . . with the prior written consent of . . . the individual to whom the record pertains. . . ."[10] This attempt to *partition* federally held personal information so that agencies use it only for the purposes for which it is provided would represent a major shield to privacy interests—if only it were taken seriously.

But in fact, this key element of the law has virtually been interpreted out of existence. First, the Act does not apply to investigative agencies. Second, and even more devastating to the drafters' original intent, the language exempts "routine uses" of personal data from this requirement. The law defines such uses as "the use of such a record for a purpose which is compatible with the purpose for which it was collected."[11] In practice, federal agencies have succeeded in bracketing nearly any form of interagency sharing a "routine use." Thus, as in other countries' privacy codes, seemingly explicit privacy safeguards have been interpreted to mean virtually the opposite of what they state.

Still, the Privacy Act has proved remarkably resilient in the face of post-9/11 pressures. Patriot Act provisions that ensure government investigators access to virtually any *privately held* personal data sources do not trump Privacy Act protections. Anti-terrorist investigations have not been defined as "routine uses" of personal data held by agencies like Social Security, the IRS, and the Census. The only conceivable avenue available to investigators for obtaining such information would be a court order against the federal agency holding such data. But as James Dempsey of the Center for Democracy and Technology notes, ". . . I think it is quite out of the question that the FBI would use . . . [the Patriot Act] against another federal agency. It is unheard of for one federal agency to get a court order against another federal agency unless the target agency was engaged in criminal conduct."[12]

Another repercussion of Watergate was the investigations of the committee headed by Senator Frank Church. Aimed at bringing to light illegal surveillance by the FBI and other agencies from the 1950s to the early 1970s, the report concluded, "*Domestic Intelligence Activity Has Threatened and Undermined The Constitutional Rights of Americans to Free Speech, Association and*

Privacy. It Has Done So Primarily Because The Constitutional System for Checking Abuse of Power Has Not Been Applied."[13]

In an environment already charged with public outrage at abuses of government surveillance powers, these words intensified pressure on Nixon's appointed successor, Gerald Ford, to seek reforms. Ford named Edward Levi as Attorney General. Levi took office with a mandate to rein in illegal activities by the FBI by bringing it under Justice Department control. Critics have doubted how decisive the much-noted "Levi guidelines" actually were in terms of legal force; they did not, after all, prevent FBI agents from gathering data purely on suspicion that citizens' political beliefs might later incline them to illegal political activities.[14] But they did usher in a period of relative restraint by FBI investigators.

The Levi reforms enjoined the FBI to adhere to federal wiretapping laws, which had recently been strengthened and clarified by Congressional action in the 1968 Omnibus Crime Control and Safe Streets Act.[15] Title III of that Act requires judicial supervision of bugging and wiretaps and notice to the monitored parties *after* the expiration of the wiretap order. Permission to monitor contents of phone conversations, as distinct from data on numbers called and durations of calls, required a court order acknowledging probable cause of criminal activity. In 1986, the Electronic Communications Privacy Act extended these protections to other communications such as e-mails.

Crucial for privacy and civil liberties concerns was the Title III provision that targets of wiretaps be notified of the surveillance after expiration of the order. That measure, and the willingness of the Levi Justice Department to enforce it, were milestones in U.S. domestic surveillance policy. It meant that surveillance was not cost free for those who carried it out. Those who learned that they had been monitored after the fact could decry the action publicly, and *in extremis* sue, where they held that the surveillance lacked legal justification. Clearly the intent was a sharp turn away from the ethos of J. Edgar Hoover's heyday.

From FISA to the Patriot Act: 1978–2001

But some in Washington held these strictures inadequate to address the special threats of espionage. Not all information-gathering activities of foreign agents are necessarily illegal, they argued. Moreover, ability to track and monitor foreign agents could be hindered by requirements to seek warrants in

advance or by informing the targets of surveillance after the fact. On this rationale, separate procedures were created for surveillance of suspected foreign intelligence operatives, under the Foreign Intelligence Surveillance Act of 1978 (FISA). This legislation sought to create a distinct set of powers directed, in the words of the Act, at "foreign-based political organization[s], not substantially composed of United States persons," or groups "engaged in international terrorism or activities in preparation therefor."[16] Surveillance over such targets would require no notification after the fact; indeed, the intent would be to conceal the monitoring forever, unless the investigation yielded a prosecution.

A special tribunal, the Federal Intelligence Security Court, was created to monitor requests for wiretaps of those suspected of unfriendly actions on behalf of foreign powers. Such actions might range from efforts to steal military secrets to foreign countries' efforts to gather sensitive industrial or trade information.

Investigative agencies could apply to this court for warrants to wiretap or gather other data—orders never to be revealed to the targets of investigation. In addition, something less than "probable cause" of a crime had to be demonstrated; investigators needed only to show that "the purpose of the surveillance is to obtain foreign intelligence information."[17] The net effect was a special set of rules for foreign intelligence surveillance, circumventing the stronger safeguards of Title III. The FISA court would deliberate in secret, so that targets of surveillance would not be aware of the fact unless ultimately prosecuted. Nor, of course, would the public have the opportunity to evaluate appropriateness of the permissions that it granted after the fact. Law Professor Peter Swire notes that FISA wiretap orders had by 2003 risen to a total of 1,727; since early in the new millennium, they constituted a majority of federal wiretaps.[18] The FISA court rarely refuses investigators' requests for surveillance orders.[19]

This dual-track arrangement for federal monitoring and investigation thus represented a compromise—with significant civil liberties protections for normal criminal investigations and far slenderer ones for those involving foreign intelligence. As Peter Swire writes,

> . . . the 1978 FISA revealed a grand compromise between the advocates for civil liberties and the intelligence community. From the civil liberties side, FISA had the advantage of creating a legal structure for

> foreign intelligence surveillance that involved Article III judges. It had the disadvantage of having standards that were less protective overall than were constitutionally and statutorily required for investigations of domestic crimes. . . . From the intelligence perspective, FISA had the disadvantage of imposing bureaucratic rules and procedures on searches that had previously been done subject to the inherent authority of the President or the Attorney General.

He adds, "To describe the compromise another way, FISA set limits on surveillance by 'The Lawless State,'" citing the title of a book exposing the surveillance activities of the Hoover era; "but gave 'The Lawful State' clear rules that permitted surveillance."[20]

The "inherent authority" that Swire mentions is the legal doctrine that the president may order wiretapping and other coercive government enforcement without approval from any other branch of government. Since 2001, the Bush administration has invoked this doctrine to great controversy in prosecuting its War on Terror.

The FISA compromise invited tensions between the interests of criminal investigators and those doing counter-espionage. The former were bound to envy the latitude that FISA accorded the latter. The result was built-in temptation for criminal investigators to redefine their work as targeting foreign intelligence. Since both categories of investigators were apt to be FBI agents, inevitable pressures arose to obtain data from FISA investigations for criminal prosecutions. To counter these tendencies, the Justice Department created the Office of Intelligence Review and Policy (OIRP) within the FBI to supervise communications between intelligence and criminal investigators. The result was a communications filter subsequently characterized as "the wall" between domestic and foreign intelligence.

In fact, this office never constituted an absolute barrier to information flow. The OIRP ensured that requests to FISA investigators to invoke its more sweeping powers be used only for counter-espionage. It did not, as some public comments following the September 11 attacks have implied, prevent criminal investigators from bringing their findings to the attention of intelligence investigators—the one exception being results of grand jury investigations. But it did serve to prevent FISA orders from serving as a Trojan Horse for investigations unrelated to foreign intelligence. Given the rarity with which

the FISA court declined requests it received, it is easy to see why some such effort was held necessary. As Peter Swire put it, "... the wall has existed since the creation of FISA in 1978, but there has always been a gate in it."[21]

This balance of forces remained in place until the terrorist attacks of September 11, 2001—though apparently with increasing pressure from government agencies seeking wider surveillance powers. September 11, everyone would agree, marked another sea change in American surveillance, comparable to the one following Watergate and the debacle of the Nixon administration. The Patriot Act, hurriedly passed within weeks following the attacks, greatly expanded the prerogatives of federal investigators engaged in foreign intelligence investigations—definitions of which it markedly broadened. Commentators have suggested that the details of this complex and far-reaching expansion of investigative powers were prepared and ready to be put forward before the events of September 11—as surveillance interests awaited an auspicious moment. In this view, the conscious aim was to redress constraints imposed on federal investigators in Watergate-era reforms.[22]

The Patriot Act widens the circumstances permitting FISA surveillance orders. Instead of allowing secret monitoring of communications only for investigations declared to have obtaining foreign intelligence information as their "primary purpose," Patriot Act language permits such investigations where such intelligence was "a significant purpose."[23] Rather than requiring that a FISA court approve specific monitoring plans, federal investigators are simply required to declare their efforts to be part of "an authorized investigation ... of international terrorism or clandestine intelligence activities."[24] The new act also removes the alleged "wall" between criminal and foreign intelligence gathering by eliminating requirements that investigators in the two categories communicate only via the FBI's Office of Intelligence Review and Policy.

Further, the Patriot Act vastly broadens access of federal investigators to documents—physical records, computer files, and any other documentation that might be useful to their investigations. These include, most controversially, records of library or bookstore choices, but also business records, telephone records, records held by landlords, psychotherapists, or any of the vast numbers of other data that Americans now generate in everyday living.

Note that targets of these orders need not be considered participants in foreign subversion. At their discretion, investigators may seize *any* personal data that might relate to an "authorized investigation"—regardless of the involvement of the person concerned in suspect activities, or lack of it.

The act also makes it possible to impose "gag rules." For example, it enables investigators to invoke "National Security Letters" as bases for accessing materials sought in their investigations—virtually at their discretion. Once served with a National Security Letter, holders of data sought by investigators are forbidden from disclosing the investigation to anyone. Again, invoking these powers requires only that the agents declare their investigation directed against "international terrorism or clandestine intelligence activities."[25]

Thus we have a regime utterly different from that under Title III domestic surveillance ground rules. There monitoring is authorized for limited periods, and monitoring orders are ultimately announced, both to the targets and the public at large. The effect of the gag rule is to keep this broad branch of surveillance activity off the radar screen of public debate and deliberation.

In response, the American Library Association recently gave an "intellectual freedom award" to one of its members identified only as "John Doe"—a Connecticut librarian served with a National Security Letter accompanying a demand for patron records. By divulging receipt of the letter in order to protest the Patriot Act, the librarian and his employer were breaking the law. "Though some 30,000 national security letters are issued a year without arousing public protest," the *New York Times* commented, "the librarian was reluctant to comply because of professional ethics aimed at keeping library records confidential."[26] Of course, the other 29,999 letters are unlikely to arouse public protest, because their recipients were under legal compulsion not to disclose them.

Officially, investigations under the Patriot Act are directed against real or potential international threats—though definitions of such threats are far more vague and sweeping than under earlier law. The act does retain the distinction between requirements for criminal investigations and those of foreign activities. But the broad and encompassing language of the Patriot Act opens the possibility that many routine law enforcement activities could find justification under its sweeping powers. As Peter Swire points out, much ordinary crime, from drug trafficking to entry of illegal aliens to money laun-

dering, involves some foreign participation. Should such foreign connections be held to justify application of Patriot Act discretion for investigators, the result will be vast expansion of police surveillance powers. Who, after all, could rule out the possibility that broad ranges of ordinary police investigations *might* yield evidence of foreign involvement?

The Patriot Act has greater impact than it would have had a few decades before, because of changes having little to do with politics. The evolving strategies and technologies of mass surveillance simply multiply possibilities for monitoring almost any American's life—for political purposes or any other. Profit-driven computerization of long-existing but difficult-to-access data sources has enabled companies to create and market comprehensive portraits of ordinary citizens' affairs. Prepared-to-order investigative reports on virtually anyone are for sale to virtually anyone willing to pay, without even the limited constraints imposed by credit reporting regulations. Sources of data for these reports range from market researchers' databases to courthouses and public record offices to credit and insurance records.

The surveillance initiatives stemming from the Bush administration's War on Terror have been a boon to these companies. As *Privacy Times* editor Evan Hendricks recently put it,

> Information resellers like ChoicePoint are doing a brisk business selling personal data to federal agencies, according to a recent report by the Government Accountability Office (GAO). The GAO confirmed the concerns of privacy officials and advocates that the widening practice amounts to an end run around Privacy Act requirements and Fair Information Practice Standards.
>
> The leading purchasers were the Departments of Justice, Homeland Security, and State and Social Security Administrations. . . .
>
> The agencies spent approximately $30 million on contractual arrangements with resellers that enabled the acquisition and use of such information. In fiscal year 2005, law enforcers were the leading purchasers at 69 percent; counterterrorism offices were second at 22 percent.[27]

Where government surveillance itself does not reach, the free market serves.

Checkpoints

Governments do two kinds of things to locate and monitor the governed. One is actively to seek and capture traces of lives like those assembled by Patriot Act investigators—sifting through library records, cell phone logs, medical data, or any number of other far-flung but predictable sources. The second is to *create* junctures in life where citizens have no choice but to identify and document themselves. In some troubled places such *checkpoints* may take the form of literal roadblocks, where all who wish to pass must identify themselves to those in charge—and where the travelers remain vulnerable, until the authorities are satisfied. But in the information-intensive world most of us inhabit, the same principle can be served by creating subtler sieves through which populations must sort themselves.

The first, proactive investigations—those requiring active trolling of relevant records from libraries, courthouses, or supermarket shopping archives—are comparatively costly. At the very least, they require time and trouble to create hypotheses as to who might warrant investigation and where their electronic or documentary traces might be located. Reliance on checkpoints is often much more cost-effective. There state agencies can simply subject all who pass to electronic checking aimed at revealing the full detail of records compiled elsewhere.

Since at least the 1980s, U.S. authorities have developed one such routine for tracking suspect financial transactions—under a Treasury Department system called FINCEN, the Financial Crimes Enforcement Network. This is a network of databases drawing on transaction records from a variety of financial institutions, including banks, casinos, brokerage firms, and other institutions handling large amounts of money. Positive self-identification is increasingly required for transactions with these institutions. The latter are required to file reports on all transactions meeting certain criteria, including all cash transactions greater than $10,000—including multiple transactions totaling that amount. Less routinely, the institutions must also file a "Suspicious Activity Report" (SAR) for other transactions (or series of transactions) that appear likely to be associated with fraud, terrorist financing, or money laundering. These reports must be kept secret from those being reported on.

The effect of these requirements—as of their many counterparts in other countries—is to increase the points at which critical information on once-private activities are routinely made accessible to the state. Though obviously

spurred by anxieties over terrorism, they also extend enforcement powers over a variety of other domains of life in which nearly all governments claim an interest. The private institutions doing the reporting clearly undergo great expense to do so; in the United States they are subject to stiff penalties for inadequate vigilance in these respects.

Another such checkpoint where nearly everyone expects requirements to identify one's self to the state is at international frontiers. Again, today's rigor is relatively recent for Americans, who needed no passport to return to their country until well into the twentieth century. Even today, some travelers entering the United States by land may be waved on without presenting a passport—though Homeland Security officials appear determined to tighten this practice. But for those arriving by air or sea, passports or other authoritative documents are essential. More important, their use links the bearer to sophisticated computerized data systems enabling interested government agencies to *act* on information about people's movements in ways never possible under conventional record-keeping practices.

Since 1986, the U.S. Customs Service has relied on TECS, the Treasury Enforcement Communications System, to monitor movements of travelers into and out of this country. TECS is an umbrella organization, now managed by the Department of Homeland Security, coordinating the interests of more than twenty government agencies and friendly foreign governments in monitoring those entering and leaving the United States.

Much abetted by the development of machine-readable passports, TECS makes it possible both to record information about travelers' movements and to take action at that crucial point where travelers are under the control of government authorities. Virtually all international travelers arriving in this country by air now have their names entered in TECS—as do many travelers by land and sea. Should authorities so decide at the point of entry, actions taken can include immediate repatriation of foreign visitors whose presence is held undesirable. They also include arrest—for those wanted on foreign or domestic warrants where the jurisdictions are willing to pay costs of extradition. In 2006, TECS triggered more than eight thousand such arrests.

In other cases, TECS and its affiliated systems work much more unobtrusively—by noting entries and exits by persons deemed of interest to participating agencies, where no immediate action is required. Participating government agencies are entitled to have specific persons' movements brought to their attention. These are agencies deemed to have a "national security

interest" in tracking international movements of persons; the agencies range from the CIA to the Treasury Department, and include certain foreign countries. This capability enables the Bureau of Alcohol, Tobacco, Firearms and Explosives, for example, to monitor transborder movements of persons of interest without their awareness. Thus, a world of difference from the period when U.S. nationals could enter and leave their country without so much as showing a passport.

A much newer checkpoint is the one governing domestic air travel. Most Americans probably have forgotten that it was possible to book and use domestic air tickets under virtually any name one chose as recently as 1995. The requirement for "photo ID" established at that point set the stage for the post-9/11 checking routines agonizingly familiar to every American traveler. These activities are overseen by the Transportation Security Administration, part of Homeland Security.

Like other checkpoints, these permit several surveillance-related activities. Best known, of course, is categorical exclusion of those whose names appear on the TSA "No Fly" list—at least 20,000, as of 2006—from boarding their flights. These measures have attained notoriety, given evidently high rates of "false positives"—persons blocked simply because their names resembled ones appearing on the list. These cases famously include U.S. Senator Edward Kennedy, a four-year-old child, and many other obvious mix-ups. More troubling are the apparently intentional exclusion or detaining of persons seemingly identified for their outspoken criticism of government policies—including pacifist activists who appear the least likely of terrorists. These incidents have led some to suspect that the No Fly List and related federal watch lists are being used as instruments of political pressure.

The Transportation Security Administration is enormously secretive about the workings of the watch lists it uses. But given the pressures on privacy built into its institutional situation, it is hard to believe that exclusion from air transit is the only use of this vital checkpoint. After all, names of nearly all passengers are entered into the computerized record well before flight time. Accordingly, one has to assume that law enforcement agencies interested in tracking, questioning, or arresting specific persons must monitor these flight lists, so as to act when persons of interest pass through checkpoints. For similar reasons, one must assume that records of people's presence at the moment of their transit through the system, and the destinations revealed at that point, are subject to further use.

Given the tendency of surveillance systems to share information and support one another, plans for closer coordination of TECS and the TSA systems seem all but inevitable. Such co-ordination would obviously make it possible to track travelers' movements seamlessly inside and outside the country—generating comprehensive information of intense interest to many interested agencies and parties. Department of Homeland Security planners have already raised these possibilities in internal discussions, according to an interview with one of its officials.

The America where one could pass a normal life rarely presenting one's formal identification to anyone other than a traffic patrol officer is an increasingly distant memory. In junctures like those noted above, the significance of identification procedures does not lie simply in the fact that people are no longer anonymous. More tellingly, identification brings individuals into contact with far-reaching systems of government action. It's not just that the agent at the border, for example, knows your legal name, age, and other information included on the passport—or other data divulged to the airline or travel agent, including dietary preferences, typical weights of baggage checked, and on and on. It's that any agency participating in the system can learn of your presence, make note of your movements for future reference, and take action accordingly. The more points in life where one must identify one's self to such interlocking systems, obviously, the stronger becomes the grip of government on the governed. And no one can doubt that the number of such points is rising.

Late in 2005, Denver commuter Deborah Davis was arrested on a commuter bus for refusing to provide adequate personal identification to federal police, on a route passing near that city's federal center.[28] More recently, I myself was required to produce photo ID in order to purchase, for cash, a one-way train ticket from suburban Baltimore to Union Station in our nation's capital. I had to wonder whether an anonymous purchase would have been permitted had I requested a round-trip.

In light of these trends, efforts by Washington to set the stage for a national ID card system warrant special attention. In 2005, the U.S. Congress passed the "Real ID Act," aimed at pressing states to adopt uniform, Washington-mandated standards for issuance of driver's licenses. Participating states will be required to verify more closely than before the identities

of driver's license applicants, including their citizenship status. To meet "Real ID" standards, cards will have to be machine readable, so that authorities anywhere in the United States can immediately access information held on the bearer anywhere else.

The act, signed into law in May 2005, does not make it legally binding for states to meet these standards. But it establishes some powerful inducements. Under it, the federal authorities claim that they will not accept driver's licenses produced by nonparticipating states as legitimate "government-issued ID" for boarding domestic air flights or entering federal facilities. Still, Real ID has sparked significant resistance, both among liberals and states-rights conservatives. At the time of this writing, legislatures of at least two states, New Hampshire and Alaska, have voted not to participate in the scheme.

Proponents of Real ID claim that its only purpose is to ensure uniformity of practice across states. But its requirements for machine readability of licenses, and the linkages it will establish across participating state databases, point to something much more far-reaching. Licenses meeting these standards will be all-purpose federally mandated identification documents, usable for passing government checkpoints throughout the country—and in all likelihood for other purposes, as well.

Beyond the Patriot Act

In December 2005, the *New York Times* reported that President Bush had secretly authorized mass monitoring of Americans' communications within the United States—without warrants from FISA or other courts. The monitoring was the work of the National Security Agency (NSA), the Executive-branch agency normally responsible for monitoring communications outside the United States. The *Times* had learned of these activities more than a year before but had deferred publication after requests from the White House.

These revelations triggered a storm of public controversy. Congressional allies of the administration stoutly defended its actions as essential for national security. The Bush administration acknowledged the existence of its orders to the NSA and the subsequent surveillance. But it insisted that the resulting surveillance was legal under the "inherent authority to conduct warrantless surveillance . . . even in peacetime."[29] This is the same "inherent authority" claimed by the Bush administration—and disputed by most legal scholars—as a basis for many manifestations of its War on Terror.

The *New York Times* revelations certainly did not provide a bright day in the history of American privacy. Far from clarifying matters, they raised profound questions. What, exactly, was the aim of the NSA surveillance? Did the program involve capturing the content of communications, or did it focus mainly on patterns of connections—who contacted whom, for example, when, and for how long? And whatever the details of the surveillance, why did the administration find it necessary to sidestep the conspicuously permissive FISA court—known rarely to decline investigators' requests?

At the time of this writing, observers continue puzzling over these questions. There are several hypotheses.

One is that the aim of the surveillance was precisely *not* to focus on communications of suspected terrorists and their American contacts. Instead, the NSA operation could have been—and could still be—a vast data-mining effort aimed at identifying patterns in the communications of American citizens and residents not initially suspected of anything. Such patterns could in turn be compared to patterns of communication among known terrorists, in hopes of focusing attention on Americans who match terrorist profiles.

Such an approach would do no more than recapitulate longstanding surveillance strategies in other fields. Sellers of consumer credit and insurance, for example, in screening applicants for their business, seek to discriminate among them on the basis of similar statistical associations. Thus insurance applicants with poor credit ratings are quoted higher premiums, on the grounds that poor credit predicts more frequent insurance claims. Perhaps the NSA was seeking to establish such associations as bases for intensified surveillance of Americans who otherwise would have escaped investigative attention. Perhaps, in other words, the NSA was looking to identify otherwise unidentified Americans whose communication patterns resembled those of suspected or known terrorists.

Another, still darker interpretation would be that those subjected to the warrantless NSA monitoring were not even potential terrorist supporters—but that they were real or potential political critics of the Bush administration. At the time of this writing, there is no evidence of that intent. But the administration, at least as much as other presidencies, has mortal political enemies who have launched devastating criticisms of its policies in the War on Terrorism and elsewhere.

If the administration's intent were to use personal data available to federal investigators to punish and intimidate its critics, its actions would hardly be

unprecedented. The pattern would be no different from that of Nixon White House efforts to silence political enemies, or the Reagan administration's apparent use of tax audits to pressure critics of its Central America policies. It would, in short, join a long and disquieting tradition of Executive-branch repression of dissent via manipulation of personal data stretching back at least as far as the Palmer Raids following World War I.

Parallels Abroad

These pressures to intensify surveillance in America—and for that matter, countervailing efforts to defend privacy and other embattled interests—are evident in liberal democracies around the world. At the very least, the responses to these pressures demonstrate that technology is not destiny, as reactions in various countries have followed obvious parallels, without precisely replicating one another.

Great Britain

Great Britain famously has no written constitution, but it does have a common-law tradition of individual rights. Many observers have also noted that ordinary Britons appear more confident of their government institutions than do Americans. Equally well noted, over the last generation, is a sweeping turnaround in British attitudes toward surveillance. From a culture that mid-twentieth-century Americans found retiring and privacy-minded, Britain has evolved into a world of pervasive everyday surveillance—as motorists, pub-goers, and shoppers now expect their activities to be monitored via computer or video camera. To the distress of privacy-watchers, the application of traditional restraints of Britain's common-law constitution to these new surveillance possibilities has proved ambiguous, at best. The surge in these new surveillance possibilities since the 1980s has often exceeded its equivalents in the United States.

Consider UK government access to *private communications.* As everywhere, these forms of personal information draw attention from government agencies pursuing everything from petty crime to far-flung terrorist schemes. British law permits a wide range of investigators to monitor contents of communications—from letters to telephone conversations and e-mail messages—without court

order. Such monitoring is possible for a sweeping array of purposes, as specified under the Regulation of Investigatory Powers Act of 2000:

(a) in the interests of national security
(b) for the purposes of preventing or detecting serious crime
(c) for the purpose of safeguarding the economic well-being of the United Kingdom; or
(d) for the purpose . . . of giving effect to the provisions of any international mutual assistance agreement.[30]

Note the openness of these purposes—especially (b). Since prevention applies to crimes that have not yet occurred, authorities are encouraged to imagine which communications could culminate in crimes perhaps not yet contemplated even by the hypothetical perpetrators. Note, too, that orders required for such surveillance are not issued by any court; they are signed by government ministers, including the Home Secretary and the Foreign Secretary. The equivalents of many such searches in the United States would require court orders at the outset.

Authority to track *connection* data on electronic communications—details of who called or e-mailed whom and when, or of what websites someone visits—is even more widely dispersed. For an array of purposes somewhat broader than those given above, connection data may be monitored by dozens of agencies, ranging from the Metropolitan Police in London to the Scottish Ambulance Service Board. Normally only a request by a senior official of one of these bodies to a communications service provider—a phone or Internet company, normally—suffices for authorization of such monitoring. According to estimates by UK information scholar Ian Brown, agencies resorted to these forms of monitoring on roughly one million occasions in 2003.[31] Neither these activities nor the actual monitoring of communications contents need be revealed after the fact to the targets—as would be the case in Title III surveillance in the United States.

An enduring concern of privacy-watchers has been retention of communications records. As proportions of all communications that are computerized rise, and costs of data-storage decline, the source of these concerns is obvious. Living a normal life in the world's prosperous countries increasingly means leaving computerized markers of where one was, with whom one was communicating, and what one was doing. The question is, how long do these records remain available for government attention?

Here the climate triggered by the September 11 attacks has particularly left its mark in the UK. Before those events, the Data Protection Act of 1998 required companies to store such data no longer than necessary for business purposes—normally, about three months, or long enough to allow for billing and for customers to dispute specific charges. Following the attacks, the Anti-Terrorism, Crime and Security Act of 2001 granted the Home Secretary the power to require retention of these connection data by phone and Internet companies for periods ranging up to twelve months. While the legislation invokes national security needs, the Home Office has consistently asserted that information garnered from the retained data may be used for any of the purposes noted above.

The UK has been the major driving force behind the European Union Data Retention Directive of 2006. This requires all EU member states to adopt legislation requiring storage of these data for periods ranging from six to twenty-four months. The publicly avowed purpose is to facilitate investigations of suspected terrorist activities—and other forms of real or suspected wrongdoing of interest to the authorities. Both the UK Information Commissioner (the country's privacy ombudsman) and the EU Data Protection Supervisor have expressed concerns that the new data retention requirements are excessive—and that they accordingly violate both EU privacy legislation and other international human rights agreements.

Monitoring of citizens' *financial affairs* is another universal preoccupation of modern states. British government agencies reach into this domain of life nearly as readily as into communications data, though court orders are more widely required than in the situations described above. Police and other agencies involved in criminal investigations must obtain court orders for access to financial information for data on customers—from banks, credit card companies, accountants, solicitors, real estate agents, financial brokers, and others. The post-9/11 Anti-Terrorism, Crime and Security Act of 2001 grants police similar powers in connection with investigations into terrorism.

In addition, many private-sector interests are under legal obligations to report financial information on British residents that might indicate illegal activities. "Suspicious Activity Reports" (SARs) must be filed when any of a variety of institutions come into possession of personal information that could point to money laundering or other criminal or terrorist activity, particularly unusual financial transactions. Among those under obligation to make these reports are not only banks, but also accountants, auditors, real estate agents,

casino operators, solicitors, car dealers, and others. These provisions were further stiffened in 2000 and 2002, and then again by EU money-laundering legislation, implemented in 2003 and 2007.

These obligations to report "suspicious" activities effectively broaden the range of junctures in everyday life that directs actionable personal data to government agencies. The resulting onslaught of SARs—over 100,000 in 2003—has apparently overwhelmed the processing capacity of the authorities receiving them. The Treasury Department's interpretation of Britain's Data Protection Act of 1998 permits institutions reporting on private citizens in this way not to inform the targets of investigation that they have been monitored.

Many sources of financial information on Britons also serve government investigators' interests in *tracking individuals' location and movements.* Investigators obviously can and do use data from financial accounts—ATM use, for example, automated toll records, or credit card transactions—as well as those derived from cell phone use or even postal communications, to keep track of people's movements. In addition, of course, state agencies have long maintained databases to monitor persons entering the UK. In recent years there have been calls for screening passports of those leaving the country, as well.

But it is regarding movements *within* the country that the UK seems poised to establish surveillance supremacy among the world's democracies. Since the late 1980s, Oxford criminologist Benjamin Goold estimates, more than one million video cameras have been installed in public places around the country, with an estimated five hundred more added every week.[32] These installations appear to provide a sense of reassurance to many Britons—though studies suggest that they have little effect on crime rates except in circumscribed settings like indoor parking garages.[33] Most of these surveillance operations require human monitoring of video screens—a labor-intensive demand that reduces their usefulness for law enforcement. But further refinement of computerized face-recognition will enable authorities to automate tracking of specific individuals, including those wanted for arrest or simply for further attention.

A related refinement is automatic recognition of vehicle number plates; here British authorities have taken great advantage of new surveillance possibilities. Speed cameras are an increasingly common feature of UK roads, with around 1,000 sites active at any one time. The most sophisticated of the technologies in use can read (rather than simply photograph) number plates in real time. These latter systems are used to check traffic in and around

London's financial center, scanning for vehicles appearing on a computerized watch list that can then be subjected to further police scrutiny. Police have begun a saturation monitoring program on major roads, in an avowed attempt to make them off-limits to known criminals. In a national six-hour trial in May 2003, authorities scanned 60,000 number plates, leading to 1,000 reported offenses and 65 arrests.[34]

Relying on this same advanced technology is the Central London Congestion Charging scheme, which came into operation early in 2003. This system assesses extra charges for vehicles using the capital's most congested streets. Around 700 cameras are situated at more than 200 enforcement sites around London, with a further 64 mobile monitoring units. Vehicles entering and leaving the congestion charging zone are photographed and have their registration numbers checked. Plans call for using the same system to track terrorist suspects entering London; other British cities are weighing similar schemes.

Nor will using mass transit enable Londoners to avoid the attentions of mass surveillance. Travel on buses, the Underground, regional rail, and other public transport is payable through the Oyster Card, a stored-value computerized pass introduced in 2003 as a tool for quicker movement within the metropolis. Five million Londoners now use it. But some highly promoted uses of the card require users to identify themselves—so that subsequent movements paid via the card are subject to easy tracking. At most recent count, police had made some 243 requests to use the system's records for such tracking; 229 of these requests had been granted.[35]

Finally, the Tony Blair government has made it a priority to seek a major advance in surveillance—in the form of the high-tech ID card systems scheduled for introduction around 2008 or 2009. Under this much-contested system, Britons will be issued supposedly tamper-proof, machine-readable photo ID cards containing biometric data. More important than the card itself will be the databases to which it can be linked—including the National Identity Register, to include data on each holder's residence, citizenship, or immigration status, among other data. Presentation of the card will be indispensable for access to many government buildings, registration for services such as health and child care, the claiming of welfare payments, and overseas travel. It could also become necessary for such activities as withdrawals of large sums from banks and access to medical care.

The Blair government has expended vast political capital to secure adoption of this measure. For some Britons, it promises an opportunity to strike at

terrorists and illegal residents. For others, it represents an expensive and unnecessary threat. Certainly it is impossible to imagine any significant support for such a measure a few decades ago. Both the opposition Tories and the Liberal Democrats have pledged to abolish the scheme, should they come to power after the next scheduled election in 2009. Whether any party in power at that point will be able to resist support for the scheme among powerful surveillance interests in the country's bureaucracy remains to be seen.

Australia

Though Australia has a written constitution, it embodies no privacy guarantees. Restraints on powers of government to acquire personal information accordingly rest on specific legislation—including the Privacy Act of 1988 establishing Australia's Federal Privacy Commissioner.

That legislation stemmed from a privacy revolt in Australian public opinion even more pointed than that triggered by the Watergate era in the United States. In 1987, the Labor Party government introduced plans for the Australia Card, a state-issued identity card that was to be carried by all Australian citizens and residents. Holders of the card were to be required to produce it when needed by state authorities, for purposes ranging from access to welfare benefits to tax determinations.

Civil libertarians worried that the card, and the databases accessible through it, would undermine privacy by concentrating all available data in the hands of government officials controlling the system. A few privacy activists decided to go on record against the plan—without much hope of success. To general astonishment, resistance to the card claimed center stage in public opinion, gathering support from privacy defenders as diverse as recent immigrants and rock stars. After major public demonstrations and protests across the spectrum of public opinion, the flabbergasted government withdrew the plan. Like the Nixon administration in 1974, it sought to repair its image by introducing privacy legislation.

Neither that ensuing legislation nor any other legal protections, however, have substantially stemmed the rising availability of personal data to government authorities since then. As in all other rich democracies, evolution of the relevant technologies and management strategies has steadily generated more and more actionable personal data—with minimal legal restraint on state access to these new sources. And undermining such restraint has been

public shock at terrorist events, including 9/11 in the United States, and deadly terrorist attacks on Australians in Bali in 2002 and 2005.

Today Australian authorities generally have little difficulty accessing any recorded personal data that they identify as relevant to their work. Contents of telephone calls and electronic communications have long been subject to monitoring by law enforcement agencies on court order. But since the 1990s, orders from the government's Administrative Appeals Tribunal also suffice. Warrants were issued for some 2,800 interceptions of telecommunications data in 2004–05, up by more than a third since before 2001; about sixty of these warrants were for investigations of terrorism. As under FISA in the United States, investigative agencies rarely meet with a refusal; in 2004–05, only six warrant applications were withdrawn or refused.[36]

According to a recent Parliamentary Committee report, Australia issues 75 percent more warrants than the total number of U.S. wiretap warrants in absolute terms, or twenty-six times more than in the United States in per capita terms.[37] Monitoring of domestic communications by the Australian Secret Intelligence Organization—devoted to countering threats to national security—is subject to even less oversight, requiring only internal government approval.

In a classic instance of intensified surveillance through legal reclassification, legislation enacted in 2006 loosens even these restraints on *stored* communications—defined as messages no longer in transit but retained in electronic form in the computer records of the recipient.[38] These include e-mails, SMS/MMS messages, pager messages, and messages left on answering systems. Under the new law, authorities can access these messages on the basis of a special court warrant, involving fewer safeguards than for real-time communications.

Further changes mandated in this legislation include provision for interception of communications with persons not themselves under suspicion, but in contact with a suspect. As with the American Patriot Act, the effect is to spread the reach of permissible surveillance to the communications of persons not alleged to be part of subversive or illegal activities. There is no requirement that those subjected to such surveillance be notified of the monitoring after it is complete. And as in the United States, Australian telecommunications providers have been required to build surveillance capacities into their systems, at considerable expense.

Connection data, as in the UK and the United States, are even more accessible. Telecommunications companies—providers of phone and Internet

service—have a legal obligation to furnish law enforcement and tax authorities, on request, with data on who called or e-mailed whom, when, where, and for how long. During 2004–05, companies provided personal data in response to nearly 900,000 such requests—this in a country with a population of about 20 million.

Australia has also cast a net for monitoring its people's *financial affairs* nearly as fine and wide as that in the UK. All personal income data held by tax authorities are available for investigators' attentions without court order. Besides tax authorities and other investigators, welfare agencies tap these data to monitor eligibility for social benefits. In addition, government agencies can delve through Australians' bank, credit card, and other financial accounts—either simply on request, or under administrative order.

As in the United States and UK, private institutions must report much personal financial data without specific inquiry from government agencies. The Australian Transaction Reports and Analysis Centre (AUSTRAC), an agency of the central government, imposes serious reporting requirements not only on financial institutions but also on a wide variety of other "cash dealers"—businesses and other organizations likely to be party to major flows of money. These include lawyers, accountants, and (under legislation announced recently) jewelers, real estate agents, and financial advisers. All are, or will be, required to report transactions of more than $10,000, all electronic international transfers, and any broadly defined "suspicious matters" to AUSTRAC. In 2004–05, the agency received more than twelve million such reports.

Government access to private-sector consumer credit files is less far-reaching than its equivalents in the United States. Australia's Privacy Act of 1988, passed at the high-water mark of public indignation against government monitoring, explicitly forbids government agencies from becoming "subscribers"—that is, regular customers—of credit reporting agencies. This means that investigative agencies must invoke legal process each time they seek data on a consumer.

Perhaps more important, Australian consumer credit files simply provide a less detailed overview of consumers' lives than would be available in the United States. Australian privacy legislation prevents credit reporting agencies from compiling information on individual credit accounts except where there is a payment delinquency. The result is that the vast arrays of "positive" credit information—that is, details of current and recent accounts held in good order—that fill American consumers' files are simply absent in Australia.

Nevertheless, in Australia as in other prosperous market societies, more actionable data from the private sector, compiled over longer periods of time, become available for government investigators every year. Traditionally, business records have been held for seven years in compliance with tax laws. New statutes now require retention for at least this long for "personal information forming the basis for financial advice."[39] These requirements run contrary to those of the 1988 Privacy Act, which include an obligation to ". . . destroy or permanently de-identify personal information if it is no longer needed for [any legitimate] purpose. . . ." The privacy statutes are increasingly overridden both by conflicting laws and by the inclination of organizations to save personal data "just in case."

In monitoring the *movements* of Australians, government investigators have fewer resources at their disposal than their British counterparts. As in the United States and the UK, authorities maintain an extensive database of Australians and foreign nationals whose movements into and out of the country are to be kept under surveillance—some 190,000 individuals in 2005. Australia was also an early adopter of international standards requiring biometric identification on passports, introducing what it dubs its "e-Passport" in 2005. Government use of video cameras in public places appears to be far less widespread than in the UK. But authorities are now working on automated face-recognition systems ("Smartgate") to screen travelers at selected airports.

In monitoring domestic travel, Australian authorities can always avail themselves of the automatic "markers" of one's presence that have become familiar to Americans—ATM withdrawals, credit card charges, cell phone uses, and the myriad of computerized transactions that leave their personally identifiable traces. Still, there are important differences in the ease of access to such data—virtually effortless for authorities in the case of phone records, but generally requiring a warrant in other cases. In addition, it is increasingly difficult to use Australian roads, bridges, and tunnels without identifying one's self. Cash payment is sometimes not an option on major toll roads. Often one must open an account from which tolls are deducted, and this means providing personal data that can later be linked to details of one's travels. In most metropolitan areas, Australians will soon pay for mass transit with "smartcards" like London's Oyster Card, which may reveal their holders' movements.

State governments maintain extensive networks of cameras on major highways and in urban areas, both for traffic management and to detect speeding and other violations. As in the UK, automated plate number rec-

ognition is increasingly used to identify specific vehicles. The users are the same agencies responsible for vehicle licensing, so that data collected afford easy linkage between vehicles and their owners. State and federal privacy commissioners have expressed concerns about the potential uses of data so collected—without thus far having much apparent effect on the activities in question.

One of the most politically sensitive aspects of government surveillance in Australia has traditionally had to do with the country's welfare state institutions. Inevitably, government involvement in health care administration and other social welfare benefits (for example, public transit subsidies for students) leads to accumulation of much sensitive personal data. Government investigators inevitably seek access to such data for purposes ranging from exclusion of ineligible beneficiaries to enforcement of tax obligations to pursuit of terrorists.

Ordinary Australians often mistrust the large-scale surveillance associated with such investigations—the most dramatic evidence being the revolt against the proposed Australia card in 1988. The essential anxiety underlying that movement seemed to be fear of a government that could centralize all data from all aspects of life and use data so compiled for open-ended enforcement purposes. Since then, Australian governments long treated such schemes as a sort of "third rail" of Australian politics—fatal to any governing party that dared to raise them.

Now that seems to be changing. Since 2005, government agencies have been promoting a new smart "Access Card," allegedly intended solely to facilitate access to state services such as welfare and health benefits. Though the authorities deny that this amounts to revival of the national ID card plan, commentators widely see it as the thin edge of a policy to just that end. Cards are to be issued to nearly all Australian residents and will include digital photographs of the bearers. Australians' nearly universal need to access government health benefits would ensure widespread recourse to the card, which would in turn likely lead to its use for tracking people's activities, transactions, and movements. Even if no such plans exist at present, demand for them once the system is up and running seems all but inevitable.

"Australian information privacy laws do not in practice have a significant limiting effect on the type and amount of surveillance by government

agencies," writes Australian privacy consultant Nigel Waters: "They serve more to ensure a minimum level of transparency and procedural fairness, as well as to require minimum standards of data quality and security. The limits of surveillance are determined far more by the availability of information in relation to different aspects of individuals' lives and the powers of agencies under other laws to access that information."[40] A statement that applies in many other settings, as well.

Canada

In Canada as elsewhere, the threat of terror attacks has nudged the country toward intensified government surveillance. But at a number of crucial points, Canada has met this trend with more restraint than her British parent or her southern neighbor.

Without invoking the term, Canada's constitution guarantees certain privacy rights. These include rights against unreasonable searches and seizure cited in the Canadian Charter of Rights and Freedoms. In addition, Canada has two comprehensive national privacy laws—the 1982 Privacy Act regulating data held by federal government agencies; and PIPEDA, the 2000 law governing personal data held in the private sector. Certain provincial legislation adds additional protections. The post-9/11 Anti-Terrorism Act and other legislation wear away at some of the privacy protections in the earlier measures, without fully subverting them.

Since 1974, Canadian law enforcement agencies seeking to intercept *contents* of oral or phone communications have faced some exacting legislative constraints. They must normally convince a court of two things—that they are investigating an offense, and that the search is required to produce evidence or other essential information about a crime. Applications for such warrants must also demonstrate that the information being sought cannot reasonably be obtained through other methods. Targets of court-ordered monitoring must be notified within ninety days of the end of the interceptions. *Stored* e-mail records are subject to less rigorous protections.

Legislation in 1997 loosened some of these strictures for investigations of "criminal organizations." Law enforcement agencies no longer needed to show, for example, that the data being sought could not be otherwise obtained. Post-9/11 legislation extended this relaxation to terrorist investigations. And since its inception in 1984, the Canadian Security Intelligence Service

(CSIS), which is charged with intelligence related to "threats to the security of Canada" including espionage, has been able to obtain judicial warrants without requirements for eventual notification of the target. In 2001, the Communications Security Establishment (analogous to the United States's NSA) was also granted significant new powers. That agency may now obtain warrants signed by two ministers that allow it to intercept communications of "foreign entities located outside Canada" (including any part of the communications happening in Canada). These include any communication whatsoever intercepted "for the sole purpose of protecting the computer systems or networks of the Government of Canada." There is no requirement for notification of targets of CSE interceptions.

As elsewhere, *connection* data—details of who contacted whom, when, and for how long, or who visited which websites—are subject to fewer protections. Under Canada's private-sector privacy law, suppliers of telephone and Internet services may provide such data to government investigators where they suspect the information relates to national security issues. The 2002 Public Safety Act amended PIPEDA to authorize these and other private-sector bodies not only to disclose, but also to collect personal data *for the purpose* of disclosure for national security purposes. For e-mail communications, connection data may of course convey important clues to the content of messages, by way of header information. These powers also cover details of users' website visits and Internet searches. Should institutions holding such data decline to disclose voluntarily, court warrants are necessary.

Canadian telecommunications providers are subject to "production orders" requiring them to produce information under their control. At the time of this writing, accessing these data still requires court warrants. The information so obtained may include contents of communications, should they be stored in the possession of the provider. For investigations of espionage, court orders are also required, both for production of records and for direct monitoring of communications.

Other legislation now being weighed by the government would require telecommunications companies to provide "tracking data" on phone and e-mail users—though again, on production of court orders. This legislation would reduce the necessary level of expectations on the part of investigators from "reasonable grounds to believe" that a crime was being committed to "reasonable grounds to suspect"—a notch lower in the strength of the claim.

All things considered, Canadians do not face the sweeping powers granted by the Patriot Act in the United States—where the content of their communications may be monitored simply on investigators' attestations that the inquiry relates to terrorism. Nor is there a special category of courts like the FISA, which have developed such a notably permissive attitude toward surveillance requests in Washington.

The Canadian government has not imposed mandatory conservation of e-mail and telephone logs, as the United States and the EU have done—though pending legislation would permit law enforcement applications to courts to extend retention of such data in specific cases. This same legislation would enable police and other investigators to obtain, without court warrant, "subscriber data" from telecommunications companies—including name, address, phone number, and IP address—for specifically identified individuals. The legislation would also do what U.S. authorities accomplished in the mid-1990s: require the country's telecommunications companies to reengineer their systems so as to facilitate wiretapping. Legislation along these lines died in Parliament in 2005 but is being reconsidered at the time of this writing.

Canadians' *accounts and financial records* are subject to the same access demands as other personal papers and records described above. In addition, since 2000 a number of institutions and professions have been required to report financial transactions defined as "suspicious" to FINTRAC, the government clearinghouse devoted to monitoring illegal transactions.

Some operations, like cash transactions over $10,000, must be reported as a matter of course. In addition, reports to FINTRAC are required whenever "there are reasonable grounds to suspect that the transaction is related to the commission of a money-laundering offense or a terrorist activity financing offense." Besides banks and other financial institutions, this obligation was initially also binding on lawyers. After legal challenges, this reporting requirement was removed in 2002.

Regarding the *movements* of Canadians, of course, financial records are themselves revealing. Records of ATM use, for example, like those of credit card use and cell phone use, are as important in tracking Canadians' locations as they are for other investigative purposes. Canadians also leave traces of their movements whenever they use certain of the country's sophisticated toll roads, which require drivers to identify themselves for billing purposes. Use of public video surveillance cameras and automatic license plate recog-

nition in Canada, though on the increase, appears very underdeveloped by contrast to Britain, the leader in these respects.

If the essentially public nature of these highway travel records troubles Canadians, however, evidence of such anxiety is scarce. Efforts by Ontario's Information and Privacy Commissioner to create an option for anonymous use of one of that province's key superhighways had so few takers that it was abandoned.

As one might expect, movements of travelers in and out of Canada are monitored by border authorities relying on a series of linked databases like those administered under TECS in the United States. Legislation adopted between October 2001 and 2004 aimed at collecting data on passengers' itineraries, manner of payment, and dietary preferences for use in monitoring air travelers. But attempts to collect these data triggered strenuous objections from Canada's Privacy Commissioner, as well as from European Union authorities. As a result, some of the data sought were dropped from the database—including that on meals, which obviously held implications for travelers' religion or ethnicity.

Finally, like other countries, Canada is weighing creation of a national identification card, or some near-equivalent. Under pressure from the United States for easy identification of travelers across the southern border, the federal minister for public safety announced plans for such a machine-readable card in early 2006. To meet international standards, such a card would probably carry some form of biometric identification—either a computerized image of the bearer's face, iris, or fingerprint. In the words of former Liberal Party Immigration Minister Denis Coderre, "... we cannot bury our heads in the sand anymore. ... Something is going on worldwide and we have to have that debate [over ID cards]."[41] Canada's Privacy Commissioner has opposed the idea of a national ID card, and there appears to be little immediate impetus to embrace such a system.[42]

Canada's May 2004 Public Safety Act enabled government investigators to obtain passenger data from airlines without court warrant. Privacy Commissioner Jennifer Stoddart entered strong objections. In a statement to Parliament, she noted:

> It may well be that few people would question [such measures] ... given the risks that terrorists pose to air transport. But the use of

this information is not confined to the purposes of anti-terrorism and transportation safety. The *Public Safety Act* also allows the information to be used to identify passengers for whom there are outstanding arrest warrants for a wide range of ordinary criminal offenses. In other words, the machinery of anti-terrorism is used to nourish the needs of ordinary law enforcement, lowering the standard ordinarily demanded of law enforcement authorities.[43]

The identical critique could be leveled against similar measures invoked in the name of combating terrorism all around the world.

France

State surveillance in France reflects conflicting forces. Traditionally, powers accorded the state in matters of national security and criminal justice have been stronger, say, than in the United States. But France also has one of the earliest privacy codes in the world, dating to 1978. And it has one of the strongest national privacy-protection agencies—the CNIL (National Commission on Information Processing and Liberties). The result is some sharp contrasts between broad state discretion and well-circumscribed individual rights over personal data.

In matters of state security, French government investigators long enjoyed sweeping and largely unchecked access to *communications* data. French law draws a sharp distinction between criminal and "administrative" investigations. Today, the latter are defined as concerning:

- national security
- safeguarding "the scientific and economic potential" of France
- prevention of terrorism, or
- the struggle against organized crime, private armed groups or militias.[44]

Until legislation adopted in 1991, state investigations into these broad concerns seem to have taken place with virtually no constitutional or legal checks. Agents of the Interior Ministry or other state agencies appear to have been free to wiretap phone conversations, monitor connection logs of telecommunications, access bank account data, or generally avail themselves of any other personal information they held necessary. Similar activities by the FBI were

of course widespread and largely unchecked in the United States during the 1950s and 60s; but they were clearly illegal, and assailed as such at the time.

The 1991 legislation, adopted by France after its censure by the European Court of Human Rights in April 1990, essentially legitimizes these sweeping powers, authorizing wiretapping and other extreme investigative measures. It grants the prime minister and the ministers of the Interior, Defense, and Finance power to authorize wiretaps largely at their discretion. Anti-terrorism legislation adopted early in 2006 permits each of these ministers to delegate this authority permanently to two persons within each of their ministries.

In principle, the 1991 legislation subjects these prerogatives regarding wiretapping and access to connection data to review by the CNCIS—National Control Commission for Security Interceptions. But this three-member body, composed of one administrative judge appointed by the president, one member of the National Assembly, and one senator appointed by their respective bodies, has a total staff of five (including the three members) and operates on a modest budget. Its formal powers are purely advisory. By any standard, it constitutes an even less forceful check on government investigative powers than the permissive FISA court in Washington.

According to the most recent report of the CNCIS, "administrative" wiretaps brought to its attention rose in number from 1,180 in 1991 to 1,870 in 2005. These investigations are more often targeted against organized crime than suspected terrorist activity.

In strictly criminal investigations, protections for individual rights more closely resemble those in the United States. But here, too, practice was relatively unrestrained until the 1991 legislation, which for the first time required approval by an independent magistrate for interceptions of telecommunications. Before then, the state prosecutor could approve such measures without recourse to the courts. Since 1991, wiretapping and similar interceptions may be ordered for investigations of serious crimes, and each order is limited to four months. Further legislation in 2004 relaxed these requirements somewhat, allowing interceptions without court approval for investigations of certain crimes, "when the necessities of the investigation demand it." Among the crimes that may trigger such investigations without court warrant are "acts of terrorism." French law does not require that targets of such investigations be notified of the monitoring at any point.

As in other countries, investigators' access to the *content* of communications—phone conversations, e-mail texts, website visits, and the like—is more closely

regulated than access to *connection* data. Yet lore among French investigative agencies has it that connection data are often more useful for surveillance than full access to contents. Connection data, for one thing, are not subject to encryption; moreover, their results can be summarized electronically, trolled by computer for specific e-mail addresses or key words.

For "administrative" investigations, French law was silent on the conditions permitting access to connection data before legislation in January 2006. One conceivable conclusion from this fact is that investigators of organized crime or terrorism acting on ministerial orders never delved into records of who was contacting whom. But no one believes this. Presumably those carrying out administrative investigations must have perused these data freely, at least whenever authorized at the ministerial level.

Given the ease with which connection data are often available, the length of time for which they are stored takes on special significance. One year has long been the baseline for which telecommunications data have legally been retained in France. As the richness of these data grows—to include data on callers' location from cell phone use, for example, or data on websites visited—many investigative interests have sought to extend their availability. In 1998, the Minister of the Interior suggested a retention period of ten years for all such data—an option rejected by the Lionel Jospin government. Legislation adopted in 2001 reiterated the one-year limit, even after the 9/11 attacks. But the January 2006 "anti-terrorism" legislation authorizes investigators under the Ministry of the Interior to delve into such data without court warrant.

In the *financial* realm, computerization of nearly all accounts; and the predictable interest of the state in monitoring the financial affairs of the governed, have yielded many surveillance practices in France parallel to those in other countries.

Banks and other financial institutions are required to participate in "Tracfin"—like FINCEN in the United States, SOCA in the UK, AUSTRAC in Australia, and FINTRAC in Canada. Under Tracfin, large transactions must routinely be reported to the Interior Ministry. As elsewhere, the government imposes further requirements to file "declarations of suspicion" when customers engage in activities deemed to require special attention—such as transfers to particular individuals or countries.

Another kind of state interest in citizens' financial affairs obviously lies in revenue collection. Here the French government confronts a population famously bent on keeping transactions off the books—and themselves out of

sight—of the nation's tax services. As with telecommunications providers, banks and other account-holding institutions are expected to open their books without court order to tax investigators. In these matters, the absence of consumer credit reporting in France ensures a measure of privacy unavailable to residents of the United States, Canada, and the UK—since there is no single institution devoted to centralizing data on consumers' accounts with all credit-granting institutions. Thus it is more difficult for tax investigators or any other interest to gain a quick overview of any given consumer's obligations and consumption habits.

A disadvantage in the surveillance equation for those seeking to avoid tax obligations is the French welfare state. Most French citizens receive medical care through the state system; nearly as many also draw some other welfare state benefits such as family allowances or old age pensions. This close contact inevitably makes it attractive to tax authorities to share the capacities of the welfare services for remaining in touch with the population. After all, people want and need contact with sources of benefits, whereas they do not usually have the same attitudes toward tax authorities. An amendment to a 1998 taxation bill accordingly specified that the tax services could use social security numbers for tax records and could use social service agencies' records to obtain and verify citizens' addresses.

Perhaps most important, the new law affords tax administrators access to data on personal finances provided by those seeking social services—as a means of verifying reports of taxable income. The CNIL, France's privacy watchdog agency, opposed this change, but it was approved by the national Constitutional Council (the French constitutional court) and remains in effect today. In the absence of any U.S. equivalent of the CNIL, it is difficult to imagine any voice in American government that would oppose such a transparent advance in tax enforcement in the interest of privacy protection.

In judicial matters, French investigators enjoy the same possibilities for access to financial records as to telecommunications records. For investigations of specific crimes, state agents may obtain court orders or even simply authority from the state prosecutor to examine account or business records held by banks or any other financial institution. The same holds for tax records, motor vehicle records, or any other records held by state or private institutions.

In "administrative" investigations—those deemed to involve state security—it is hard to say what legal restraints apply, if any. Given the lack of oversight accorded these activities, and their recent history of something approaching

completely free rein, it would be rash to assume any limits on the discretion of investigators.

In their attention to the *movements* of the governed, French authorities have an advantage only now being cultivated in the other four countries—a long-standing system of national identity cards. Applicants for identity cards must provide their fingerprints, but these are now stored locally, rather than in a national database. Police may ask to see identity cards, but bearers are under no legal obligation to present them. When they are presented to authorities, however, the fact that identity cards are machine-readable makes it possible for them to be checked electronically against the national register of persons wanted by the police.

Identity cards are routinely checked for all those persons boarding foreign and domestic flights. Under the anti-terrorist law of 2006, airlines, railroads, and passenger ships must furnish lists of their travelers to the Minister of the Interior before any departure. Data so collected now become part of a national data pool of traveler information, shared with other police forces via Interpol.

If they avoid travel outside the EU, most residents of France do not often have occasion to have their identity cards or passports "read" electronically. The routine verifications of these documents for domestic travel aim simply at determining that names given by passengers match those on their ID documents. But the French do leave electronic markers of their movements in most of the same situations familiar in other market economies. They pay by debit cards—at higher rates than in any other European country; they draw cash from ATMs; they rely obsessively on cell phones; and they use automated toll systems and pre-paid subway cards—always generating data on their presence and activities.

Use of such data by investigators in criminal cases follows the principles noted above. A judge, and in some cases the state prosecutor alone, can authorize such access in investigations of major crimes. It is hard to doubt that "administrative" investigators have recourse to such data—given the broad discretion that state agencies seem to have in this category of surveillance.

The Coalescence of Government Surveillance

Parallels across the five countries "jump in your eyes," as the French like to say. Flying under the flag of response to international terrorism, all five have significantly extended the breadth and penetration of government surveillance.

Without exception, all have established new monitoring patterns for money uses that would once have been strictly private matters—often including not only international payments but also domestic transactions among private parties. All have extended retention of records of telephone and cyberspace communications, to enable government investigators to trace these patterns after the fact. All have eased restrictions on monitoring of those identified as possible foreign agents—lifting requirements for independent judicial review for at least some forms of investigation. All have multiplied the checkpoints where people are required to identify themselves to authorities—permitting the state to monitor more closely who is where, and when—often relying on automated techniques for things like license plate recognition. And all have taken at least tentative steps toward creating national ID card systems—with their inevitable automated linkages to arrays of acknowledged and unacknowledged government databases of personal information.

In all these countries, privacy commissioners have inveighed against the dangers of such developments—except of course for the United States, which has forestalled such complaints by never creating such an office. But warnings and protests, from official quarters and the grass roots, appear not to have made much of a dent in the broader trend. All in all, the last decade has not been kind to privacy concerns in any global perspective.

Still, privacy values have clearly proved more resilient in some countries than in others. Over all, Canada has by most standards proved significantly less willing to compromise individuals' control over their information than the others. The United States, most observers would probably agree, has effected particularly sweeping and unchecked circumventions of judicial checks in its draconian Patriot Act—and in subsequent end-runs around even the modest restrictions posed by that legislation. And France has in some respects bested the Americans in the sweeping prerogatives accorded to "administrative" investigations.

The UK has clearly gone farthest in electronic monitoring of people and vehicles in public places—its restraints on government access to personal information held by government and private institutions having never been very strong in the first place. And Britain's steps toward creation of a national identity card system have taken it much farther in that direction than other countries except France—and has met with less effective popular resistance. Even populist Australia, with its explosive history of popular objections to a national ID card, is moving to introduce a card very likely to evolve toward this function.

In these significant national differences, optimistic privacy-watchers may discern silver linings. Clearly privacy instincts and protections are not altogether dead, they might point out—even in those countries where they have taken the most serious beatings. People have spoken out against unchecked surveillance—even in the face of threatening events that were bound to generate demand for more of it. Climates of public opinion succeed each other cyclically, some might hopefully observe. Eventually we can hope for a swing away from the authoritarian, privacy-eroding climate of the so-called War on Terror.

Unfortunately, such optimism misses something fundamental in the developments considered here. True, privacy principles continue to have strong public exponents, and even occasional vindications in some settings—*vide* the widespread opposition in the United States to the Bush administration's secret monitoring of domestic telecommunications and to preparations for a national ID card. Here many conservatives have joined the leftward side of the political spectrum in objecting to privacy-eroding government surveillance.

But the evolution of government surveillance described above reflects something even more far-reaching than a response to shocking acts of mass violence. It entails a profound shift in what one might call the *ecology* of personal data. In all the five countries considered here, and in many more, governments are gaining access to more different kinds of information on people's lives. And they are fashioning more efficient checkpoints where such data can be brought to bear in forceful decision making on the people concerned. The net effect of these developments is to broaden the coverage of ordinary people's everyday lives through mass surveillance—and thereby to extend the forms of compliance that governments can expect from their people.

Consider a seemingly whimsical example from daily life in New York, where I live. All New Yorkers note the necessity to pay state sales tax on most purchases from institutions—about 8 percent on everything from restaurant meals in Manhattan to lawn mowers from suburban megastores. But most of my fellow New Yorkers would be intrigued, I believe, to learn that they are also legally obligated to pay this same tax on purchases made from private parties.

Thus if I purchase a lawn mower from my next door neighbor for, say, one hundred dollars, state law requires me to forward about eight dollars to Albany in sales tax. If informed of this obligation, I believe, most Empire State

residents would simply regard the idea as quaint. They might even react with the sort of sarcasm that some cruel outsiders consider the normal mode of expression in the Bronx. The law requiring sales tax payments on purchases from private parties is a matter of ignorance-bordering-on-contempt, because the state can exercise no surveillance over the conduct in question.

There is one notable exception. When New Yorkers purchase vehicles from private parties, their first stop is usually the local Department of Motor Vehicles office, to obtain new license plates and registration documents. There they find that payment of sales tax on their purchases is indispensable to completing the process. Stories of rare bargains resulting in absurdly low sale prices or lavish gifts from relatives meet with well-trained skepticism from DMV staff, who insist on payment of 8 percent of the book value of the new possession. Confronting a wall of bureaucratic resolution, the new owner predictably pays.

What has all this to do with evolving pressures on privacy? A great deal, if you perceive in this situation a microcosm of the tug-of-war played out everywhere between governments and the governed. The legally valid requirement to pay sales tax on purchases between private parties is a dead letter—or a figure of mirthful contempt—unless and until the state can bring systematic surveillance to bear on the conduct in question.

Unlike lawn mowers, most privately owned vehicles are driven on public roads and highways—where they are subject to easy monitoring for compliance with requirements for legal registration, safety inspection, and the like. In these relatively public settings, representatives of state authority can readily take decisive action against drivers who do not comply. In short, putting a car on the road shifts the equation of advantage, in what sociologists sometimes call the *staging of social control,* between government and governed. It brings what would otherwise be obscure and unknowable behavior out into the public realm. And in so doing, it renders one domain of once-private life readily subject to government control.

To realize such extensions, governments need to do two things. First, develop actionable information to clarify who has done what. Second, create checkpoints where those targeted for control are, however briefly, subject to action by enforcers acting on such data. When New York motorists seek to put privately purchased vehicles on the road, both conditions are amply fulfilled. The fact that the vehicle has been sold, and its market value, are

easily documented. And its use on the road without proper registration is subject to ready observation and easy sanction.

These identical dynamics play themselves out in enforcement of institutional demands far more complex and consequential than auto registration in New York. Governments seek all sorts of compliance from their people—ranging from tax payment to political support. These and countless other control aspirations have no more hope of realization than taxation of purchases between private parties, unless and until states can monitor them. And in the absence of situations where both the compliant and noncompliant can be confronted with state power and held responsible for their actions, surveillance alone may not do much good.

That is why governments establish "checkpoints," where the governed must necessarily identify themselves and thereby make themselves available for corrective action. Among the most effective checkpoints, in present-day America, are international airports, where Americans and foreigners alike come briefly under the fullest scrutiny of the state.

Where travelers' records dictate forceful action or further monitoring, the staging could hardly be more advantageous to the state. Travelers are effectively detained while undergoing processing by INS authorities on arriving or while waiting to board departing flights. In either case, they are easily available for arrest or questioning. Those not considered to warrant arrest are still apt to have their movements tracked by agencies interested in their whereabouts. Thus anyone wishing to conceal his or her presence or destination from the U.S. government or its allies will prudently avoid entering or leaving the United States through such checkpoints.

Authorities, in turn, seek to interpose checkpoints precisely where people have little choice but to present themselves. The more such checkpoints there are, and the more unavoidable it is to pass through them, the stronger the authorities' position. And note that such checkpoints further reinforce one another where—as is normally the case—passage through them generates new data on travelers' presence and movements. Here as elsewhere, surveillance feeds on itself: ability to enforce grows in step with collection of data to support further enforcement.

Thus pressures on privacy in America have grown not only with the sheer amount of personal documentation accumulated on Americans. They have also grown through the linkage of crucial intakes of personal information with situations and relationships that most people cannot afford to do with-

out. Social Security and income taxation do not just provide opportunities for gathering personal data. They also constitute checkpoints in the lives of most Americans—points at which people's presence can be pinpointed, their incomes garnisheed, or (as in the case of undocumented aliens) their employment denied altogether. For those with something to hide from the government, working "off the books" becomes the only available alternative—an alternative readily curtailed, should the authorities crack down.

Meanwhile, checkpoints proliferate—as illustrated by the case of Deborah Davis, the Denver commuter arrested in 2005 for refusing to present ID while riding a public bus near a federal building. And in this context, efforts to establish what amounts to ID cards with national standards hold far-reaching significance. Machine-readable cards affording access to varieties of databases will enable authorities at each checkpoint to take forceful action toward each bearer—or to fine-tune further monitoring of his or her movements and activities.

Many Americans, one suspects, weigh the appeal of the prospective national ID card in terms of utterly practical, short-term calculation. Would the information visible on the card be more "personal" or embarrassing than what appears on cards one already carries? Would the existence of the card raise the total number of occasions when one had to present some form of identification? Would it simplify one's processing through security lines, government offices, or other high-security locations? Judged in these terms—as surveillance supporters will surely emphasize—the cards might appear to make life easier, and even more private.

But in any larger view, what matters is not what may be visibly displayed on the card or the ease of its use. Their impact will instead register through the *forms of information on the holder that authorities can access,* in the *array of interested parties entitled to share in such access,* and in the *number and nature of the checkpoints at which such access may be demanded.* Any such card will become a universally recognized "node" through which all official data of interest to any participating agency will be available. And claims not to have a card, or refusals to present it, will prove highly counterproductive for anyone foolish enough to try.

So the question is, what kinds of personal data will be brought to bear through the card—and with what consequences? We do not know in any definitive

way, but certain uses are extremely probable. Presumably those in the country illegally will not have cards and so will face immediate action at checkpoints. Presumably those listed as wanted for arrest will face equally decisive action—at least, so long as the jurisdiction issuing the warrant is willing to bear the costs of extradition. Presumably, too, long-term visitors to the country who overstay their visas will be subject to quick identification at checkpoints.

These are just the most obvious cases. At this writing, the federal government acknowledges maintaining a variety of "watch lists" of persons targeted for special treatment. These include lists maintained by the FBI, the State Department, the Treasury Department, and others. No one wants to be included on one of these lists—or to have a name resembling someone who does. Among the lists are the Transportation Security Administration's No Fly List and the Treasury Department's list of Specially Designated Nationals. Inclusion on the latter means blockage from moving funds abroad. Presumably those on any of these lists would immediately be identifiable wherever their ID cards were checked.

But this is still just the beginning. Consider the enormous array of enforcement interests represented by one government agency or another—interests standing to benefit by altering treatments people received at these crucial points. What consequences would they wish to impose on their enforcement targets when identified at checkpoints? Would parents absconding from child-support obligations, for example, be identified through the cards? What about those in serious arrears in their local, state, or federal taxes? Wouldn't it only be just to deny them normal passage through at least some checkpoints—to encourage them to meet obligations that otherwise fall on law-abiding taxpayers? What about persons with histories of violence toward law enforcement agents? Shouldn't those who encounter them in the future have some warning about the dangers they pose? What about those who are HIV-positive? Shouldn't medical care workers and others be able to identify them at once via their ID cards—even if—or especially if—they are unconscious, or uncooperative?

And what about convicted sex offenders, or persons with histories of offenses against children? Shouldn't the card make it possible to spot them instantly, so that they could be blocked from situations where they might pose a danger? What about those with histories of spouse abuse, arson, or hate crimes? And if these forms of criminality could be made known through

authorized use of the card, what details of bearers' criminal records should *not* be accessible—to users with legitimate interests in protecting themselves or their property? Would the card enable the "right" users to learn the religion, ethnicity, or political party registration of the bearer? One can imagine situations in which any number of government agencies might claim compelling need to act on such information.

And what consequences should ensue from bringing to bear information so revealed? At a minimum, some of the "news" transmitted through the card would block the bearer from whatever he or she was about to do—boarding an airplane, entering a building, withdrawing money from an account, or making a major purchase, for example. At some points, the consequences would obviously be arrest. Elsewhere, data brought to bear through the card would trigger strikingly different treatment from those staffing the checkpoint—or those at the next step beyond. Imagine the differences in treatment one could expect to receive, say, from law enforcement agencies on being identified as HIV-positive, or as having a history of violence against police.

And when and where would one be obliged to present the card? Start with the easy cases. Cards would undoubtedly be required at all junctures where "government-issued photo ID" is now demanded—airport security and entrance to federal buildings and facilities, at a minimum. But there are many other points where those in charge would like to exclude dangerous persons—or at least monitor their behavior more closely. Toll roads, bridges, and tunnels—all potential foci of terrorist activity—would be natural junctures. Trains and other mass transit, both established targets of terrorist action, would be obvious checkpoints.

Credit card and ATM use could also require ID card checks. Supporters of the cards would uphold this practice as a means of combating theft—especially where biometric features of the card could prevent it from being used by anyone else. Other likely checkpoints would be entry to parks, sports stadiums, performance halls, libraries, universities, places of worship, or any other place where people gravitate in large numbers. And note: checking at such locations would have the inestimable advantage of generating vast logs of data on the movements and activities of Americans—a rich surveillance resource for purposes now only imagined, and not yet imagined.

The greater the number of participating interests, the more attractive will become use of the card for still further interests. Private institutions will

have their own claims to make on data accessible through the card. If knowledge of HIV status is accessible through the card, health care providers and insurance companies will surely expect to be given authorization to learn it. If the card makes it possible to identify those held guilty of crimes against children, then schools, day care centers, and the Boy and Girl Scouts will certainly demand to know—and perhaps seek the option of adding their own experience to the relevant databases. If the card afforded access to criminal record information, employers and insurers would surely seek to avail themselves of it. As with Americans' income tax returns, the sheer existence and availability of data like these would generate enormous pressure for access to them.

Let me be clear: I do not assert that all these uses form part of anyone's conscious intent in promoting national ID cards. What I argue seems to me even more provocative—that pressures like these seem all but inevitable, should such a system be created. Regardless of anyone's intent at this stage, massive demands to share the facilities of any system of this kind simply represent the extension of trends long apparent in mass surveillance.

Recall the 2004 Bush administration proposal for a nationally centralized, comprehensive repository of information on all Americans' health care histories. The plan, still in the policy pipeline, aims to streamline health care administration by ensuring that all relevant information on every American is quickly available to care-givers, whenever it might be needed—a transparently worthy goal.

But assume that these plans bear fruit. It is hard to imagine how access to each patient's file would not be possible via his or her ID card—at least, for those duly authorized to exercise such access. And consider the range of interests that will seek such access. Will Social Security have the right to scrutinize contributors' files in weighing disability claims? Will the military be able to access the file—to screen for unreported illnesses or mental conditions among potential recruits? Will law enforcement agencies be permitted to troll the files in search of DNA data that might help investigate unresolved crimes? Will sellers of medical and life insurance be permitted to use the files to verify applicants' accounts of their own medical histories? Will prospective employers have access?

No doubt someone will propose that such access be possible only with consent of the patient. But in what sense can the consent of "private" individuals be meaningful when they deal with organizations like these?

Conclusion

In tracing the evolution of privacy, as at the cinema, the best seats are not always closest to the action. In day-to-day action, change is often jerky and discontinuous. New and unexpected uses for personal information are constantly vaulting into the realm of the possible—often to much public dismay and controversy. Sometimes privacy forces prevail in blocking or constraining such changes; elsewhere, the changes quickly become established elements of newly successful claims on personal information.

In the longer view, trends are hard to miss. For more than one hundred years in the world's "advanced" societies, sources of actionable personal information have been proliferating. In step with this trend, government institutions have grown more adept at identifying and accessing such data and bringing it to bear in forceful decision making on the individuals concerned. Given the trump-card role of efficiency in shaping public policy, pressures to access any personal data that *can* be accessed in support of enforcement efforts are intense. Under these circumstances, it's hardly surprising that the realm of life subject to government monitoring and enforcement steadily broadens.

Clearly the expansion of government surveillance has often brought benefits. Most of us would not prefer a return to tax farming. We also appreciate precise calculations of our eligibility for social welfare benefits, action against dangerous criminals, efficient organization of medical care, and many other government performances involving surveillance. But the overall increase in government access to our lives, and the shrinking individual choice in the matter, clearly raises questions not easily dismissed. Above all, where will these trends end?

The shock of mass murder by terrorists clearly has nudged these processes ahead—accelerating development of new means for compiling and acting on new forms of personal data. But it would be rash to imagine that abatement in the War on Terror, should it ever occur, will provide much enduring relief. The incremental accretion of new forms of information-capture on behalf of

established aims of government supervision and enforcement was set well before the recent rise of terrorism. It is a trend drawing on deep-seated expectations of government performance—in matters going far beyond the response to specific violent deeds.

If, as I hold, there are no "natural limits" to this trend, we need to think more hard-headedly about what limits might be placed on it through thoughtful human intervention.

Part III ■ ■ ■ ■ ■

Personal Data in the Marketplace: Credit, Insurance, and Advertising

At TransUnion, we carefully safeguard the credit histories of an estimated nearly 500 million customers worldwide.

The existence of an individual's updated credit file makes it possible for businesses to make nearly instantaneous, objective credit and insurance decisions. Processes that formerly took days or weeks may now be completed in minutes without question of personal prejudice or subjective judgment.

Our database also gives consumers more choices. It makes it possible for credit card issuers and other businesses to target their offers so that consumers may shop for the best products and terms. Ready access to current credit information makes the modern consumer economy possible. . . .

—from "TransUnion Public Policies"

Researching my first book on privacy in the 1970s, I spent hours talking to British civil servants. These expert administrators were key sources on the uses of personal information by that country's police, social security, and other public bureaucracies. When not responding to my questions about their work, they would often politely inquire about the other parts of my book. What other record systems was I studying besides their own? Other chapters,

I explained, dealt with commercial data systems in the United States, mainly those associated with consumer credit.

These very proper public officials sometimes betrayed just the slightest hint of distaste that their work could be compared to such profit-driven, privacy-invading activities. Commerce in private persons' bank records, retail accounts, or other financial affairs, they gently suggested, would never be acceptable to the privacy-minded British public. The fact that these civil servants were themselves deeply engaged in monitoring their fellow Britons' lives seemed irrelevant to them. Their role, after all, was to administer publicly mandated government programs, carried out for the common good rather than for commercial gain. By contrast, notions that a bank or retail establishment might exchange personal information on someone's account for commercial advantage struck my informants as contrary to basic public values of discretion and privacy.

Today, nearly thirty-five years later, British consumers confront surveillance over their financial affairs that is virtually as comprehensive and aggressive as anything in the United States. Indeed, American credit reporting giants have purchased most of the British industry and revamped it along American lines. British consumers today find it all but impossible to obtain a bank account, credit card, or retail credit account without acquiescing to comprehensive scrutiny over their financial affairs. As in the United States, those records increasingly shape the treatment Britons receive when they seek insurance or employment. Databases of personal information have grown nearly as rampantly in direct marketing.

If traditional British values of discretion and privacy over matters of personal finance and consumption habits have posed much of an obstacle to these changes, it is hard to discern. Nor have British privacy law or its Information Commission, that country's official privacy protection agency, created major barriers to the growth of these practices. For privacy-watchers, a trajectory like this can only give pause.

The logic of surveillance in the world of markets and profit-making is fundamentally no different from that underlying government record-keeping. *Discrimination* is the ultimate aim. Government agencies seek to discriminate among citizens requiring different forms of official action. This may mean distinguishing those with sympathies for terrorism from the rest of the pop-

ulation; or it may involve judging who is responsible for paying taxes, and how much; or it might require distinguishing those legally entitled to drive from those excluded from doing so; or those eligible for social insurance benefits from the ineligible. To justify such discrimination, and the demands for personal information that they entail, governments invoke values of efficiency and justice—insisting that pressures on privacy are warranted in the interests of good stewardship of public funds or of protecting the state or its citizens from danger.

In the private sector, the reward for effective discrimination is profit. For countless enterprises, the ability to make just the "right" offer to the "right" customer—and to avoid dealing with unprofitable customers altogether—is a make-or-break proposition. This means distinguishing those consumers whose credit accounts are likely to be profitable from those destined to produce losses; or those insurance applicants likely to generate claims from those likely to yield only premiums; or those consumers likely to respond to marketing appeals from those unable or unwilling to do so.

In settings like these, access to critical personal information spells the difference between profit and loss. And in the world we inhabit, such information is constantly becoming available from new, often quite non-intuitive sources—from the computerized records of our supermarket choices, for example, or from our website visits, court appearances, prescription records, or travel bookings. No wonder, then, that commercial empires have grown up devoted to the creation and exchange of such personal information—and that personal data have come to be a *commodity,* marketed much as petroleum, pork bellies, or municipal bonds.

This chapter concentrates on the marketing of personal data in three domains: consumer credit, insurance, and direct advertising. In most prosperous market societies, each of these industries has developed its own system for creation and exchange of personal data. To be sure, these are not the only purposes for which personal data are marketed. Others include screening prospective tenants, employment applicants, or even prospective jurors. Wherever there is money to be made by administering just the "right" response to each individual, markets arise to furnish personal data supporting such discrimination. Needless to say, these activities often trigger indignation among the public and resistance from privacy-watchers, even as they furnish employment and profitable services for others.

Involuntary subjection to private-sector surveillance is in a sense ironic. Most of us expect *government* demands for personal data to carry the force of law. But markets are supposed to be the realm of choice. Consumers reluctant to see "their" data sold and traded, one might reason, should be able to react simply by shifting their dealings to businesses who respect their wishes. In the domain of the sovereign consumer, one ought theoretically to be able to take one's business elsewhere.

But typically, there is no "elsewhere." The logic of surveillance dictates as much. Personal data markets grow up to support discrimination—between more and less profitable credit customers; between more and less attractive insurance applicants; between more and less susceptible buyers of goods and services. Under these circumstances, seekers of privacy are likely to be precisely those with "something to hide"—that is, something that businesses find it profitable to discover. Such prized data may range from records of bad debts in credit to genetic profiles suggesting risk of disease in insurance. Against citizens' desire for privacy in these matters, surveillance systems strain for *comprehensiveness*—seeking to bypass individuals' efforts to censor data about themselves and instead to collect *all* relevant data, including the favorable, the unfavorable, and everything in between.

Responding to these tensions, every major democracy has sought to erect at least some limits to the marketing of personal data. The United States has done the least in this respect—and hence can boast the most sophisticated and far-reaching commerce in personal information. Limits imposed by other countries vary in both extent and kind. France and Australia impose significant limitations on the unauthorized capture and sale of credit information, compared to the wide-open American model. Britain and France, under EU privacy legislation, constrain the collection and use of personal data in direct marketing in ways unmatched in the United States. And American-style sharing of data on insurance risks is similarly restricted abroad.

We need to pay attention to these national differences—to how they have evolved, to their current workings, and to their future prospects. What can they tell us about market pressures on privacy and the possibilities for responding to these pressures? Do the policy strictures imposed around the world indeed promise meaningful defenses for privacy interests? Do they *work?* If so, at what cost in efficiency or convenience? If not, why not? And—above all—are the efforts to resist unlimited marketization of personal data gaining or losing?

The United States: A Virtually Free Market for Personal Information

In privacy matters, as in many others, America goes to extremes. By consensus of privacy-watchers around the world, this country has the least effective public measures to control commercial exchange of personal data of any prosperous democracy. More than a generation after Watergate-era efforts to legislate comprehensive rights over commercialization of personal data, the United States still has none—whereas such codes are basic in Europe, Canada, Australia, and other prosperous democracies.

Other commentators would no doubt put matters more positively. In America, they would assert, the genius of the market for identifying and exploiting imaginative uses of personal information has flourished in ways other countries have yet to match.

These two takes on American experience need involve no conflict in matters of fact. The lack of constraint on marketing personal data indeed sets the stage for ingenious and far-reaching practices for exploiting such data. Thus Americans inhabit a world where details of prescriptions they draw at the pharmacy can influence the advertising they are subjected to; where personal data recorded in court actions, property transactions, and vehicle and driver licensing are compiled and sold to buyers with few questions asked; where a rising balance in one credit account automatically triggers rises in rates charged to the same consumer in other accounts; and where low credit ratings lead to higher costs for automobile or homeowners insurance. And since the September 11 attacks, government investigators have increasingly become major buyers of the personal information marketed in these ways.

Consumer Credit

America's credit reporting industry is a manifestation of surveillance virtuosity unsurpassed by any other system, government or private. Today the vast majority of American adults are the subjects of credit files and reports from one or more of the country's three giant reporting companies—Experian, Equifax, and TransUnion. These and other companies centralize data from

credit accounts, public records, and elsewhere to provide real-time readings of consumers' desirability as credit customers.

Credit reporting companies sold an estimated one billion reports and scores on American consumers in 2004. In 2002, the industry grossed roughly $4.6 billion on its American sales alone, making it comparable to aluminum manufacturing or private catering in dollar volume. Sales of personal data by credit reporters shape Americans' access to everything from credit accounts to employment and insurance coverage. Without a credit record, a normal consumer existence in the United States is all but impossible.

From all evidence, the first credit reporting systems were simple "blacklists" of bad debts, shared among retailers in America's largest cities. Overcoming their natural instincts of competition, department stores and other local merchants agreed that all would benefit by preventing consumers who had failed to pay their bills at one establishment from repeating the experience with the others.

The first qualitative leap from the simple exchange of information on bad accounts was the realization that judgments on consumers' credit use could be forward-looking, as well as retrospective. The "right" personal information could make it possible to identify credit applicants whose records were free of bad debts but who were approaching the limits of their expendable income. In short, consumers who were "loaded up," in the industry jargon—risky possibilities for new credit accounts.

This insight led early credit bureaus to compile data on *all* of a consumer's credit accounts—those in good standing, as well as any that had become problematic. This "positive" credit reporting, as industry spokespeople like to call it, enabled the credit-grantor to anticipate consumers' credit performance, perhaps before they could do so themselves.

By the mid-twentieth century, most credit reporting companies were small, local businesses, often controlled or even owned outright by the largest local retailers. They collected personal information from various sources—consumers themselves (via the applications they completed in seeking credit); merchants (who shared their credit account information with the credit agencies); employers (often willing to verify credit applicants' reports of the employment status and salary); and public records (for data on bankruptcies, tax liens, lawsuits, and court judgments). Credit agencies sold this information, by mail or over the phone, to retailers and other businesses.

Note that the *customers* of reporting companies were not the consumers who furnished the subject-matter for the reports but those seeking to do business with these consumers. Most credit reporting agencies attempted to keep their activities as much as possible out of the public eye—apparently on the assumption that public attention could only complicate their work. For decades, ordinary consumers were often unaware even of the existence of this industry.

Credit reporting companies imposed a firm rule on the businesses who purchased their informational products: purchasers of credit reports must also supply account data from their files to the reporter. Such reciprocity ensures constant renewal of the seller's stock of informational capital. Then as now, many buyers of reports would prefer to avoid this obligation, thereby making it more difficult for would-be competitors to identify their best customers. But the industry has consistently enforced the principle that buyers of credit information must also be providers of data on their customers' accounts.

Note that these considerable achievements in credit surveillance date to well before the advent of computing. By the 1950s, I would estimate, most middle-class American families were the subject of credit files—then typically manila folders kept in file cabinets and plied by armies of mostly female clerks. Many of the more sophisticated credit bureaus had perfected the art of providing quick responses to inquiries over the phone from retailers seeking instant information on the background of specific consumers. Thus an auto dealer or department store would obtain customers' names and addresses while they were still shopping and telephone for a report. The agency would then respond at once—preferably before the customer had the chance to leave the establishment and compare prices elsewhere, or perhaps even reconsider the purchase altogether. Such impressive performances relied on nothing more technologically sophisticated than file cabinets of credit records and the telephone.

By the 1960s, a few industry visionaries had grasped the possibilities of computing. The new information technologies, they saw, were ideally suited to transforming the industry—mastering the storage, retrieval, and transmission of vast amounts of fine detail and thereby cutting labor costs while raising the capacity and speed of all operations. Today, of course, virtually every step in credit surveillance occurs electronically, once data from credit applications are entered into consumers' computerized credit files.

But other changes, no less momentous, were also stirring just after mid-century. Most influential was the rising mobility of Americans and the centralization of American retailing. People were shopping less at strictly local retailers and looking more to nationwide enterprises—Sears, J. C. Penney, Macy's, etc.—as sources of goods, services, and credit. Crucial in this trend was the rise of credit card use among middle- and even low-income Americans. For the credit reporting industry, this meant that buyers of credit reports were more likely to be vast regional or national companies and less likely to be local merchants. The same centralization, of course, also applied to the *sources* of information for credit files, which increasingly arrived en masse from companies operating on a national scale.

The credit reporting industry evolved in concert with these changes. Aggressive, increasingly computerized companies with national operations bought out smaller, local reporting agencies, or drove them out of business. Today the big three credit reporting companies overwhelmingly dominate the American market.

By the end of the 1960s, Americans' passive acquiescence to credit reporting was wearing thin. Critical writings and media reports began calling attention to practices that the industry had long succeeded in keeping off the public radar screen. Increasingly aware of the effects of credit reporting on their lives, and increasingly mistrustful of authority in all forms, Americans demanded that "something had to be done" to defend their interests in the flow of credit information. The result was the Fair Credit Reporting Act of 1970, the first national privacy legislation in the United States.

But FCRA challenged virtually none of the practices essential to the industry. It ratified the sale of credit reports for purposes of credit, employment, insurance, tenancy, and other business purposes—virtually the full array of purposes for which they had always been sold. It required that bureaus take "reasonable steps" to ensure accuracy of their reports but imposed no liability on the companies, unless inaccuracies stemmed from actual malice.

It mandated procedures to correct disputed information in credit reports. But it placed the burden of action in these cases entirely on the consumer, leaving responses to consumer complaints largely to the discretion of the company. With some modifications, these principles have continued to the present day. The subsequent Fair and Accurate Credit Transactions Act enacted in 2003 strengthens a few of these provisions but continues to leave it to consumers to identify mistakes in credit records and to appeal for their

correction. And in a significant victory for the credit reporting industry, FACTA prohibits states from enacting more stringent controls on the marketing of credit data than those authorized in the federal law.

Total consumer debt in America—that is, obligations unsecured by collateral—rose from $131 billion in 1970 to more than $2 trillion in 2006. By the end of the twentieth century, most American adults probably could not remember a time when family finances were possible without recourse to easy personal credit. And in this increasingly credit-dependant economy, Americans required recourse to their credit records not just more frequently, but more rapidly.

A key result was the industry's shift to marketing credit *scores* as its key product. In their classic form, credit reports resembled school report cards—lists of current and recent credit accounts showing how much was owed and how promptly the account was paid, along with citations of public record information such as bankruptcy. These discursive reports had the virtue of leaving it to the user to determine how much significance to ascribe to different elements of information conveyed there. But they collided with rising demands for instant decision making—on-the-spot approvals of consumers' credit by retailers, for example, or instant revisions of credit limits to accommodate eager shoppers.

Since the late 1980s, the industry response has been to distill consumers' entire credit records to single, three-digit scores intended to capture their overall desirability as credit customers. The scoring systems add points for consumers' records of promptly paid current and past accounts and for large amounts of *unused* credit. They deduct points for records of late payments and default; for current accounts near the limit of available credit; and of course for bankruptcy. Virtually instantaneous transmission of these scores to retailers, credit card companies, and other buyers has become essential to the fast-moving American consumption style that the U.S. credit industry is now exporting all around the world.

Today it would be hard to overstate the impact of credit scores on Americans' lives. Credit reporting companies—like TransUnion, source of the statement at the beginning of this part—assign virtually every American consumer one of these three-digit scores, evaluating his or her desirability as a credit customer. Constantly changing—so as to reflect unfolding changes in consumers' available resources—the scores filter access to everything from credit cards to employment to home ownership. A low score can readily block

access to a bank account, insurance, a job, or a place to live—since banks, employers, insurance companies, and landlords all prefer to deal with good credit risks. Good scores, by contrast, open the floodgates to commercial invitations to use more credit for everything from consolidation of existing credit accounts to Caribbean vacations. It is not too much to say that an American's credit score encapsulates his or her claim on the creature comforts of this consumer society.

The sophisticated discriminations afforded by these systems take one's breath away. Credit scores change by the day, as the reporting system tracks consumers' new credit purchases, payments made and missed, and credit extended or restricted. One result of such close monitoring is consumers' rude discoveries that the rates they pay for credit abruptly rise, even for accounts in good standing, when their credit scores decline. In an ultra-responsive system of "positive reporting," approaching the limit of credit available in one account typically lowers one's credit score—and in turn sets off a chain reaction of higher monthly charges throughout the rest of one's accounts.

Things have come a long way from the first pooled "blacklists" of bad debts.

Direct Marketing

Visitors from abroad are often astonished at the pervasiveness of direct marketing in the United States. The daily American experience of sifting through deceptively packaged communications in one's letter box, or of fending off telephone appeals for unwanted offers, has little equivalent in countries with stronger privacy laws. America's direct marketing industry has developed systems of personal data nearly as vast and far-reaching as those fueling credit reporting. Still, direct marketing in America represents a modest exception to the general triumph of surveillance interests in the private sector. For here and there, popular indignation has actually triggered measures leading to significant restrictions in privacy-invading practices by a powerful industry.

Direct marketing means targeting commercial appeals to the susceptibilities of specific consumers. As in credit and insurance, discrimination is of the essence. Mailings, e-mail spam, or junk phone calls that yield no sales represent pure loss. By compiling the right personal data—on income, consumption habits, political affiliation, education, reading habits, and on and

on—and combining such data with pertinent information on characteristics of neighborhood and region, direct marketers seek to deliver the most profitable customers to their clients.

Increasingly important as sources of raw material for these discriminations are data that consumers effectively generate on themselves—only to be packaged and sold by institutional interests. Credit card companies, mail-order houses, periodicals, and countless other commercial interests regularly sell data on their customers' choices and consumer predilections. Particularly striking among these practices are uses of data on consumers' supermarket choices, harvested at the checkout counter through shoppers' use of discount cards. Chain stores scour these data to orchestrate their marketing, targeting customers with discount coupons and other inducements to maximize their return business.

Further sources of direct marketing data include surveys consumers complete in exchange for free offers and questionnaires submitted along with warrantee forms for new purchases. Others are data on drug prescriptions, captured in the course of transmission from pharmacists and made available to pharmaceutical companies for marketing purposes. Still others are culled from hotel registration lists, magazine subscription lists, data provided (often unwittingly) by website visitors or callers to 800 numbers—and on and on.

Such data are truly commodities—bought and sold, transmitted, traded, and massaged—by nearly two thousand information brokerage companies in the United States. The Direct Marketing Association, the industry's powerful Washington lobby, estimates the volume of its members' business in 2005 at more than $161 billion. This level of activity makes an industry largely devoted to "data mining" comparable in size to the American mining industry in the old-fashioned sense—coal, iron, bauxite, etc.

Enriching the discrimination value of these data are other forms of information that are highly suggestive of personal inclinations, yet not personal in the sense of describing only one person. Data characterizing neighborhoods where consumers live, for example in terms of values of houses, or even the size of lots, or the predominant makes of car registered there, or the prevailing party registration of voters—these and many other shared characteristics of residents on a particular street, or in a highly specific postal code, or in a single community also help target direct advertising appeals. Combined with other strictly personal data, they establish strong probabilities of susceptibility to precisely targeted advertising appeals.

The most stunning uses of these databases occur through ingenious *triangulation* of insights from different sources. A resident of a largely gay neighborhood may remain in the closet for all public purposes. But data on his magazine subscriptions, his prescription medicines, or his recreational choices—all often available in marketing lists—may reveal him as sharing enough characteristics in common with other gays as to bracket him in that category for marketing purposes. Indeed, characteristics of the neighborhood in which this same consumer lives—large numbers of single males, high readership of certain publications, distinctive product choices—may establish such associations, even in the absence of any information about him other than his address.

Such is the sophistication of American direct marketing that companies hype highly targeted lists based on just such triangulations. One can reasonably expect to purchase a listing of five thousand women who are both public employees and buyers of sexy underwear; or business owners who espouse far-right political causes; or registered Republicans who are also purchasers of pornography—or, for that matter, of pornography with S-M themes. Often industry research reveals associations that are as unintuitive as they are vital for marketing—for example, the discovery in a recent presidential campaign that buyers of a particular car-washing product proved enormously susceptible to Republican campaign appeals. Once such associations are established, it matters little why they occur, and even less how those targeted as a result feel about the attention directed their way.

Sometimes the results are disturbing to those targeted. Privacy law experts Joel Reidenberg and Paul Schwartz note the sale of guest list information from a hotel frequented by lesbians to sellers of products likely to be purchased by this same population. They go on to cite some extraordinary sets of personal data offered for sale by brokers: women who buy wigs; callers to a romance telephone service; impotent middle-aged men; gamblers; buyers of hair removal products; male buyers of fashion underwear; believers in the feminist political movement, anti-gay movement, and prayer in the public schools movement.[1]

In Europe, such sales would be illegal. The E.C. Privacy Directive of 1995 proscribes "secondary use"—that is, further commercialization of personal data from business transactions without the consumer's consent. The practical result is drastic curtailment of the "background noise" of personalized commercial hype that is all but universal in the United States. Industry lobbyists have vigorously and effectively opposed attempts to restrict the nonconsensual

harvesting of personal data in the United States. They have based these appeals, with some success, on legal arguments that such commerce represents a form of free speech, and as such is protected under the First Amendment.[2]

But regarding *use* of direct marketing data, American privacy forces have gained some modest victories—notably in the control of "junk" telephone calls. By the end of the twentieth century, many American families had come to take it for granted that their dinner hours would be punctuated by unwanted phone calls from hard-selling marketers pushing everything from insurance to home repair to political candidates. Consumers had no way of knowing where or how their names and phone numbers had become available, and still less chance of stopping the onslaught.

But by the 1990s, states began to establish "do not call" registers, to which residents could add their names and phone numbers. Callers who continued to make commercial calls to these numbers were subject to prosecution. In 2003, over the opposition of the Direct Marketing Association, the Federal Communications Commission and the Federal Trade Commission established a national version of such a list, adding Washington's authority to actions already taken by the states. Significantly, the listing exempts charities, political campaigns, and organizations claiming "an established business relationship" with the consumer—an uneasily elastic concept.

Against unwanted mail, protections are weaker. The Direct Marketing Association has established a centralized "do not mail" database for consumers wishing to avoid junk mail, and its members are required to respect these wishes. Nonmembers of the association are free to target anyone whose name and address they can obtain.

Insurance

Insurance marketing is possible only under conditions of uncertainty. Were losses certain, no one would ever offer insurance against them. Nor would anyone ever purchase insurance, given certainty that no loss would occur. People accordingly would prefer to purchase insurance only when certain of needing it. And insurers would prefer to sell it only to those destined never to file claims.

Uncertainty in these matters thus creates a space in which the sale of insurance flourishes. But such uncertainty is rarely complete, and rarely evenly distributed between buyers and sellers of insurance. Those seeking

insurance—for their lives, their possessions, or their future liabilities—often know more than they want to divulge on the risks that insuring them poses. And sellers of insurance, for their part, have learned how to identify risks that even would-be buyers are not aware of themselves. The press to create systems of finding, exchanging, and interpreting personal data to support discrimination in insurance sales generates its own distinctive pressures on privacy.

The simplest measures involve collecting data on claims and mishaps from the past, on the assumption that they portend more of the same for the future. But other, more sophisticated strategies involve assembling and interpreting personal information that has no obvious *logical* connection to future claims but that appears to predict such experience and hence distinguish more desirable insurance customers from the less desirable.

In life insurance, MIB—a Connecticut company—pools data on applicants' medical conditions for use by all insurers. Companies selling life insurance widely require applicants to undergo medical examinations, often accompanying these with far-reaching questionnaires concerning risk-related lifestyle matters. To prevent applicants from evading the effects of these inquiries by "shopping around" among carriers, North American insurers forward results of these inquiries to MIB. Every application for life insurance triggers an inquiry to MIB, so that it is all but impossible to evade information turned up in past applications. MIB also makes its database available to sellers of individual health care policies. In both cases, the intended effect is to ensure that information indicating heightened risk of mortality, once obtained in one insurance investigation, is never lost.

Insurance applicants often take much exception to such reporting. Consider the story of Mark LaBonte, an Oakland, California, resident.

> As part of a life insurance application, LaBonte was required to take a blood test for HIV. The report, fortunately, was negative. But his agent then informed him that the insurance company, Minnesota Mutual, wanted to review his file. Within a month, the company declined coverage. The file, it turned out, recorded LaBonte's remarks making it clear that he was gay and that he had been practicing safe sex with an HIV-infected partner. He is convinced that these admissions constituted a red flag, blocking the coverage that he sought. He also complains that, by reporting its decision to the MIB, Minnesota Mutual had prejudiced other insurance companies against him.[3]

Evidently, vast contention surrounds the assessment of risk and the kinds of risks that ought to bear on insurability.

In auto insurance, a major source of actionable personal data is state agencies. Every American consumer probably realizes that the rates offered for such insurance depend on one's past driving record—and that state motor vehicle departments compile and furnish such records. The agencies centralize data on accidents reported to police, citations for motor violations, and suspensions and limitations imposed on drivers' licenses. Provision of such information to insurance companies, and to companies providing reports to these companies, constitutes a major trunk line of personal data flow. California, for example, issues such reports in bulk to insurers and other businesses, at rates as low as $100 per thousand reports. So crucial are these data to insurers that providing such data has become a major source of revenue for nearly every state government. California, for example, now realizes more than $40 million annually in revenues from such sales.

Aggressive entrepreneurs are also major conduits of personal data fueling insurance discrimination. Best known among them are ChoicePoint and Acxiom—both corporate offshoots of the consumer credit reporting industry. These companies systematically compile personal data from state vehicle and driving records; from insurance companies' own records of past policies issued and claims paid; and from courthouses and other public record sources. These public institutions increasingly record—and disseminate—such information electronically, vastly lowering the costs of collecting and re-selling it. Where data are still in hard-copy form, entrepreneurs dispatch workers to courthouses and other repositories throughout the country. There they laboriously record data on real estate transactions; taxes paid and not paid; marriages and divorces; criminal convictions and civil judgments; bankruptcies; and virtually any other form of personal data that is publicly available. These data are in turn computerized and sold in reports to insurance companies and other interested parties.

This information has long held interest for insurers. But only the rise of computing could have afforded today's combination of centralization with breadth of coverage—so that facts and incidents from anywhere in the country are apt to find their way into reports available to buyers anywhere else. This comprehensiveness obviously aims at bringing to light precisely those elements of personal history that applicants are most likely to censor out of their applications for insurance coverage, jobs, and other relationships.

Buyers of the resulting reports include sellers of virtually all forms of insurance. They also include employers and a variety of other parties contemplating dealings with the subjects of reports. For insurers, obviously, a key interest is the applicant's claims history. Any insurer will obviously balk at insuring against a loss that has already been the subject of many claims from the same applicant—a fifth diamond ring, where a previous four have been reported stolen; or a seventh sports car, where the six previous have been written off after accidents.

But beyond these predictable associations, insurers also use data from these reports in far more *inferential* ways. Many insurers will no doubt steer clear of applicants whose reports reveal criminal convictions or legal judgments, even where the insurance sought has no obvious relation to the untoward incident. Here the rationale would be that one form of trouble predicts others—that applicants with criminal convictions are more likely to file claims. Similarly, industry observers have recently noted that some sellers of homeowners' insurance monitor policyholders' *inquiries* about their coverage, for example, as to whether a particular form of loss was covered, or at what deductible.

Thus Evan Hendricks, editor of *Privacy Times,* writes of ChoicePoint's CLUE reporting system: "This system was designed to keep track of claims filed by homeowners going back five years. . . . [but it has become] controversial for a couple of reasons. First, anecdotal information indicates there is a significant error rate that directly causes wrongful denials of homeowner policies or hikes in premiums. Second, some people have found their premiums were raised for simply asking questions about their coverage. Others saw their rates go up after they reported minor damage but refrained from filing a claim."[4]

Here the insurers' strategy is clear: inquiries about coverage predict future claims. Even in the absence of claims as faits accomplis, a rational system of pricing dictates a preference to do business with consumers who don't even *think* about using their coverage.

Another use of personal information is still newer, and more subtly inferential. This is the industry's reliance on *credit scores* as predictors of future claims. Early in the 1990s, America's credit reporting giants began promoting the idea that the three-digit scores increasingly used to set terms for consumers' access to credit could play the same role in screening insurance applicants. Credit scores, they held, inversely predict insurance losses—that is,

insurance applicants with the worst credit are also the most likely to file claims. By offering higher prices to those with lower credit scores, the pitch went, insurance companies could avoid dealings with the least profitable insurance applicants or raise the premiums charged to them.

Providers of auto, homeowners, and other forms of insurance in America have largely accepted this premise—to the extent that they routinely purchase credit scores and rely on them to set terms for coverage. Both industries have sought a low profile on this new form of surveillance, for reasons easily understood: the effect is surely to add to the disadvantages experienced by low-income consumers, who typically have lower credit scores. In addition to finding it more difficult to obtain credit, and paying more when they obtain it, low-income consumers now also face higher charges when they seek insurance.

The industry has had little to say publicly about reasons for the purported link between credit and insurance risks. One industry spokesman offered the anodyne suggestion that anxieties over credit might make insurance policyholders more accident-prone.[5] Ultimately, the reasons for the association matter little to the organizations concerned, if only it enables them to sharpen their discrimination and thereby raise profits. For the insurance industry, that association is now credible. The credit reporting industry has thus managed to open a significant new market for its products—broadening the impact of mass surveillance in the process.

When publicly aired, these practices have often triggered indignation. Why penalize those at the bottom of the heap of consumer advantage doubly, in the absence of any logical connection between the two forms of risk? A few states have accordingly outlawed this new use of credit scores.[6] Nevertheless, it has become an accepted recourse in most of the United States. As the following discussion shows, the American credit reporting industry is now exporting this innovation to other consumer societies.

As every American knows, medical care has become one of the most intensively monitored and documented realms of life. By historical standards, this obsession with recording, transmitting, and analyzing details on what used to be considered the most private areas of life is relatively recent. When patients and their private physicians were the only parties involved, record-keeping was vastly less extensive, sharing of patient data minimal, and assurances of

confidentiality realistic. Upending this relatively simple reality has been the vast expansion of interested parties in medical care delivery—health maintenance organizations and third-party payors, above all, but also government agencies and billing operations engaged in allocating costs for treatment. Cross-cutting demands for patient data among such parties—as bases for treatment decisions, billing, and cost control—have generated blizzards of personal documentation. Efforts to detect and combat fraudulent billing of government and private insurance programs generate intense monitoring of care delivery. By the end of the twentieth century, individual control over access to and use of such data had all but collapsed.

In a country without universal health care coverage, individuals seeking to secure health insurance face market-driven industry efforts to avoid insuring those likely to generate claims. This environment obviously sharpens patient interests in controlling data on their own medical care—lest information about earlier diagnoses and treatments trigger higher premiums from insurers, or even outright refusal of coverage. And where patients are indeed covered by private or government health insurance, the parties concerned demand ever more intense documentation of treatment in their efforts to deflect costs to other parties.

In response to some of these pressures, investigative companies have often resorted to aggressive strategies for collecting medical data. Robert Gellman, former Congressional staff member and privacy consultant, cites the activities of Factual Services Bureau, a company that specialized in discovering and selling medical data for use in court litigation. "The company's investigators typically posed as doctors," Gellman comments, "and sought medical information by telephone from public and private hospitals, clinics and doctors' offices, including psychiatrists' offices. The company paid hospital employees to smuggle out health records. Another technique involved the use of false pretenses through mail solicitations. The company was successful in obtaining health records most of the time, and it even advertised its ability to acquire health records."[7]

Faced with these and a host of other disturbing practices, Washington long struggled to create some national standard for privacy in medical information—and for years, failed spectacularly. After false starts dating to 1980, Congress finally passed HIPAA, the Health Insurance Portability and Accountability Act in 1996, giving itself until 1999 to create privacy rules mandated in the act. That deadline came and went without results, as

conflicting interests asserted themselves in a feeding frenzy of claims over access to patients' medical data.

In 2001, the Department of Health and Human Services adopted the HIPAA "Privacy Rule," intended to provide a minimum privacy standard for personal data held by medical care organizations: providers, insurers, billing services, and others engaged in transmitting patient data. It ensures patients rights of access to their records; opportunities to seek corrections to erroneous entries; and the ability to determine to whom their data have been disclosed. But though termed a "Privacy Rule," it actually authorizes release of medical information for a broad range of purposes without patient consent.

These purposes include (as most Americans would probably expect) disclosure to other medical care providers, billing services, and insurers. But the Privacy Rule also permits disclosure without patient consent to law enforcement and national security agencies; investigators of "abuse, neglect or domestic violence" or "to avert a serious, imminent threat to public safety."[8] In addition, disclosure without consent is permitted to organizations involved in "health care operations"—an array of bureaucratic activities ranging from fraud prevention to monitoring of care-givers' performance. Disclosure of certain forms of mental health information may be blocked by the patient. But broad ranges of other "routine" disclosures—to use the language of the rule—may go forth even over patients' objections. Patients may request restrictions on release of their data, but in many cases institutions are not required to heed such requests.

Theoretically these strictures should preclude sale or trade of medical information to insurance companies and those selling reports to such companies—as their activities are not among the officially permitted purposes for disclosure. But given the frictionless flow of medical data among institutions authorized under HIPAA, one has to wonder. It is easy to imagine ways in which information requested and supplied through authorized channels could be diverted to interests quite unfriendly to those of patients. For example, what private health insurer or HMO would want to enroll a single male who repeatedly had himself tested for HIV—even if all test results to date had been negative?

All things considered, HIPAA privacy strictures fall conspicuously in the "Fair Information Practices" tradition of privacy measures. Parallels to America's Fair Credit Reporting Act of 1970 and Privacy Act of 1974 are striking. Like the FCRA, the HIPAA Privacy Rule does grant individuals the right to

access their own files—and to correct the record, if holders of the data are willing to cooperate. But it provides slender possibilities for patients to "just say no" to uses and disclosures of data on themselves that they may find repugnant. And it establishes no private "right of action"—ability to sue—where even the mandated protections are violated. Like the Privacy Act, it brackets an array of questionable uses of personal information as "routine," thereby begging the question of whether they *ought* to be routine. And like the Fair Credit Reporting Act, it leaves undisturbed most of the established forms of institutional access to patient data prevailing when the rule was enacted.

According to news reports, nearly twenty thousand patient grievances were filed in the roughly three years following adoption of the Privacy Rule. The Bush administration, however, has prosecuted just two criminal cases, and imposed no civil penalties.[9] Here, as elsewhere, privacy protection is understood to entail informing people of uses of data on them but not fundamentally constraining the institutions involved in such use.

Blurring Boundaries

By now, it should be clear how much surveillance systems benefit from *symbiosis* with one another. Organizations exploiting personal data for decision making on people reach out for such mutual support as a matter of reflex. Each of them needs bits of data and possibilities for action that only other such systems can provide.

Examples from these private-sector systems are abundant. Perhaps most striking is the flow of credit information into insurance—the reliance of insurers on credit scores for fine-tuning discriminations among those seeking coverage. But the same principle is at work in the use of credit data by direct marketers in some countries, who rely on consumers' credit files to target advertising to those judged most promising to become profit-generating customers. Given the logic of mass surveillance, some ingenious entrepreneur will no doubt eventually find ways to use personal data generated by insurance accounts to direct the targeting of credit and advertising.

Explaining these trends hardly requires conspiracy theories. Like the propensity of businesses to reduce employment by raising productivity, the tendency of surveillance planners to form symbioses with other surveillance systems is simply ordained in their situation. Knowing more about people almost always helps institutions refine discrimination in dealing with them. And

as more personal data are generated at more different junctures, the entrepreneurial imagination constantly seeks new outlets for their sale or trade.

Of course, these trends ratchet up pressure on privacy. Indeed, they countervail against one of the basic fair information practices noted in part I—the notion that personal data provided for one purpose should not be diverted for other purposes without consent from the individual. By contrast, the attraction of symbiosis among surveillance systems is precisely to exploit the uncensored qualities of information provided in settings different from those in which it is used.

Today in America, virtually any publicly recorded personal data are subject to sale, for almost any commercial purpose—as are many data intended to be anything but public. Where the purposes are not covered by existing legislation, they flourish exuberantly in the absence of laws specifically forbidding them. Major steps in this direction came with the rise of companies like Acxiom and Choicepoint, created by the giants of the credit reporting industry to sell personal reports to the insurance industry. While the insurance industry remains a major outlet for these companies, they have continued to find buyers in quite different institutions—including U.S. government agencies.

Supporting this expansion is the growing ease of electronically capturing public records of all sorts. The spreading availability of such information has in turn inspired many entrepreneurs to furnish reports to buyers with the widest variety of interests in those being reported on—often with no questions asked. The sales appeals from these reporting companies make no apologies for the breadth of interest that they cater to—as in the following example from a company called Abika: "Background checks are a good start to get to know someone. Just about anything that you would like to know about someone could be archived somewhere or known by someone. . . . Whether its [*sic*] a personal or business relationship, people need to feel secure about the people they enter into relationships with. Even in the workplace the value of background checks is undisputed. Background checks can be customized to fit your needs. . . ." Among the data services Abika offers are "Search Unlisted Phone Number," "Reverse Phone Number Search," "List of Calls made," "Search Possible Girlfriends/Boyfriends/Roommates/Spouses," "Mail Forwarding Addresses."[10]

Those in the industry draw a distinction between "FCRA and non-FCRA products," that is, those reports required to comply with the Fair Credit

Reporting Act, and the rest. Providers of the latter are under no obligation to provide people free access to records held on themselves or mechanisms to correct erroneous entries. Acxiom and ChoicePoint sell both FCRA and non-FCRA reports. Companies like Abika sell only non-FCRA products and generally appear prepared to do so to virtually anyone claiming a legitimate business interest and prepared to pay up to several hundred dollars for a made-to-order sweep of available databases.

Markets are wonderful devices. They bring together those willing to pay for the most diverse sorts of goods and services with those who can provide them. And they encourage investment aimed at capitalizing on future marketing possibilities—even where only visionaries recognize the prospects. That is what has occurred in American surveillance industries in recent decades. Realization that buyers will pay for personal reports of the most disparate kinds has inspired forms of exchange that no one could have anticipated a generation ago. The rendering of public records—everything from criminal convictions to property liens and divorce actions—into computerized storage has vastly accelerated this trend. And American privacy law affords precious few opportunities for consumers to "just say no" to these treatments of their data.

Markets Abroad: The American Model versus Privacy Constraints

There is nothing subtle about the commercial pressures that have given rise to these markets in personal data. They arise directly from efforts of major industries to allocate consumer credit, sell insurance, or precisely target advertising appeals. But the outcomes of these pressures manifest in the United States are not foregone. Other democratic, consumer-oriented societies have imposed varying constraints on the commercialization of personal information.

Australia: Some Populist Privacy Protections

Those who know both countries often remark how closely the United States resembles Australia. Both are English-speaking, ethnically diverse, immigrant countries, with political and legal traditions derived from Britain. Both are highly suburbanized, with high living standards and high rates of home

ownership. And both are exuberant consumer societies, where acquiring and spending approach the level of national obsessions, and where the credit, insurance, and direct marketing industries compete for consumers' dollars. Yet despite these parallels, market-generated pressures on privacy that have succeeded so fabulously in the United States have met with significant resistance in Australia—at least thus far.

Australians rely on *consumer credit* in broadly the same ways as Americans—through use of credit cards, credit accounts with retailers, and loans from banks and finance companies. As in all consumer societies, access to credit is stratified, with the "best" customers obtaining credit more often from banks, and those posing greater risks obliged to deal with finance companies and other second-tier credit grantors.

But all credit relationships pose the same universal problem of discrimination: how is the grantor of credit to determine how much credit to offer a particular consumer, and at what terms?

Like its American counterpart, Australia's credit reporting system originated in credit grantors' exchange of data on bad credit accounts. By the mid-1980s, these systems had been consolidated into a single, industry-owned credit reporting corporation. That company planned to create an American-style system of "positive" credit reporting—selling not only data on bad accounts, but also *all* current credit use.

But history intervened to disrupt these plans. In 1987, a quite unexpected privacy controversy rocked Australia—the revolt against the government's proposed "Australia card" described in part II. Given the public mood, privacy advocates saw a chance to block the extension of credit surveillance. Legislators were persuaded to restrict credit reporting to the then-prevailing practices—recording and reporting mainly on *bad* credit accounts, that is, those legally in default. Legislation upholding this restriction passed in 1989 and with minor adjustments prevails at the time of this writing.

Credit reporting nonetheless remains an important feature of Australian consumer life. The consolidated national reporting company mentioned above has passed into private hands, where it now faces competition from the multinational Dun and Bradstreet. Whenever Australian consumers open an account with a bank, take out a loan, or apply for a credit card, they can expect a credit report to be drawn from one or both of these companies. In addition to listings of officially delinquent accounts, such reports may include a record of recent *inquiries* to one's record. Some credit grantors would

interpret large numbers of inquiries as a bad sign, indicating an urgent need for credit. Credit reporting companies also compile certain public record data such as bankruptcies, tax liens, and the like. But buyers of credit reports typically cannot determine how many accounts in good standing the applicant has open—except by seeking such information directly from the applicant. Still less can credit grantors determine the amounts owing on other "good" accounts without directly contacting creditors willingly identified by applicants on their credit applications. Thus the system permits applicants to shape and censor the data on their credit histories that they put forward to banks, credit card companies, and other prospective sources of credit.

Australian credit grantors accordingly have blunter surveillance instruments at their disposal than their American counterparts for judging applicants' current obligations. Indeed, Australian consumers who maintain long-standing credit relations with a single set of companies and incur no delinquencies are apt to have minimal credit records. In this relatively privacy-friendly environment, less news mostly amounts to good news to prospective credit grantors.

The Australian system leaves creditors in the dark about their customers' other accounts—so long as they remain in good standing. By the same token, it obviously makes it more difficult to calibrate credit extended to any given consumer precisely to the level most profitable to the credit grantor. It likewise prevents credit grantors from raising rates charged to account-holders when the total amount of their outstanding credit in *other* accounts rises—a frequent recourse among American creditors. And it blocks the American-style commerce in credit *scores* based on comprehensive monitoring of all of a consumer's credit accounts. Australian credit grantors are of course free to develop their own ratings of the desirability of any specific credit applicant, based on information available to the creditor. But that information normally does not include data from other accounts in good standing.

Still, consumer credit and credit reporting flourish in Australia. Credit grantors evidently consider the investment in credit reports a cost-effective way of reducing their risk—and consumers show every sign of awareness that officially reported credit delinquencies can jeopardize future access to credit. As a result, many providers of services not ordinarily considered to involve credit—like phone service, electricity, and water—have sought legal designation as creditors, so that consumers' failure to pay these bills will be penalized via a black mark on their credit records.

Nor have Australia's privacy-friendly restrictions on "positive" credit reporting posed any absolute obstacle to access to the gratifications sought by consumers in both countries—though some forms of credit use are at lower levels than their U.S. counterparts. A study by Stephen Nunez carried out in connection with this work found that Australians hold about a fourth as many credit cards as Americans, on the average, but about half again as many debit cards. Total outstanding consumer debt in Australia, as a proportion of GDP, is about two-thirds that in the United States. Percentage of homes owned by occupants with mortgages is about 8 percentage points lower in Australia than in the United States—suggesting that restrictions on credit reporting have not posed a major barrier to home ownership. Fuller presentation of these findings appears in the appendix to this work.

Restrictions on use of personal information by Australia's *direct marketing industry* are less dramatic than in credit. The Australian industry draws personal data from most of the same sources as in the United States. These include public records, lists of customers maintained by retailers, mail-order houses, public utilities, responses to questionnaires aimed at soliciting consumer information, telephone directories, and a host of others. In both countries, direct marketers actively buy and sell such listings among themselves—often exploiting such sales to create more precisely targeted lists, such as registered Labor voters who own mutual funds, or evangelical Christians who purchase certain types of underwear.

But collection of such data is more restricted than in the United States. Under Australia's privacy law, the freedom of any organization to use personal data for direct marketing depends on the circumstances under which it was collected. Data deemed to be collected for purposes of direct marketing may be disclosed for that purpose without permission from the individual—that is, where "the person from whom it was collected would reasonably expect the organization that collected it to use or disclose it for direct marketing."[11] Where such use is not the primary purpose of collection, personal data may still be used if the individual has had an opportunity to opt out.

As in the United States, direct marketing by phone has antagonized countless Australians. At the urging of the Australian Federal Privacy Commission, Australia's right-of-center government has now enacted a federal law establishing a Do Not Call Register. Like its American counterpart, the law enables Australian consumers to register their desire to avoid phone solicitations, imposing fines on those marketers who disregard these wishes. Significantly, the

list of proposed exemptions from these requirements is slightly broader than in the American case: charities, registered political parties, educational institutions calling students or alumni, and government agencies.

As in the United States, the Australian *insurance industry* relies on a mixture of commercial reporting and databases created by the industry itself to generate the personal information it seeks.

Baycorp Advantage, the largest producer of consumer credit reports, also provides reports on applicants for various forms of insurance, as do other companies. Routinely drawn upon by insurance companies considering applications for coverage, these reports list such matters as past claims; insurance inquiries (that is, requests for quotations for costs of insurance coverage); credit inquiries (that is, inquiries made to the applicant's credit record); and public record information on such matters as bankruptcies, tax liens, criminal convictions, and the like. These reports play the same role as those furnished in the United States by companies like ChoicePoint and Acxiom—both now active in Australia, as well—enabling insurers to judge risks posed by insurance applicants.

In addition, the Australian insurance industry maintains several indexes of risk-related data, including vehicles listed by the police as stolen and vehicles removed from registration. Information for these data systems is obviously derived from public record sources.

But insurance data flows in Australia do confront some privacy constraints that have no parallel in the American case. Australian privacy law limits dissemination of information on drivers' accidents and police citations, which constitute a basic (and unquestioned) data flow in the United States (and much of Canada, as well). It forbids the pooling of data from medical examinations given in connection with life insurance, as in America's MIB. And the absence of "positive" credit reporting in Australia makes it impossible to furnish credit scores as a basis for weighing insurance risk. As one thoughtful industry executive noted in response to my query, "The correlation between credit rating and insurance risk . . . is not as strong [in Australia as in the United States] as we do not use a positive credit reporting system. . . ."[12]

All things considered, Australian consumers are subject to less pressure on their privacy than their U.S. counterparts—largely because of legislation restricting exploitation of certain potentially profitable personal data. But as one

Australian consumer advocate remarked to me, "We always look to the United States to see what's coming next here in Australia" in the way of marketing innovations and retail practices.

With that in mind, it is worth noting that elements of these industries in Australia have been mounting major lobbying efforts in recent years to scrap privacy constraints on credit reporting in favor of the American model.

Canada

If any country could be expected to follow American practice in treatment of personal information, it should be Canada. The two populations, everyone notes, share broadly similar lifestyles and consumption habits—absorbing many of the same mass communications and purchasing identical or similar products and services from many of the same corporate sources.

Yet Canadians often take pains to differentiate themselves from their southern neighbors in matters of political culture. Many recoil at what they see as the social extremes of the United States. Nearly all observers agree that Canadians place greater faith in government institutions to regulate public affairs and ensure a modicum of social justice. They also increasingly expect their government not to follow U.S. foreign policy as matter of reflex. Consistent with these stances, Canada's policymakers set out in the 1980s to accomplish what the United States has successfully resisted—adoption of comprehensive national privacy legislation governing both government and private-sector record-keeping.

Thus in contrast to patchwork legislation south of the border, Canada has adopted two broad national acts governing treatment of personal data. The Privacy Act of 1982 governs treatment of personal information held by government agencies. The second, the Personal Information Protection and Electronic Documents Act of 2000 (PIPEDA), applies to the private sector. One intent in enacting PIPEDA was to encourage electronic commerce—and thereby stoke the engines of economic growth. Another was to harmonize Canadian data protection practices with those of the European Union. Canadians in effect sought to forestall the trans-Atlantic conflicts that ultimately broke out between Europe and the United States. There the EU judged American private-sector privacy guarantees not "adequate," thus threatening to block export of personal data from Europe to America.

PIPEDA appears to afford strong defense of individuals' interests in their data. Its precepts are obviously informed by the consensus "fair information practices" described in part I. The act requires that private-sector organizations specify the purposes for which personal data are collected and collect no more than necessary for those purposes. It requires consent from the individual for the uses to be made of such data; such consent must also be obtained when data in a file are redirected to new purposes. And, in a potentially far-reaching assertion, PIPEDA specifies "An organization shall not, as a condition of the supply of a product or service, require an individual to consent to the collection, use, or disclosure of information beyond that required to fulfill the explicitly specified, and legitimate purposes [for which it was collected]."[14] A forceful privacy principle, if kept. But in fact, this precept has been overwhelmed in practice by the same pressures on privacy so abundantly manifest in the United States.

Two large, U.S.-owned companies, TransUnion Canada and Equifax-Canada, dominate Canada's *credit reporting* industry. Their files cover the vast majority of Canada's adult population. Practice closely follows the American model of "positive reporting." Canadian banks, retailers, credit card companies, and other credit grantors who regularly purchase credit information are required to funnel information from all their credit accounts back for inclusion into the reporting companies' files. As in the United States, Canadian credit bureaus also harvest data from public records on court judgments, tax liens, bankruptcies, and other legal matters. Once collated, this information is sold in the form of discursive reports listing individual accounts and payment histories—but more and more commonly as three-digit credit scores. Besides credit grantors—retailers, banks, lending companies, and credit card companies—buyers of credit reports and scores include landlords, insurance companies, and employers.

Under PIPEDA, Canadian consumers' subjection to these practices is, strictly speaking, voluntary. Applications for bank accounts, credit cards, or other credit relationships typically bear language authorizing the institution to gather and review relevant personal data. Canadian law thus far has regarded such "consent" as sufficient to justify the full operation of American-style credit surveillance—perhaps on the principle that these activities are "necessary for the purposes identified by the organization" providing credit, to quote the language of PIPEDA. As in the United States, Canadian law guarantees

consumers the right to review reports about them drawn in this connection and to challenge erroneous information in their records.

But the more far-reaching principles of the Canadian law simply have not been taken seriously in practice. I refer to the language quoted above, affirming that no one need be subjected to recording of his or her personal information, except where necessary to "fulfill the explicitly specified, and legitimate purposes" for which it is collected.

One could argue that consulting an applicant's existing credit record is necessary for decisions on whether to extend credit, and at what terms—though as we have seen, the Australian credit industry successfully generates credit decisions using far less information than that amassed on American and Canadian consumers. But once credit is granted and an account established, it is very hard to see why the consumer should have subsequent details of his or her use of that account—amount of credit drawn, for example, or timing of payments—automatically provided back to the credit reporting agency. In a privacy-friendly environment, consumers would be able to choose whether their use of credit would remain an "open book" for credit reporters following the initial decision to grant credit. Under the stated principles of PIPEDA, privacy-minded Canadians ought to be able to "just say no" to further surveillance, once they have the credit they need.

Meaningful exercise of this option on any scale would place Canadian privacy practice on a collision course with a well-entrenched industry. That industry, like its U.S. counterpart, flourishes by collecting and reporting *all* available data on consumers' credit use—not just those authorized by the consumer. Consumers' effective refusal to permit such reporting would block the automatic flow of data on their ongoing financial affairs back to credit reporting companies and thus dry up their sources of raw materials for further reports. But any attempt at such refusal would meet with vociferous resistance from the industry. A Canadian credit reporting executive told me in 2003 that no one in the industry expected anything of the sort to occur as a result of PIPEDA. At the time of this writing, Canada's Federal Privacy Commission has given no sign of challenging this assumption.

Canadian *insurance surveillance* closely follows the U.S. mode. Applications for life insurance, for example, include a blanket "consent" to contact applicants' current and past medical care providers for patients' health information. Moreover, Canadian life insurance companies rely on MIB much

as their American counterparts do. This is the Connecticut-based organization that compiles medical information collected in screening life-insurance applications and makes such data available to other carriers who might later consider the same applicant. This system works to grant adverse medical data something like eternal life, preventing applicants from obtaining coverage elsewhere when results of one medical examination result in denial of an application for insurance.

Canadian property and casualty insurers also rely on U.S.-style data systems aimed at tracking past claims and other risk-related information. In place of ChoicePoint and similar U.S. companies, Canadian insurers often rely on CGI, a company reporting claims information and other personal data on insurance applicants. In addition to claims history information, CGI reports also include data on applicants' driving histories drawn from provincial government offices. As in the United States, provincial authorities provide driver data freely to insurance companies and to CGI. CGI essentially works on the classic credit reporting model, in which companies purchasing reports are required to furnish information on claims to CGI's central databases. Applying for insurance coverage normally requires granting "consent" to such monitoring.

Finally, as in the United States, the credit reporting industry has succeeded in marketing credit scores as bases for insurance pricing. Most Canadian provinces have blocked the use of these scores for auto insurance, apparently out of privacy considerations, but impose no such limitations on their use for homeowners' or other forms of insurance. The reasons why this use of personal data should be acceptable in one context but not in the other are unclear.

Insofar as credit scores predict the profitability of insurance applicants, their utility as a screening device is clear. But it is surely stretching things to regard such inquiries as "required to fulfill the explicitly specified, and legitimate purposes" pursued by insurance consumers—to use the language of PIPEDA.

In November 2005, privacy had one of its rare moments at the center stage of Canadian media—though not in a way to gladden the hearts of privacy-watchers. A story in the newsmagazine *MacLean's* detailed how, with a few phone calls and payment of US$200, its reporter was able to order detailed phone records of Jennifer Stoddart, the country's federal privacy

commissioner—including dates, times, and places where calls took place, both from her fixed lines and her government-issued BlackBerry cell phone.[14] Perhaps it is significant that the cost of the report, as cited in *MacLean's,* was in U.S. currency. Much of Canada's telecommunications pass through the United States, so it is possible that data for the report were captured there.

Collection and resale of phone records is illegal under PIPEDA in Canada (though not of course in the United States)—because it does not involve even the token consent required by PIPEDA from the target. But similar activities are widespread. A careful report by a research group at the University of Ottawa concluded that data brokers will

> . . . for a fee, provide background checks, criminal records searches, unlisted telephone numbers, cell phone records, psychological profiles, and other information about individuals.
>
> The vast majority of these . . . data brokers are based in the United States. . . . However, there is still a thriving industry based on demand for information about individual Canadians.[15]

If the federal privacy commissioner remains in the dark about these activities, it is hard to see what defense other Canadians have against them.

Canadian *direct marketing* provides some intriguing contrasts to American practice. Like their U.S. counterparts, Canadian direct marketing companies harvest personal data from the most diverse sources—surveys accompanying product registrations, website visits, subscriptions, 800-number inquiries, public records, and others. These data are combined, massaged, and marketed to retailers and other private-sector interests with sales appeals to make. Nonprofit organizations seeking to raise funds and even government agencies are also customers.[16]

PIPEDA, by the letter of the law, should make it easy for Canadians to withdraw from the surveillance processes supporting these appeals. The law clearly states: "When personal information is to be used for a new purpose not previously identified . . . the consent of the individual is required before information can be used for that purpose."[17] These words suggest that active consent is necessary before data Canadians provide on themselves are converted to new purposes—especially when the new purposes may involve unwanted sales appeals. In reality, the protections are considerably weaker.

True, some scrupulous holders of personal data do in fact secure active consent by having customers check a box indicating willingness to have their

data shared—the privacy-friendly "opt-in" routine. Other organizations consider themselves free to re-sell personal data if only "opt-out" opportunities go untaken—that is, if their customers or others whose data they hold fail to check statements indicating objections to the sharing. And under rules promulgated by the Canadian Marketing Association, organizations may *assume* consent "on the part of their existing customers to the company's own marketing of goods and services 'directly related to the customer's original transaction.' "[18]

Unsurprisingly, there have been controversies as to how the directness of such relations should be understood—and as to how conspicuously "opt-out" opportunities should be displayed. But when the latter are in fact invoked, the message seems to be respected by members of the CMA, who constitute the majority of the country's direct marketing industry. The Canadian association, in contrast to its American counterpart, also took early positions to limit dissemination of certain direct advertising to children and to limit e-mail spam. According to industry legend, the reaction of the American Direct Marketing Association to this self-restraint by its Canadian counterpart has been little short of apoplectic.

Great Britain

Those polite civil servants who stressed their fellow Britons' distaste for buying and selling of personal information were probably correct—as of the early 1970s. Since then, British society has undergone something akin to a cultural revolution, bringing head-spinning transformations in public values and private conduct regarding consumption and wealth. The Thatcher era triggered waves of enthusiasm for self-enrichment; conspicuous consumption became a totem of personal success. In the ensuing scramble, retailers, banks, finance companies, and other institutions fostering and profiting from these trends faced a newly competitive environment. One result has been the rise of markets in information on British consumers, very much in the American model.

Until the 1970s, *consumer credit reporting* in Britain was little developed. Most Britons, if they used credit at all, relied on local banks, retailers, or finance companies with whom they had face-to-face relations. But by the 1980s, many financial institutions were competing for credit business, seeking to steal one another's "best" customers by offering more attractive terms for

personal loans, mortgages, credit cards, and the like. Under these circumstances, grantors of credit could hardly expect to rely solely on their own backlogs of account data to discriminate between more and less attractive credit applicants. Thus the rise in demand for independent sources of data on credit-seekers—and the rise of "positive" credit reporting on the U.S. model.

American credit reporting giants stepped into this situation. During the 1980s, Experian and Equifax purchased British credit reporting companies and set about transforming the industry. Along with the British Callcredit, they now dominate credit reporting in Britain—an industry whose practices are increasingly indistinguishable from those of its U.S. counterparts.

These mega-agencies draw personal data from virtually the same array of sources basic to the American and Canadian industries, including public records and past and current credit accounts. British credit reporters also rely on Electoral Registers—listings of addresses of persons eligible to vote, compiled and sold by local governments—to corroborate data provided by consumers on credit applications. Civil liberties groups have objected to these latter sales, on grounds that these personal data are collected under legal compulsion.

As in North America, reporting companies require their regular customers—that is, businesses purchasing their reports—to sign detailed reciprocity agreements, promising to feed back to the reporters the full details of their credit accounts. Again as in North America, access to the full, uncensored details of consumers' current accounts makes it possible to condense credit information into three-digit credit scores. Reporting companies sell these precise, instantly interpretable indices en masse.

Buyers of these informational products—both credit scores and more detailed, discursive credit reports—also parallel the North American profile. They include not only credit grantors, but employers, landlords, and banks (for screening out undesirable applicants for accounts). And as in North America, credit reporters have succeeded in selling their products to the insurance industry, opening a vast new market for the reporters. Thus British consumers also have the terms offered to them for insurance coverage shaped by their current and recent credit histories. British privacy policies seem to pose no obstacle to this use. Indeed, staff responsible for monitoring insurance activities at the UK Information Commissioner's Office seemed unaware of this use of credit information when I inquired about the matter in 2004.

As in Canada, British consumers must formally give their consent before being subjected to such surveillance. The fine print of a typical blanket consent statement required to open a bank account reads:

> Where considering your application and where appropriate from time to time during your relationship with us, we will make searches about you at credit reference agencies . . . and from the Electoral Register, for the purpose of verifying your identity. . . . We may use credit-scoring methods to assess applications and to verify your identity and we may also search the Electoral Register ourselves and carry out other identity checks. . . .
>
> Members of the HSBC Group may record, use, exchange, analyze and assess relevant information held about you and your relationships with the HSBC Group. This will include the nature of your transactions, for credit assessment, market research, insurance claim and underwriting purposes and in servicing your relationship with the HSBC Group. This may include any information provided by you or someone acting on your behalf which is relevant to your relationship with us.[19]

Granting such "consent" is a routine part of opening an account with British banks today. In addition, surveillance requirements intended to detect money laundering and other illegal activities make it all but impossible to open an account, no matter how law-abiding the applicant, without providing data on one's salary, employment history, marital status, and other matters.

These practices flourish largely unhindered by privacy regulations or regulators. Unlike Canada, the other outpost of U.S.-style "positive" credit reporting, Britain is part of the European Union and hence theoretically subject to the relatively strong provisions of its 1995 Privacy Directive. Other EU countries interpret that directive to forbid "secondary release" of data from credit accounts. In these countries retailers, credit card companies, banks, and others are unable legally to share account data with credit reporters or other interested parties, except at the initiative of the account holder. But in Britain, as in Canada, the consumer's signature on the blanket authorization required of applicants for credit and bank accounts is understood to constitute consent. Refusal to provide such consent is of course always possible, but results are predictable. Most Britons would probably not consider the resulting life without a bank account or credit to represent a realistic alternative.

British *direct marketers* also collect personal data from much the same sources as their American counterparts—which is to say, from virtually any records conveying hints of consumer susceptibilities. As in the credit industry, the UK marketing industry relies on the lists of eligible voters provided by local governments, triangulating them with economic and demographic information on neighborhoods where consumers reside. This symbiosis makes it possible for marketers to deliver to retailers "made to order" appeals to customers with just the consumption habits and spending capabilities desired by the businesses concerned.

But direct marketing privacy codes are stronger in Britain than in the United States or Canada. As in Canada, British consumers have the right to opt out of direct marketing databases by indicating that preference at the point where personal data are collected. The industry also maintains a national Do Not Call list for those seeking to avoid marketing appeals by phone; makers of such calls are required to identify themselves and provide contact information if the recipient of the call requests it. And British privacy law grants consumers the right to have their names stricken from direct advertising lists—an option that U.S. law does not afford. There are no such opt-out possibilities in Britain for credit or insurance data.

As in consumer credit, British *insurance surveillance* relies on sweeping consent statements on applications to clear the way for inquiries into the lives of insurance applicants. The industry has spawned three separate systems for exchanging records of homeowners', auto, and personal injury insurance claims among prospective insurers. These systems are managed by two data processing companies, CRIF and Experian (the American credit reporting giant), ensuring that past claims are taken into consideration by insurers when British consumers seek new coverage. In contrast to the United States, British government agencies do not provide data on drivers and accidents directly to insurers.

Applicants for life insurance are expected to consent to inquiries of their own physicians, as well as to examination from independent doctors. As in North America, the British insurance industry ensures that results of medical examinations leading to declined coverage attain the surveillance equivalent of eternal life. Information revealed in such examinations is forwarded to the industry's "Impaired Lives Register" (formerly, the "Damaged Lives Register"), to prevent applicants from withholding it in subsequent insurance applications.

France: State Limits to Commerce in Personal Data

In the early 1990s the CNIL, France's national privacy protection agency, received an intriguing complaint from a bank employee, a student doing a stint of summer work. The bank, where the student was also a depositor, was using personal information from its files to bracket its patrons into a handful of categories—not all of them flattering. Among the names the bank gave these customer groups were "big spenders but over their heads," "malcontents," and "not likely to improve over time." Perhaps the fact that the employee found himself classified in the last group had some role in his bringing the complaint.[20]

The reasons for these Cartesian efforts at classification were not capricious. The characterizations were supposed to guide bank staff in their efforts to cultivate (or avoid) new business with the designated customers. Some classifications—for example, "modernists"—were meant to give a green light to marketing overtures. But the complainant held that these uses of account data and other personal information available to the banks represented an infraction of France's 1978 privacy law.

The CNIL took the complaint very seriously—and ultimately issued some Solomon-like directions. Customers did indeed have a legitimate interest in knowing how banks were using their personal information, the watchdog body concluded. At the same time, banks should not be forbidden to use such data to classify their customers, even if the classifications did not meet with the latter's satisfaction. *However,* any such classification scheme had to be openly acknowledged to customers, who should be able to determine to what category they had been allocated. Though the record does not show it, one suspects that this requirement had the effect of dissuading banks' recourse to classification schemes—or at least causing them to choose less vivid names for the categories.

The CNIL also went on to introduce some more far-reaching constraints on banks' use of personal data available to them. Not all such data should be considered available for banks' use, it held: "This means particularly that information that might be deduced as to the parties to a customer's transactions are not subject to exploitation, nor are any sensitive personal data (political or religious convictions, labor union sympathies, or ethnic or moral identifications) whose collection is specifically protected in the 'information and liberty' law [of 1978]."[21] It is difficult to imagine a privacy protection

agency in Australia, Canada, or the UK taking such a strong and thoughtful position limiting what many bankers in these countries would no doubt consider "their" information.

Privacy protection in France strikes a sharp contrast to the American-Canadian-British model. Even more than in Australia, markets in personal data are subjected to state control and supervision—where they are not proscribed outright. Like Britain a member of the EU, France has taken the strictures of the union's 1995 Privacy Directive more seriously than its liberal-minded neighbor across the Channel. Much of the muscle constraining the free flow of personal data emanates from France's Commission Nationale de l'Informatique et des Libertés ("the CNIL"), created in 1978, one of Europe's oldest national privacy commissions.

France has no private *consumer credit reporting* industry. Details of consumers' financial accounts—bank balances, account histories with credit grantors, details of lawsuits and bankruptcies, salary information, and the like—may not, under the law, be furnished to third parties without permission from the individual. French law, moreover, does not recognize blanket "consent," like the one quoted above from the UK, as authorizing the sweeping exchanges of personal data on seekers of bank accounts, credit relationships, or insurance.

One result is that French consumers seeking new accounts with banks, loan companies, or retailers retain significant control over provision of their data to these institutions. To evaluate an application, the institution must rely almost entirely on personal information supplied by the applicant. Depending on what the consumer is applying for, he or she may be asked to present pay stubs, rent records, or receipts from other credit accounts as supporting documents. What credit grantors cannot normally access is any information on recent or current accounts—or for that matter, on any unpaid debts, legal entanglements, or other personal information—that the applicant does not choose to disclose.

The system thus normally provides no easy means for prospective creditors to spot applicants already overloaded with credit obligations—to the extent that more debt would be difficult to sustain. In short, "positive credit reporting" in the American mode is impossible. As a result, of course, "credit scores" marketed with such success in the United States, Canada, and the UK cannot be formulated for French consumers. The comprehensive account information providing bases for such scores is not compiled in any one place, and there are no credit reporting agencies to sell the scores.

The French system does embody one centralized check on consumers who fail to fulfill credit obligations. This is the FICP (Fichier des Incidents de Credit aux Particuliers), maintained by the Banque de France—a comprehensive list of those consumers legally delinquent in consumer credit obligations. Creditors are legally required to report their delinquent accounts to the FICP and likewise required to consult this list in considering new credit applications. The law requires prompt removal of names from the list, once credit defaults are rectified. Lenders extending credit to consumers already listed with the FICP have limited legal recourse to recovering their losses if the consumer declares inability to pay. The contrast to draconian U.S. personal bankruptcy law, recently tightened at the behest of the credit industry, is breathtaking.

French consumers thus accumulate nothing that could be called a "credit record," so long as no accounts are formally delinquent. The situation is even more extreme than in Australia, where the credit reporting industry also has little to report on consumers who avoid delinquencies. Australia's significant privacy restrictions do permit reporting agencies to report recent *inquiries* from businesses about a consumer's standing—thus enabling credit grantors to identify those shopping for a lot of credit within a short time. Of course, French consumers have the option of reporting other credit applications or existing relationships to prospective new creditors, and French credit grantors may likewise verify these reports directly with the businesses thus identified. But unless and until accounts become delinquent, there is no central compilation of such data.

Yet like Australia, France remains a vigorous consumer society. Home mortgages, personal and auto loans, credit accounts with retailers all play a conspicuous role in French life. Credit cards mostly do not, their place being taken by debit cards that permit a one-month delay in payment of full amounts owed. These cards obviously keep creditors on a shorter financial leash than U.S. credit cards and accordingly pose fewer risks for the banks issuing them. But all in all, one sees little obvious evidence that restricted markets for personal credit information have blocked access to the creature comforts beloved by French consumers.

Uses of personal information in the French *insurance* industry are also far less aggressive than in the United States. Just as it lacks a consumer credit reporting industry, France has no private companies like America's Acxiom or ChoicePoint to generate and sell personal data to insurers. Their activities

would certainly be illegal under French privacy law. France's insurance industry does, however, maintain its own exchanges of data that pool claims experience in property and casualty insurance—making it difficult or expensive for consumers to obtain insurance where there have been repeated losses in the past. AGIRA (for auto and driver insurance) and ALF (for other property and casualty insurance) serve as directories for companies considering applications for coverage. These repositories of claims-related information appear to operate nearly as much on a hair trigger as their American counterparts—in that even policyholders' *inquiries* above coverage can lead to raised rates for such things as auto insurance. These systems effectively direct inquiries by any insurer on prospective customers to companies reporting past business with the same person. But under the eye of the CNIL, there appears to be no way in which data from other systems—credit, criminal records, lawsuits, or the like—can enter into insurance decision making, as it does in other countries.

In the sale of life insurance, France is also more resistant to pressures on privacy. Obviously French insurers exert themselves to avoid selling coverage to those at high risk, requiring medical examinations for large policies. But the CNIL, France's national privacy protection agency, has resisted the pooling of such data across insurance companies of the sort accomplished by the MIB in North America. Instead, it has fostered a system of life insurance screening by which physicians carrying out life insurance examinations report only degrees of elevated risk they discover—without reporting the reasons for such risk. Under the CNIL's rules, these reports may not be shared beyond the insurance company that seeks them in the first place. The contrast to the American system, where information on the nature and extent of risks to longevity are retained indefinitely, is conspicuous.

French state agencies, as elsewhere, forward risk-related personal information to insurance companies. The Ministry of Transport maintains records of driving infractions and accidents, and furnishes reports on these matters to insurers—though without a fee. Another government source of information is the Ministry of Transport's database derived from "gray cards," attesting to the legal registration of vehicles. These data include the year and make of the registered vehicle and the owner's name and address; accordingly, they are attractive bases for marketing efforts. But unlike similar public record sources in other countries, the individual retains the right to opt out of such disclosure.

In the conversion of personal data for *direct marketing,* France offers far more significant privacy safeguards than does the United States. Direct

marketing—mailings and other communications targeted to consumers by name and situation—does occur. But French interpretation of the EU Privacy Directive forbids unauthorized "secondary release" of personal data. Personal data provided for any of the whole range of commercial purposes—credit accounts, banking, magazine subscriptions, product registrations, or the like—requires express consent from the individual before it can be shared. Indiscriminate "harvesting" of personal data from website visits, inquiries to product hotlines, purchases of mail-order houses, and the like is hence out of the question—except insofar as consumers "opt in" to indicate acceptance of such uses.

French direct marketing companies accordingly rely on inducements to consumers to provide data on themselves, and the requests for information are clearly earmarked as forming the basis for marketing appeals. Such companies commonly disseminate questionnaires—as do American direct marketers—asking consumers to provide data on themselves in exchange for promises of free samples of various products or services. Other data for the repositories maintained by these companies come from direct communications between retailers and consumers, where the latter have checked the boxes indicating an opt-in to marketing use of their data. French privacy law grants all consumers the option of having their names stricken from any marketing list.

The result of these strictures is a privacy regime surrounding one's consumption life strikingly different from that familiar to Americans. Unlike Americans, French consumers do not find themselves targeted for personalized appeals for everything from home improvements to treatments for diseases they would prefer not to discuss. To be sure, all sorts of *indiscriminate* advertising still flow—usually stuffed into one's mail box by private delivery services, with or without the householder's consent. But unsolicited appeals predicated on personal details originally furnished for other purposes are illegal without consent from the person concerned.

Surveillance in Motion

Pressures to sell and trade personal data are evidently universal in the world's prosperous market societies. Nevertheless, these pressures have not all run their course quite in the same way in all countries—at least, not yet.

By nearly any standard, the United States leads the way in market-driven flow of personal data. Canada and the UK show the effects of the export of American business models in allowing many of the same practices; yet even these countries impose some constraints on the marketing of personal information. And France and Australia, to varying degrees and in different ways, impose still more significant constraints.

What are we to make of these differences? One conclusion would be that market pressures on privacy are not destiny. Privacy measures *work*—at least where conscientiously conceived and applied with political will. Perhaps some enduring characteristics of French *etatiste* traditions or Australian populist values, for example, provide durable counterweights to commercial erosion of privacy.

But remember that the sketches of prevailing practice given above are snapshots in time. What prospects do these arrangements have to endure, we need to ask? Could it be that resistance to unlimited marketing of personal data has simply fared best in those environments where countervailing pressures are least developed? Could it be—in the worst-case interpretation for privacy-watchers—that all the world's consumer societies are in fact on a kind of conveyor belt, leading ultimately to a destination today most fully attained by the United States?

Imagine a world where market principles reigned absolutely supreme—with any and all personal data available for sale to the highest bidder. That would surely spell enhanced profitability for businesses in all sorts of discriminating dealings with the public. Or at least, for *most* businesses. In any such sweeping change, there would paradoxically be some businesses that lose—those that start with superior access to personal data.

Consider consumer credit. Here as elsewhere, businesses vie with one another for the "best" personal information—and hence, the ability to deal with the most profitable customers on the most profitable terms. The absence of comprehensive, "positive" credit reporting, we have seen, renders much of the choicest information less accessible to would-be credit grantors. Without it retailers, credit card companies, and other credit providers can only obtain personal information directly from consumers themselves, much as these companies would prefer direct access to uncensored data. Under these circumstances, nearly all credit grantors share a certain burden of ignorance.

But not *quite* all. Even in the absence of credit reporting, some organizations enjoy something close to a comprehensive view of consumers' financial affairs. I am speaking of *banks.* Systematic scrutiny of consumers' banking records reveals almost as much as the details of their credit reports—including amount and sources of income, consumption habits, credit accounts in use, extent of monthly obligations, and (at least by inference) promptness in meeting those obligations. These data tell banks virtually all that they might want to know about any consumer's desirability as a credit customer.

Banks were traditionally ultra-discreet regarding the sharing of such information—as my British civil servant informants emphasized to me in the early 1970s. That discretion, whatever its spiritual rewards to bankers, yielded significant financial payoffs. For by refusing to disclose customer data to other would-be credit grantors, banks could pick and choose the most reliable risks among their own account holders for their own credit offerings. So long as consumers continued to turn to "their own" banks as the preferred source of credit, banks supporting the privacy of their customers' data could do well by doing good—leaving less desirable consumers to seek credit from "second-tier" lenders at less desirable terms. For banks, this closed world of consumer finance represented an informational Garden of Eden.

Could this idyllic environment harbor the equivalent of a Serpent? It does—in the form of competition. Should consumers begin to shop around for credit opportunities, banks' "best" customers might go elsewhere. Banks would then have to better their terms of credit, in hopes of retaining their own customers and attracting others. But in this case, they would find themselves in the same position as any other credit grantor—that is, in ignorance of the full financial situations of credit applicants, simply because many of their credit applicants would have credit histories about which the banks would have no direct knowledge. Facing such ignorance, banks would have to consider recourse to some form of credit reporting. And that would mean sharing their customer data with the agencies providing credit reports—something that every credit reporting agency insists upon.

Banks of course resist sharing customers' data with credit reporting agencies, for the same reasons that retailers resist sharing such data. Nearly all commercial users of personal data would prefer to withhold their own customer data from potential competitors, while maximizing their access to such data from others. In credit granting, such an arrangement would make it possible to encourage bad customers to take their business elsewhere (thereby

undermining competitors' profits), while "cherry picking" the best customers from one's own and others' past accounts for further business.

When I first learned that Australia and France had consumer credit reporting systems that functioned without monitoring "good" credit accounts, I was impressed with the apparent strength of privacy values in these countries. This reaction now seems premature, if not naïve. In both countries the politically potent banking industry currently favors the status quo as a way of avoiding competition for the most sought-after credit customers. But major pressures are building in both countries to broaden credit surveillance. In both, banking lobbies could well change their relatively privacy-friendly positions, if faced by serious competition. Should they apply their political muscle in favor of "positive" reporting, legislation to implement it could follow quickly.

Something like this seems to have occurred in Britain during the 1980s, though no legislative changes were involved. Banks defended their habits of relative discretion until the challenge of competing for credit customers made it necessary to seek outside sources of data. When British banks began aggressively marketing credit cards, personal loans, mortgages, and other credit products to consumers other than their own long-standing customers, they had no choice but to sign agreements to provide data from their accounts to reporting agencies in turn. Today personal data held by banks are apt to be disseminated not only to credit grantors, but also, via credit reporting companies, to insurers and employers.

In Australia, at the time of this writing, the banking industry has not endorsed a shift to "positive" reporting. But other business interests are actively lobbying to alter that country's relatively privacy-friendly credit reporting system in the direction of the U.S. model. The Australian Finance Conference (AFC), a trade association of credit-granting businesses, has been leading these efforts—in opposition to the efforts of Australian consumer activists. AFC officials to whom I spoke in September 2003 seemed optimistic that the banking industry would eventually rally to their cause.

In France, pressures for change in this direction are also afoot. Should that country adopt a system of positive reporting any time soon, that system would hardly resemble the North American model. More likely, any change would simply involve expansion of the file maintained by the Banque de France to include listings of all current credit accounts—without necessarily citing the amounts of indebtedness or other data coveted by British and American credit reporters. There would be no commercial incentive to extend the scope

of reporting, and no basis for anything like credit scores. The state would remain in charge of consumers' "private" information but would do so in a way preventing consumers from concealing extensive indebtedness. Such a system, if adopted, would still leave France one of the more privacy-friendly countries of western Europe in terms of the sharing of consumers' credit information.

Yet even in France, resistance to marketing consumer credit information is not entirely what it seems. For exchanges of personal credit data *within* corporate entities in France are replicating some of the patterns of credit reporting found in other countries. A handful of corporate conglomerates owned by banks and other big financial interests also control lending companies providing credit to middle- and low-income consumers—amassing in the process databases comparable in scope to those maintained elsewhere by independent credit reporting companies. Some observers believe that sharing of personal information occurs between the parent companies and conglomerates—granting the latter a significant additional advantage in their efforts to discriminate among credit-seekers. Such sharing is not acknowledged and is probably not legal under French privacy regulations. But at the very least, the combining of account information across a variety of credit grantors under the same ownership does create patterns that begin to replicate "positive reporting" as practiced in the United States, Canada, and the UK.

In short, if Australian and French banks make common cause with the already potent lobbies in those countries for "positive" credit reporting, the resulting pressures could prove overwhelming. Indeed, government policymakers may also find advantages in the marketing of consumer account data—as a spur to consumer spending, supposedly boosting economic growth. Should the idea take hold that broadening access to consumers' account information promises both profits for the financial sector and growth for the entire economy, privacy values will face a severe test.

Safe Harbor

For a revealing look at privacy principles in collision with concentrated economic clout, consider the trans-Atlantic power struggle culminating in Safe Harbor. That is the name given to agreements struck between the

European Union and the United States in 2000, narrowly averting a trade war over privacy. At issue was something most Americans would scarcely have considered a hot-button issue—the export of personal data from Europe to the United States.

In fact, many American corporations and other organizations did and do collect personal data on Europeans, data then transmitted to the United States for storage and processing. Users include credit card operations doing business with European consumers, multinational companies with European employees, and direct marketing companies targeting European consumers. The question was simple: when could such information legally be transmitted to the United States, and how could it be used here?

That question triggered tension between the significant strictures in the European Community Privacy Directive of 1995 and the virtually non-existent protections under U.S. law. That directive is Europe's master privacy legislation, now incorporated into the law of each member country. It stipulates that "Member states shall provide that the transfer to a third country of personal data . . . may take place only if . . . the third country in question ensures an adequate level of protection."[22]

This provision requires EU authorities to certify the "adequacy" of privacy protection in any country likely to be involved in commercial exchange of personal data gathered in Europe. As a result, many such countries set to work developing privacy codes that would permit unfettered commercial exchange of personal data with Europe. Even authoritarian Singapore, with an eye to lucrative opportunities for processing personal data from European companies, began developing a national privacy code that would pass European standards of "adequacy."

The United States was not one of these countries. Even at the time of the 1995 European legislation, America stood out for its lack of a comprehensive legislation regulating private-sector uses of personal data. Some specific forms of information were the subject of sector-specific laws—video rentals, for example, or (in later legislation) medical data. But the United States has never established broad rights and protections applying to all personal data held in the private sector, nor has it ever created anything like a national Privacy Commission. By the end of the 1990s, it became apparent that the business-friendly Clinton administration had no intention of taking steps to make its privacy legislation "adequate" by European standards. Someone had clearly calculated that American economic power would

suffice to protect American business from interference from across the Atlantic.

The obvious consequence of such a stance, under the letter of the EC Directive, was to block flow of personal information collected in Europe to the United States. Thus, for example, personal data collected by American banks on European customers or prospects would have to remain in Europe. But Clinton administration officials threatened that any such action would trigger economic retaliation from the American side.

In the end, Europe blinked. Over objections of the European Parliament, the European Commission acquiesced to a "compromise" that met American requirements in virtually every respect. Dubbed "Safe Harbor"—a name nearly as fulsome as "positive credit reporting"—the agreement freed the United States from any obligation to adopt a national privacy code embodying European standards of "adequate" protections. Instead, the agreement permitted transfer of personal data to individual American *companies* that promised to maintain acceptable safeguards.

The capitulation was nearly complete. "Safe Harbor" permits American corporations themselves to certify the practices that they follow regarding personal information—a version of the "self-regulation" of business practices widely fostered by the Clinton administration. It provides no system for checking the application of these assurances, nor any mechanism for individuals depicted in files to challenge treatment of "their" data. It has no provision governing what further uses might be made of such information if transferred in turn to other organizations. In short, it embodies a quantum step down from the protections envisaged in the European Privacy Directive.

Perhaps because of its very lack of teeth, Safe Harbor is today regarded as tantamount to a dead letter. Most organizations importing personal data into the United States at the time of this writing appear simply to disregard the measure. One consultant who advises corporate clients on privacy issues told me that he recommends that they do exactly this—on the assumption that enforcement is so lax that noncompliance is unlikely to bring any sanctions.

For anyone concerned about the strength of privacy values in confrontation with commercial pressures, this is not a heartening story. No one could consider the principles embodied in the European Privacy Directive radical.

Embodying the consensus fair information practices noted in part I, they were intended to be utterly compatible with the workings of markets and businesses. But in a face-off with American economic power, Europe's commitment even to these basic principles came off second best. It appears that no one wanted to be held responsible if European jobs or other economic activity were jeopardized by a trade war with the Americans.

Some Rare Privacy Victories

Frontal collisions between avowed privacy principles and the entrenched practices of organizations rarely produce outcomes heartening to privacy-watchers. Examples go back to the earliest efforts to frame legislation and policy for privacy protection. America's Fair Credit Reporting Act was framed so as to ratify standard industry practices in marketing personal data in credit, insurance, and employment. That law makes credit reporting practices more accessible to consumers and opens the possibility of their challenging inaccurate or inappropriate data. But it does not enable consumers simply to decline to have records about themselves compiled and sold by the system. The Privacy Act of 1974 enunciated principles that could have stopped unauthorized sharing of data among government agencies, but those provisions were almost immediately neutralized in practice.

Similarly, Canada's PIPEDA would appear to grant consumers significant control over collection and use of credit and direct marketing data. But there, too, established industry practice has largely prevailed over the explicit precepts of the law. Much the same observation might be made about credit reporting in the UK. The language of the European Directive would seem to guarantee British consumers the right not to be subjected to credit reporting, if they preferred. But confronted by a flourishing industry predicated on total access to all consumers' accounts, UK authorities have paid little attention to this implication of the law. One could extend this list at length.

Against these downbeat trends, privacy-watchers can point to a few straws blown by winds in a different direction. Even in the United States, public sentiment sometimes bucks the interests of organizations and instead asserts privacy interests. Some of the most fascinating of these involve voter resistance to efforts of banks to funnel customers' account data to corporate allies blandly identified as "affiliates." These are insurance companies, brokerage

services, and other businesses that would dearly love to target choice prospects identified as such through their bank records.

One such story comes from North Dakota. That state had long had a law prohibiting banks from exchanging customer data for commercial purposes—for example, to credit reporting agencies—unless the customer explicitly requested otherwise. In 2001, the state legislature watered down that relatively strong protection, changing it to an "opt-out" procedure. Under this change, banks would not be required to withhold customer data unless the latter specifically requested them to do so.

To widespread astonishment, that action by the state's elected representatives triggered a voter revolt, via a special election to reinstate the more privacy-friendly opt-in rule. Sensing a key interest at stake, banking industry lobbyists from across the country poured money into North Dakota in efforts to squash the measure, outspending the privacy campaigners by a ratio of six to one. Yet some 100,000 North Dakotans came out to vote, overwhelmingly upholding the right to privacy over their bank data.

The intensity of industry efforts in a sparsely populated state not known for setting national policy trends was striking—as were the populist instincts of its mostly rural voters. Imagine, then, the fight a few years later in California, where activists had long sought to establish meaningful controls for consumers over dissemination of their bank records. Here, too, the issue in 2003 was a grassroots effort to ban sharing of account information among corporate "affiliates" without permission from account holders.

In California, business interests had long and effectively opposed efforts to rein in such unauthorized exchange of personal data. Governor Gray Davis fought efforts to bring the matter to a vote, and the state legislature did not act until supporters started collecting signatures for a ballot initiative similar to the one in North Dakota. The California bill that emerged was ultimately weaker than North Dakota's, in that it required consumers to "opt out" of data sharing, rather than to "opt in" if they wished to permit it. When it finally came to a vote, the bill passed overwhelmingly in both House and Senate, and the reluctant governor signed it into law.

But the industry counter-attacked at the federal level. Under a blitz of lobbying, Congress passed revisions to the Fair Credit Reporting Act "preempting" states from adopting privacy laws more stringent than those in the federal act. Industry spokespeople preached far and wide that allowing states to enact laws like California's affording more serious privacy protection than

elsewhere would create a "patchwork" of disparate and costly practices for the credit industry. Despite spirited campaigning by consumer groups and state attorneys general, the preemption passed Congress and was signed by President Bush in December 2003. California's noble experiment in enabling consumers to "just say no" to unauthorized dissemination of their account information had run up against a brick wall of financial industry clout.

Conclusion

These episodes demonstrate that citizens can and do opt for greater control over their information when confronted with clear alternatives. It made no sense to voters in California and North Dakota that banks should release details of their financial lives for marketing purposes without consent. In this respect, one can view these grassroots affirmations of privacy values as *conservative* steps—measures to maintain a more privacy-friendly status quo, rather than attempts to carve out new realms of privacy protection where there had been none before.

Again, such successful stands are rare. And still rarer are instances in which major surveillance systems, either in government or the private sector, have actually been *dismantled* in response to privacy concerns—once firmly instated and operating. Surveillance systems are expensive to create; once created, they generate both results and constituencies that make them difficult to eradicate.

But something tantamount to such a reversal has occurred even in the United States with regard to some forms of direct marketing. Laws governing *collection* of personal data for marketing purposes are less restrictive in this country than in Canada, Australia, Britain, or France. EU regulations forbid the unauthorized mass "harvesting" of personal data from website visits, subscription lists, and credit accounts that are pervasive and largely uncontrolled in the United States. Yet in the face of considerable public indignation, the American direct marketing industry has had to accept significant curtailment, not of the collection and exchange of such data, but of some of its *uses*—above all, unwanted telephone appeals. These widely despised invasions of privacy have now been significantly cut back, though not eliminated, by the 2003 federal Do Not Call listing.

Why have privacy concerns led to significant restrictions of junk phone calls, in such contrast to the broad expansion of surveillance in credit

reporting and insurance? Why have politicians been obliged to clamp down on this one particular lucrative, privacy-eroding practice and not others?

The reason probably lies in the *unilateral* quality of marketing appeals. Credit and insurance both involve relationships in which consumers actively seek some benefit. But the processes involved in generating credit privileges or insurance represents, as privacy-watchers often put it, a "black box" for most consumers. One can understand that certain personal data flow into the process, and decisions—in the form of credit privileges or insurance coverage—flow out. But details of how information actually enters into allocations are anything but transparent to most observers. This obscurity makes it easy for the users of data to proclaim their "needs" for unlimited personal data, in order to provide the outcomes consumers seek.

But few if any consumers actually seek the attentions of direct marketers. People are accordingly much more likely to view such activities as pure impositions. Under these circumstances, opposition to the privacy invasions embodied in direct marketing is easily focused.

Obviously notions that the *demands* of organizations for personal information correspond to inflexible *needs*—and that satisfaction of such needs is indispensable for provision of products and services essential to normal life—do not bode well for privacy values. We need to take a closer look at these ideas.

Part IV ■ ■ ■ ■ ■

The Future of Privacy

Christopher Robin lived at the very top of the Forest. It rained, and it rained, and it rained, but the water couldn't come up to *his* house. . . . Every morning he went out with his umbrella and put a stick in the place where the water came up to, and every next morning he went out and couldn't see his stick any more, so he put another stick in the place where the water came up to, and then he walked home, again, and each morning he had a shorter way to walk than he had had the morning before. On the morning of the fifth day he saw the water all round him, and knew that for the first time in his life he was on a real island.

—*Winnie the Pooh*

For many of us, the erosion of privacy forms a disconcerting background hum to everyday life. But for a few, it is a never-ending cacophony. These few are the full-time activists staffing organizations devoted to defending privacy.

In the United States, these high-energy, low-budget organizations include the Electronic Frontier Foundation in San Francisco; the Privacy Rights Clearinghouse in San Diego; and the Center for Democracy and Technology and the Electronic Privacy Information Center in Washington, D.C. In London, they include Privacy International and Statewatch. In Paris, IRIS (Imaginons un Reseau Internet Solidaire); in Quebec, Option Consommateurs; in Seoul, Citizens' Action Network; in Sydney, the Australia

Privacy Foundation. And besides these hard-striving nongovernmental activists, many dedicated full-time privacy specialists labor in government privacy-protection agencies—the CNIL (National Commission on Information Processing and Liberties) in Paris, for example, or Hungary's Privacy and Freedom of Information Office. For these determined privacy-watchers, protecting people's rights in the use of their information is a never-ending obsession.

The role of these figures is above all *reactive.* They rush like overtaxed firefighters from one privacy conflagration to another. They speak out for workers whose employers troll company medical records and fire employees with potentially expensive diseases. They call press conferences to decry government attempts to impose identification card systems on unwilling populations. They testify before legislatures on the risks of tracking school children judged to have behavior problems. They issue press releases decrying schemes to archive DNA records of the general public. They lead the charge against companies discovered to have leaked consumers' confidential data to direct marketers or would-be identity thieves. They speak out when school systems want to subject pupils to intrusive body searches or electronic monitoring. And on and on.

For those involved, this work is endlessly bracing, engaging, and fascinating. Ever-emerging technological possibilities and the ingenuity of planners generate a steady stream of new ways of creating, capturing, and using personal data for one institutional purpose or another. And these innovations, planned or accomplished, pose one challenge after another to the privacy-protecting Davids, who mobilize thinly stretched resources against organizational Goliaths.

Off the record, privacy defenders confess to worries about the long-term prospects for their cause. The problem, they say, is not that their efforts may fail, though inevitably this is often true. Perhaps more disturbing is the fact that even the most notable victories often appear as provisional non-defeats—subject to rude reversal down the road. Airlines promise to guard the privacy of information on passengers, only to yield such data freely when government agencies demand it. Or corporations make similar promises about data collected on consumers via their websites, only to sell or trade such data to direct marketers or other corporations. Even hard-fought provisions of major privacy legislation, such as America's Privacy Act of 1974, often fall victim to interpretations in practice that gut key elements of their evident original intent.

Then there is the pervasive sense, widely shared among privacy-watchers, that public opinion is growing complaisant or even fatalistic concerning privacy invasion. True, many public opinion studies in the United States and abroad demonstrate high levels of public discomfort about the appropriation of personal information. When asked whether Washington is doing enough to protect personal information, Americans typically say that it should be doing more—at the rate of 68 percent, in one recent *New York Times* poll.[1] The trouble is, these attitudes do not necessarily translate into active demands for legislation or other concrete privacy measures. Given the chance in ballot box measures, American voters readily opt for more privacy. But they do not often seem to phone, fax, or write their elected representatives to demand more of it. Often one senses a perception of helplessness over declining control over one's personal information.

Worse, options for protecting one's own information in everyday life seem often to go unclaimed. In Ontario, privacy-watchers grew concerned about plans for an electronic toll-taking system for Highway 407—a privately run, state-of-the-art expressway. The system would have used electronic transponders to compile data on dates, times, and exact routes of individual users' travels, generating a database offering obvious potential for privacy abuse. In response, the office of Ontario's Privacy and Information Commissioner helped devise an elaborate plan to enable motorists to be billed without accumulating a computerized record of their travels. But from a pool of some six million transponder accounts, no more than twenty-one travelers ever invoked the privacy-friendly option—which admittedly required a bit of extra effort to exercise. That option has since been discontinued.[2]

Indeed, many people seem willing actively to surrender their own information, in hopes of gaining time or convenience. At the time of this writing, U.S. authorities are inviting air travelers to join the "Registered Traveler Program"—and pay a fee to have themselves subjected to advance background checks by private security firms, so that in the future they can be whisked past other travelers to departure gates. Much as citizens of democracies affirm desire for more privacy in general, they seem willing enough to yield bits of it in exchange for scraps of ease, freedom from harassment, or simple creature comforts.

The trouble is, attractive possibilities for such renunciation promise to grow without limit. Privacy advocates often find themselves baffled by these possibilities. They would consign themselves to political oblivion were they

categorically to oppose cell phone adoption, or convenient consumer credit, or any and all measures to track and combat terrorists. Yet no one could reasonably deny that these and many other familiar innovations abet the shift of more and more personal information to government and private institutions—and beyond individual control. Thus the reactive stance that privacy advocates find themselves assuming: they denounce "abuses" of surveillance, but they find it hard to oppose seemingly moderate increments of it. Facing one innovative new use of personal data after another, privacy forces urge application of fair information practices to new data systems while decrying those innovations that ultimately "go too far."

But how far is *too* far? The community of privacy-watchers has formulated no succinct response to this slippery question. They can readily address flamboyant "horror stories"—cases where personal data are appropriated and used in ways that clearly serve the interests neither of the individuals nor of the institutions involved. It is easy to mobilize public opinion against companies that allow consumers' account information to be captured by thieves or hackers. Nor does anyone have trouble deploring government investigators' reliance on reports from private reporting companies that draw from blatantly inaccurate sources. But what about uses of highly personal data that are evidently intrusive, yet appear to serve purposes widely held legitimate and necessary—the tracking of cell phone communications, or the allocation of "correct" amounts of credit, or the identification of income tax evaders or potential terrorists? Here privacy advocates often do not have their speeches prepared—or if they do, they may find that they are not reading from the same page.

Again, many people seem to identify the point at which routine claims on personal information cross the line into intolerable privacy invasion in much the same way most people classify pornography: they know it when they see it. But as with pornography, reasonable people often disagree on where to draw the line. One man's shameless exploitation of sex for profit may turn out to be the next woman's harmless erotica, or even serious art or literature for a third consumer.

Clearly any judgments on where and how to draw a line against the endless, incremental erosion of privacy requires that most elusive vision—a view of the whole. What is the ultimate trajectory of developments like those discussed in parts II and III? At what point do these trends present an opportunity for

privacy defenders to draw a line against unlimited erosion of their cherished value? What are the implications of simply succumbing to them? How far do we have to go before we reach that point by default?

Christopher Robin could measure the rising tide around his home at the top of the forest by the narrowing distance from his front door to the stick that marked high water. Privacy-watchers have no such simple criterion. But few would dispute that the island of personal information remaining under our own control is shrinking.

Privacy Protection: The Official Response

To be sure, four decades of agonizing over privacy as a public issue have yielded a well-elaborated official response to public anxieties on the subject. Recall the consensus fair information practices summarized in part I. These precepts enjoin openness about the existence of personal data systems; accurate and lawful practices in the use of such systems; opportunities for individuals to know and challenge the contents of records on themselves; and restriction of the use of data to purposes for which it was originally collected. Variation across nations notwithstanding, these ideas are globally recognized as basic premises of privacy protection.

The problem with these principles is not that they are bad ideas in themselves. It is that they skirt the most crucial, and excruciating, questions. For one thing, they do not specify when surveillance systems deserve to exist in the first place—or when subjection to them should be required, for those who would prefer anonymity. The principles seek to make personal record-keeping processes open, predictable, and governed by rights and responsibilities on both sides. They define success as ensuring that the journey to intensified surveillance proceeds according to "rules of the road" that most people could recognize as fair and open. But they offer no guidance on whether we should want to make the trip in the first place.

Moreover, rules like these are rarely held to apply at all in many crucial settings—notably investigative agencies of the state and their private-sector allies. Police, security services, espionage agencies, tax authorities, and similar bodies rarely allow that their surveillance activities should be open, transparent, and subject to challenge by those concerned. Private-sector reporting agencies like the American companies that write "background reports" on

a no-questions-asked basis for those willing to pay for them are nearly as secretive. The reasons are clear: due process gets in the way of effective intelligence. Targets of investigation are apt to change their conduct or cover their tracks if they realize that they are being monitored. Requiring permission from individuals before their data can flow between surveillance institutions can only interfere with the efficiency of operations.

Records, Computers and Rights of Citizens, the early and influential U.S. government report, set a far-reaching pattern, making a delicate distinction between "administrative" and "intelligence" records. "Intelligence records," it states, "are seldom deliberately made public, except as evidence in legal proceedings."[3]

The statement is true as far as it goes. And clearly there is a rationale for keeping secret some monitoring activities, by some investigative agencies, under some circumstances. But the fact that personal data are compiled by "investigators" should hardly short-circuit questions of what domains of life should be subject to such "investigation." The consensus principles offer no guidance on such crucial questions.

The rhetorical flourish surrounding fair information practices often vaguely implies a mythical unity between surveillance interests and those of privacy. Due process guarantees, we are assured, are actually good for all concerned. They build public confidence in the systems involved. Without reassurance that their data will be properly treated, people will drag their feet—refusing to yield their data or otherwise resisting the orderly extension of surveillance. And if such privacy guarantees are not coordinated across jurisdictions, the "free flow" of personal information will be impeded—and with it, the engines of economic growth and state security.

The preamble to the European Community's Privacy Directive of 1995—one of the most influential global privacy doctrines—could hardly be clearer in these respects:

> Whereas the establishment and functioning of an internal market in which . . . the free movements of goods, persons, services and capital is ensured require . . . that personal data should be able to flow freely from one Member State to another. . . .
>
> . . . whereas the national authorities in the various Member States are being called upon by virtue of Community law to collaborate and exchange personal data so as to be able to perform their

duties or carry out tasks on behalf of an authority in another Member State within the context of the area without internal frontiers as constituted by the internal market. . . .

Whereas the difference in levels of protection of the rights and freedoms of individuals, notably the right to privacy, with regard to the processing of personal data afforded in the Member States may prevent the transmission of such data . . . whereas this difference may therefore constitute an obstacle to the pursuit of a number of economic activities . . . distort competition and impede authorities in the discharge of their responsibilities . . .[4]

And on and on. . . .

From Brussels to Hong Kong to Ottawa, this soothing message of privacy-protection-as-grease-for-the-wheels-of-administration-and-commerce marks the selling of official privacy protection schemes. The political appeal is self-evident. Presenting any innovation as a win-win proposition for all concerned may well paper over unresolved conflicts and maximize support in the short run. But such language should hardly distract us from the truly historic questions: How much of our lives will ultimately be subjected to mass surveillance?, and, What options have we for limiting such coverage?

Let us be frank. Surveillance proceeds most efficiently when personal information flows frictionlessly from one institution to another, without the possibility of alteration or resistance from those depicted. Surveillance systems profit by active involvement from persons under scrutiny only where it encourages correction of erroneous data—and certain levels of inaccuracy may be a small price to pay, in the interest of keeping the targets of monitoring out of the loop. As more actionable data become available from more varied sources, it becomes increasingly feasible and attractive to avoid direct dealings with the people being monitored altogether. For surveillance interests, the ideal is a seamless and efficient interlocking collection and sharing of personal data. But obviously this logic spells disaster for privacy.

In this light, the resilience of privacy-and-efficiency-too promises is disconcerting. The tone was set early on. "A free society should not have to choose between more rational use of authority and personal privacy," wrote Alan Westin in 1971.[5]

This could be the worst idea to afflict privacy thinking throughout its short history. Westin, to be sure, has also been the source of many of the best

ideas on the subject. But avoiding underlying conflicts between institutional efficiency and individual control over personal data fosters distraction from the issues that matter most. Much better to start with candor: by assembling more personal information from more different sources—and with less and less interference from the people concerned—institutions of all sorts do better in framing their dealings with those individuals. But such efficiencies are purchased in the coin of privacy. No one—I hope—openly prefers that either value triumph at the expense of the other for any and all purposes. But the crucial question is, where are concerns over privacy serious enough to warrant renouncing the quest for efficiency that is driving its destruction?

Privacy Codes: A Balance Sheet

It would be wrong to paint the repercussions of official privacy protection efforts only in shades of gray. I have tried to show how privacy codes have had markedly varying results across time, across countries, and across different domains of record-keeping. They have accomplished some things far better than others, and they have worked better in some settings than elsewhere.

One *broadly positive role* of privacy legislation has been to encourage *openness and due process* in processes that would otherwise be baffling to those subjected to them. Nearly every privacy law mandates some rights for data subjects to access their files—and usually to challenge the accuracy and uses of filed information. These measures bring untold benefits simply in de-mystifying surveillance processes and in stopping them from going too far wrong. Like the "green" codes requiring environmental impact statements, they represent some check against malfeasance and abuse of power by record-keepers. And they provide bases for public scrutiny and debate on the practices involved.

The limits of these virtues are also apparent. For one thing, ease of access to and correction of data held in file is very uneven. The strongest codes enable data subjects simply to remove their records from surveillance systems altogether—as in those countries permitting people to have their names removed from direct marketing lists. At the other extreme are laws that place the burden on individuals to discover the contents of their own files and then appeal to the discretion of data-keepers to correct the record. American credit reporting laws, for example, permit consumers to file brief statements to dispute contents of their credit records—statements that must be transmitted

with their credit reports. But action on those expressions remains at the discretion of the credit industry. If they calculate efficiently, credit grantors will steer clear of consumers who dispute their records *for any purpose*—justly or not—on the grounds that disputatious consumers are ipso facto more trouble than they're worth.

And of course, major and growing domains of surveillance remain closed to individual scrutiny a priori. These include the "investigative" activities carried out by law enforcement agencies, corporate investigators (insurance companies, for example), and national security agencies. Obviously there are reasons why some such processes must be kept from scrutiny for some purposes, and over some periods. But the idea that any and all surveillance that can be labeled "investigative" ought to be definitively free from review and response from the targets of investigation is chilling. And there are disquieting signs that the proportion of surveillance activities defined to lie in the realm beyond the reach of individuals is expanding. A most dramatic case is the American Patriot Act, which forbids anyone required to yield personal information on persons under investigation from revealing even the fact that such requests have been made.

A *second positive achievement* of some privacy codes has been to *forestall extension of surveillance* into domains of life where it would otherwise certainly have spread by now. If the reviews in parts II and III have demonstrated anything, it should be the tendency of surveillance systems to spread. It simply lies in the interests of both government and private surveillance operations to expand—to cover more people and more of the lives of the people they cover. Here and there, privacy codes and related legislation have served to block that extension, or significantly to constrain it.

The most dramatic cases discussed above are the restrictions on "positive" credit reporting in Australia and France. Through quite different historical sequences, these two countries both developed laws forbidding routine reporting of data on consumers' "good" credit accounts to interested financial institutions. Blanket "consent" to such surveillance as a condition of normal account relations is not recognized. Under the resulting, relatively privacy-friendly systems, consumers may supply data on their other credit accounts to prospective creditors. But they may also withhold such data at their discretion. Without legal restrictions, it is all but certain that American companies would by now have spread their practices to France and Australia, as they have done in Canada and the UK. Just such a shift from "negative" to "positive" credit

reporting has come about in Hong Kong in recent years, in the absence of legislative protections.

Similarly, strong privacy legislation in the European Union has been indispensable in blocking American-style release of account data from retailers, mail-order houses, periodical subscription lists, and the like to direct marketers.

Even in the UK, less compliant with the EU Privacy Directive than continental countries, such commerce requires consent. The result is a distinctly more privacy-friendly environment—where organizations wishing to use personal data for marketing generally face the burden of making their activities appealing enough to consumers to secure the latter's approval.

These salutary developments call attention to one predictable pattern in the tensions between privacy and the pressures militating against it. *Extensions of mass surveillance are far easier to forestall than to dismantle.* Rollbacks of major systems for monitoring individual lives, and shaping institutional action toward those monitored, appear rare. Something about such systems as functioning faits accomplis makes it very difficult to restore privacy-friendly environments once they are destroyed.

Let me be exact about my meaning here. I hardly suggest that opposition to new surveillance systems is doomed to failure—on the contrary. The last few decades have seen a number of schemes for highly privacy-invading systems turned back through vigorous popular protest and activism. One of the earliest and most dramatic was the Australian ID card scheme, blocked by an outburst of popular protest in the late 1980s. Similar protests in South Korea have more recently stymied elements of an elaborate government scheme for compiling and monitoring schoolchildren's records. In the United States, even the political umbrella of the so-called War on Terror did not suffice to protect the infamous Total Awareness Program—blocked in Congress in 2003. Much the same fate befell CAPPS II, the Department of Homeland Security program aimed at developing advance profiles of domestic air travelers—withdrawn in 2004.

My point is simply that opposition to major surveillance systems has its best chance *before* they are up and running. By contrast, it is difficult to think of many such systems that have been dismantled after a sustained period of producing results for their constituents.

There are a few exceptions. On a relatively small scale, the Children's Online Privacy Protection Act, which came into effect in 2000 in the United States, should have dismantled a small industry devoted to trading in personal data on children under thirteen—though there seems to be uncertainty as to whether all these direct marketing operations have indeed ceased. This measure seems to have won support, even against a profitable industry, because the businesses involved appeared to be patronized by sexual predators.

On a larger scale, the UK created a comprehensive identity card system during World War II, only to dismantle it after the war—to the dissatisfaction of many in law enforcement circles. The system had apparently become so thoroughly identified by the British public with wartime austerity as to be politically untenable. But of course, a bit more than sixty years later the British government is exerting itself to create a still more sophisticated, computerized version of that system.

Why is the dismantling of surveillance systems, once they are up and running, so rare? Perhaps because such operations, once instated, create vast sunk costs and major bureaucratic constituencies. Once whole categories of activity—from sales of credit reports to the tracking of air travelers—start to generate income and activity for surveillance professionals, the forces for their self-preservation are set in motion. Like expensive but over-sophisticated weapons systems, they become too costly to fail, even if that means that definitions of "success" have to be revised. Thus one suspects that the high-tech ID card scheme proposed by the Blair government in the UK, once set in motion, will never be dismantled—despite promises of the opposition parties to do so, if and when they gain power. Against such forces, privacy advocates wisely judge their prospects much better, when the task is to prevent such systems from gaining acceptance in the first place.

Similarly, what I call "frontal collisions" between officially enshrined privacy principles and established surveillance institutions have generally not gone well for privacy. Perhaps the most depressing example is the notorious "Safe Harbor" debacle. There the European Union abandoned explicit (and quite moderate) provisions of its privacy code in the face of political and economic threats from the United States. This collapse of a low-key privacy-protection policy, itself designed in part to smooth the international flow of personal information, continues to disturb many Europeans. But fears of major trade disruptions with the United States obviously overcame well-established privacy guarantees on the European side.

Another set of such "frontal collisions," of course, arose following the September 11 terrorist attacks on the United States. Practices explicitly mandated to protect privacy—for example, limits on the archiving of telephone and e-mail connection data—were overtly thrown to the winds, under the banner of waging war on terrorism. Note that the new demands for personal information imposed in these cases did not apply only to persons specifically suspected of terrorist actions or sympathies. They involved collection or retention of broad categories of data, on the assumption that *some* of this information might at some future point support the so-called War on Terror. Demands by American authorities for personal data on air passengers booked on flights to the United States are another case in point—clearly contrary to established European privacy guarantees, yet easily overriding them in an environment of security anxieties.

But though flying under the flag of the so-called War on Terror, measures like extended retention of telecommunication logs in fact aim at strengthening surveillance more broadly. The data now to be retained for as long as twenty-four months are to be shared by law enforcement agencies of all sorts, not just counter-terror specialists. Objections by privacy commissioners and others to these blanket extensions have not posed much of an obstacle to these changes. Around the world, the War on Terror has provided an indispensable Trojan Horse for intensified surveillance for all sorts of purposes.

One "near-miss" of a frontal collision came in the framing of America's Patriot Act in the weeks following September 11, 2001. As James Dempsey of the Center for Democracy and Technology points out, language in that legislation left intact most protections for government-held personal data systems established by the Privacy Act of 1974. Had that not been the case, the Patriot Act would have placed Americans' Social Security files, Census data, IRS records, and the like in the same vulnerable position as their library and bookstore choices—that is, subject to access by federal investigators virtually at their discretion. As Dempsey remarks, if the legislation "had started with the words, 'Notwithstanding any other law,' the story might be different, but it doesn't."[6]

Again, some countries' privacy guarantees have proved more robust than others'—against both government pressures and those emanating from the private sector. Thus France's CNIL has taken strong and sometimes successful

stands against private-sector privacy invasions, stances that have few equivalents in other countries. At the same time, however, France's state surveillance services seem to have been, at least until lately, even freer of challenge from courts and grassroots interests than elsewhere. By contrast, Canada has been stronger than other countries in its defense against government pressures on privacy in the wake of September 11. Thus it would be absurd to imagine that pressures on privacy have the same force in all national settings.

Nevertheless, the similarities in those pressures across national boundaries are unmistakable. Demands by institutions for personal data are nothing if not global phenomena—cropping up with striking predictability throughout the world's "advanced" societies. Each of the five countries outlined in this book, and many others, has instituted parallel efforts to monitor overseas financial transactions, movements of persons within and across national boundaries, and telecommunications logs in the wake of 9/11. All monitor use of cell phones, ATM machines, and credit and debit cards. All are entertaining creation of national ID card systems, where they do not already exist. The sheer fact that these data exist, or could be brought into existence, all but ensures that state agencies will clamor for access to them. And all these demands, of course, have their equivalents in the private sector.

The fact that privacy codes have provided effective resistance to such demands in many settings is heartening. But it would be rash to foretell how well such resistance will fare in the future. Meaningful privacy protection—by which I mean willingness to restrict use of personal data by established institutions even when that use would clearly be efficient—requires aroused public opinion. And the one thing we know about public opinion is that it is highly reactive. Shocks or threats—spurred by terrorist acts, or sickening crimes, or fears of economic loss—may force privacy concerns onto the back burner.

But if public opinion is evanescent and malleable, the enticements of expanding surveillance possibilities are enduring and utterly predictable. If any prophecy approaches the status of a sure thing, it is the expectation that new ways of creating, compiling, and using personal data will continue to emerge. Though we may not now know what they are, we can be sure that coming decades will generate a steady stream of new ways of monitoring people's whereabouts, their mental states, their medical conditions, their communication patterns, their consumption habits, and on and on. Institutional pressures to partake of these data are no less inevitable. Anyone who

claims confidence that privacy values will remain strong in the face of these developments is asserting powers not given to mortal human beings.

Origins of the Conflict

Why are the pressures on privacy so severe? What is it about the world we live in that makes demand for personal information, and the impulse of institutions to act on it, so relentless?

In fact, these trends arise directly from the scientific mentality that pervades our world. The Enlightenment philosopher and sociologist Auguste Comte captured the very spirit of the scientific age he saw dawning with the slogan, "Know, in order to predict; predict, in order to control." For Comte and his contemporaries, the prospect of ever-expanding knowledge of and control over human affairs was altogether positive. Science was making all the world intelligible, and such understanding would in turn form bases for remaking that world to suit human needs. With such deepened scientific understanding of social life, Comte believed, conflict would give way to general harmony, and politics to administration. Notions that innovations spawned by science might actually threaten key social values were nowhere on the radar screen.

Today's rise of mass surveillance stems from the scientific and technological activism lauded by Comte, applied to human beings. Comte saw his own age as evolving beyond an unscientific era where the form of institutions—of the state, the church, or the community—was simply *given* by custom and tradition. Emerging from that world, Comte discerned, was one where institutions would be constituted, as he saw it, scientifically. Organizations of all kinds, from educational institutions to industries, would be designed for efficiency and evaluated accordingly.

These prophecies have largely come true. Today we take it for granted that institutions—from universities to software companies to public welfare agencies—will be organized for efficient achievement of their appointed ends. Those publicly acknowledged to fall short on this criterion stand to lose legitimacy and support. Universities that train no students and foster no research; armies incapable of mounting successful campaigns; charities that absorb most of their contributions in operating expenses—organizations that fail such elementary tests of efficiency are candidates for public reproach or

dissolution. So total is this historical transformation in public expectations that the few remaining institutions with forms and practices governed by tradition—the Vatican, for example, or the British Monarchy, or the Dali Lama—strike us as agreeably quaint.

Surveillance systems reflect the same efficiency expectations held out for virtually all other organizations. Whether charged to collect taxes, allocate consumer credit or insurance, control crime, or combat terrorism, such systems are expected to obtain the greatest possible results from the least expenditures. The fact that these organizations are expected to shape human lives—rather than, say, manufacture pharmaceuticals or launch space satellites—counts for little. Surveillance organizations are expected to guide *discrimination*—as to who is worth extending credit to, and how much; or as to who is eligible to drive, and who is not; or as to who warrants tracking as a potential terrorist, and who does not. Hence the enormous pressures to acquire and exploit *actionable* personal data, bases for efficient guidance in meting out just the "right" treatment to each individual.

And hence the force of public expectation that any and all data capable of serving these purposes must be acquired and exploited. Once information is known to exist that would enable police efficiently to pinpoint potential child molesters—or make it possible for agencies to identify welfare cheaters or bad insurance risks or illness-prone applicants for health insurance—pressure to exploit such information grows overwhelmingly. The utilitarian logic of modern institutions views personal information simply as another vital resource—its use to be governed by cost-benefit rationality. Notions that such data ought to have some special ethical status are a hard sell.

In this world, the possibilities for organizations of all kinds to do "better"—that is, to know more about people and thereby to control their treatment more closely—are always growing. As new forms of actionable personal data become available, demands predictably arise to exploit them.

Think of an expanding snowball rolling down a freshly covered slope. A century ago, anyone seeking to assemble documented information on ordinary people would have faced slender possibilities, even in the most "advanced" countries. In the United States, even universal registration of births, marriages, and deaths was not complete in all states until well into the twentieth century. Social Security and income taxation did not document the lives

of the majority of American wage earners until the 1930s. Most American adults apparently did not have bank accounts until about World War II, or credit files until sometime around mid-century. Until the second half of the twentieth century, the list of record-systems likely to provide authoritative information on the majority of American adults was a very short one. Other prosperous societies would show different sequences in what forms of mass monitoring of the lives of ordinary people came into existence—for example, whether pension records preceded identity card systems. But I have been able to identify few such systems in any country much before the end of the nineteenth century.

At the beginning of the new millennium, it would be hard to list all the junctures of a typical American's life that regularly generate actionable personal information—data describing the individual and suitable for shaping institutional action where the person is concerned. It is all but impossible to live a normal American life without generating at least some *credit or debit transaction data.* Our movements within the country yield data on our whereabouts through *ATM and cell phone use, security checks, and automated toll receipts.* Our international travels are monitored through *TECS* and related government tracking systems. "*Public record data*" from courthouses and county record offices document life events from property transfers to divorces and bankruptcies—and now are electronically gathered and aggressively marketed. Even where the information remains in conventional form, aggressive companies assume the expense of computerizing the data, the better to retail them to interested private and government buyers. *Website visits* leave traces through cookies, and *e-mail and telephone* communications are regularly mined for purposes never envisaged by those who initiate the exchanges. This list could be extended at length—indeed, it is extending itself as I write.

As the snowball accelerates, it grows commensurately. The greater and more varied the sources of actionable data, the more quickly the interlocking systems can grow. S*urveillance feeds on itself.* The more of it there is, the more there can be. And the more personal data surveillance strategists can assume to exist in specific places, the less they need to involve the persons concerned in its acquisition.

Conspiratorial intent clearly fuels some of this growth—for example, companies' creation of websites whose unacknowledged purpose is to capture personal information for marketing. But in broader perspective, no conspiracy theory is needed to account for the larger pattern by which symbiotic,

mutually reinforcing surveillance systems come to monitor more and more of every normal life. This pattern is ultimately the result of modern institutions' seeking to fulfill their mandate: to allocate exactly the "right" treatment to each of countless discrete individuals. To this end, systems of all kinds grow both vertically and horizontally—in the amount of data that they compile and in their interconnections with other surveillance systems. The resulting pressures on privacy reflect nothing less intuitive than efficiency calculations applied to what has become a key resource for organizations—information on ordinary people and their lives.

Unexpected intersections of personal data systems often pose novel and perplexing dilemmas. In 2005, auditors at the New York State Comptroller's office announced that sex offenders in that state had for years been receiving Medicaid reimbursements for Viagra prescriptions. State and national Medicaid authorities rushed to block future payments of the kind, with much embarrassment all around.[7] But any thoughtful observer will wonder how many other associations might be brought to light through careful cross-checking of surveillance systems. Roman Catholic priests undergoing sex therapy? Corporate treasurers undergoing treatment for kleptomania?

Sometimes big profits await those imaginative enough to apply discriminations afforded by one system to management problems elsewhere. Recall the American credit reporting industry's marketing coup, when someone had the wit to inquire what predictive value credit scores would have for insurers. The answer, according to the insurance industry, was "a great deal." By purchasing credit scores on applicants for insurance, that industry raised rates for those with poor credit standing—brightening its bottom line, except where the practice is blocked by privacy laws. For the credit reporting industry, of course, the discovery was a bonanza—opening a vast new market for a "product" it already had, so to speak, on the shelf.

One can safely assume that shrewd entrepreneurs today are seeking to replicate such discoveries in many another industry. Once associations become apparent between any form of personal information and behavior that someone has an interest in controlling, demands to exploit such data for further discrimination become overwhelming. Should someone demonstrate that convicted terrorists have predictable preferences for a given brand of toothpaste *and* use of particular discount coupons to purchase it—say, by scanning records generated by supermarket discount cards—it would immediately become a dangerous thing for any consumer to share those habits.

Again, it will not do to blame "technology" for these trends. Advances in computing and related technologies certainly make it easier to collect, compile, and compare what once would have been utterly disparate and dispersed forms of personal information. But nothing about the technologies themselves dictates the *purposes* for which they will be mobilized. Indeed, surveillance interests often take the lead in shaping the form and direction of change in information technologies.

For decades in the United States, law enforcement authorities found it relatively easy to pinpoint the location of phones that they wiretapped. But the rise of cell phone use in the 1990s brought problems: the whereabouts of parties under surveillance was often unclear. To an innocent observer, it would have appeared that technology had evolved so as to favor privacy.

But American law enforcement was hardly prepared to accept that conclusion. If new telecommunications technologies posed problems for wiretapping, those technologies would simply have to be revamped to fulfill surveillance needs. As media analyst David J. Phillips puts it, "Once a type of information has been deemed to be 'reasonably accessible' under certain technological and industrial configurations, police agencies have successfully promulgated mandates to require that information to remain available, even as those configurations change." The FBI, he goes on to explain, urgently sought the ability to pinpoint the location of cell phone users. Thus it

> required specific technical change to the telecommunications system. These changes were justified in part by the claim that since the address of wired telephones had always been available under similar orders, then, in order to maintain the status quo, the location of wireless phones should also be available. But in fact the legal availability of the address of wired lines was initially justified by the technical "accessibility" to the phone company of its own service records. . . . Because the location of wired phones was legally accessible to police, then the location of wireless phones should be available as well, even if that meant changing the phone system in order to make that information "readily available."[8]

Similar developments have followed the replacement of conventional phone lines with fiber-optic cable. As Phillips and others have noted, fiber-optic lines are far more difficult to tap than the earlier technologies. The response was to require phone companies to *build in* accessibility to wiretaps of fiber-optic

lines—at their own considerable expense. That expense, one must assume, is ultimately borne by phone users.

Sometimes surveillance interests wait until technological change has run its course before asserting their claims over new forms of personal information. In the case of mobile phone technologies, the FBI initially disclaimed any intent to exploit routine recourse to cell phone data to track suspects. In lobbying for the CALEA legislation noted above in 1994, FBI Director Louis Freeh assured Congressional oversight bodies that such data would not be monitored without a court order. "There is no intent whatsoever," Freeh stated, "to acquire anything that could properly be called 'tracking' information."[9] Today such recourse by the FBI and other investigative agencies, without court warrant, is routine. In a statement defending the practice, federal prosecutors in 2005 asserted, "A cell phone user voluntarily transmits a signal to the cell phone company, and thereby 'assumes the risk' that the cell phone provider will reveal to law enforcement the cell-site information. This is not a privacy expectation that society is prepared to view as reasonable."[10] Thus we see what privacy-watchers call a "ratcheting down" of officially defined "reasonable expectations of privacy." As normal life comes to generate more traces of personal information in more different places, institutions increasingly regard access to the resulting archives of personal data as routine. Most people could once take it for granted that their whereabouts were not subject to ready verification by state agencies. Today any such assumptions would be dangerous—at least for cell phone users. And as people grow inured to the pervasiveness of such monitoring, their expectations of privacy—reasonable or not—erode.

Again, these uses of telecommunications technology are not *required* by the technologies themselves, but opportunistically exploited by aggressive institutions. In a different world, the same technologies might serve quite different purposes. They might, for example, serve to track the exact activities and expenditures of high-priced lobbyists and the legislators whose favors they cultivate. The reasons why such imaginative use of these technological potentials remain unexploited lie in the prevailing balance of political forces, not in any inherent logic or direction of information technology.

Or consider the vast efforts being promoted around the world to impose computer-readable ID cards as universal requirements for populations of democracies. Though greeted with varying degrees of hostility by those likely to be subjected to them, these systems have caught the imagination of

governments—which promote them as means to control an array of social evils ranging from welfare fraud to illegal immigration to terrorist activity. At the time of this writing, the most aggressive efforts of this sort emanate from the Blair government in Britain.

It is far from clear that grandiose schemes for universal, government-issued ID cards, even if they gain political support, will succeed in accomplishing what their sponsors promise. In Britain, an exhaustive research study carried out at the London School of Economics has called the technological feasibility of such a vast and expensive system into doubt.[11] Yet the desire of governments to get a closer grip on their populations incites planners to hype systems with no more than speculative chances of achieving their publicly touted aims.

Once national databases of entire populations exist, state agencies of all sorts find uses for them that may never have been announced, or even anticipated in advance. Think of all the surveillance purposes that have been added to basic federal record systems in the United States—those associated with the Social Security Administration, the IRS, and the passport system—since their founding. Under these circumstances, capital poured into creation of a national ID card system is apt to serve in the same way as investment in America's notorious anti-missile defense projects: unlikely to succeed in its own terms, but certain to create constituencies and sunk costs that will grant the enterprise the bureaucratic equivalent of Eternal Life.

The Destination

Where are these trends taking us? What sort of social world is emerging from the growth of these systems and their intensifying interaction with one another?

In my first book on privacy and surveillance, I proposed the idea of a "total surveillance society" as the theoretical end point of these developments. Concepts like this are what social scientists term *ideal types*—"textbook cases" of the ultimate realization of trends only partly manifest in the real world. They are ideal not in the sense of being desirable, but in that they exist only in the realm of pure ideas, like the idea of a perfect circle or a perfect vacuum. Social scientists use ideal types—like perfect competition or a perfectly developed caste system—as intellectual benchmarks for classification of real-

world situations. The notion of a total surveillance society thus helps identify a broad movement in that direction over recent decades.

Such movement involves growth in *surveillance capacity*—the strength of surveillance systems. Surveillance capacity grows in terms of the *numbers of persons* subject to surveillance; the *amount of information* that the system can bring to bear on each individual; the *subtlety of decision making* achieved on the basis of that information; the *centralization* or interconnectivity of data within the system; the *speed* of information flow and decision making; and the *points of contact* linking systems to the individuals they monitor.[12] The theoretical extreme where all these dimensions were maximized, I argued, would be a world where privacy was reduced to zero. Every moment, every fact about everyone would register at once with a centralized (or at least, totally intercommunicating) system; and all the information thus collected would be automatically available for use by organizations in their dealings with us.

More than thirty years after *Private Lives and Public Surveillance* was first published, the world has clearly traveled well along the road toward total surveillance. The proportion of populations covered by systems of mass surveillance; the number and variety of points in life where such systems take in data; the subtlety of the judgments they afford and the effectiveness of the actions taken on the bases of these judgments—all these things continue to rise, as steadily as the waters surrounding Christopher Robin's house at the top of the forest.

These developments have often brought with them real benefits. Growth in mass surveillance supports a host of valued services and conveniences, from easy credit to social security benefits to protection from crime and terrorism. But these advantages have come at significant costs in privacy.

Parts II and III detailed countless instances in which seemingly strong privacy guarantees have crumbled over the decades in the face of abrupt or incremental pressures. Think of the evolution of income taxation and Social Security in the United States—from institutions aimed at achieving closely delineated administrative aims to broad trunk lines of surveillance data. The very reach and authority of these systems has made them irresistible vehicles for purposes ranging from enforcement of child support obligations to the monitoring of applicants for mortgages.

Or think of the fate of the Privacy Act of 1974 in the United States, or for that matter PIPEDA, Canada's private-sector privacy law. Both these privacy codes quickly came to accept, in practice, the sharing of data provided for one

purpose, for other purposes not necessarily friendly to the individual—in a 180-degree reversal of their stated intent. Or think of the collapse of EU strictures against automatic retention of telecommunications data, following declaration of the so-called War on Terror. Or think of the surrender of French privacy interests to pressures from that country's taxation services for access to citizens' address files compiled by that country's welfare state services. Or think of Australia's national ID card scheme—once the third rail of that country's national politics following the public revolt against that scheme in 1988, now revived in thinly veiled form. Or think of the debacle of Safe Harbor, in which the most explicit European privacy guarantees buckled in the face of commercial and political pressures from the United States.

To be sure, these erosions of privacy would spur less alarm if only one could match them with a parallel roster of privacy victories. These would be instances in which established systems of personal data collection and use were sharply curtailed or dismantled—or in which areas of life once subject to close institutional monitoring have been freed of such attention. But it is hard to think of many such instances. Again, public outcries have blocked instatement of clearly privacy-invading systems while they were still aborning—for example, the Bush administration's Total Information Awareness scheme. But one has to regard these instances more as cases of the extension of surveillance forestalled than as reversals of a secular trend toward more surveillance.

Collapsing Resistance?

One thing that particularly alarms privacy-watchers is the apparent desensitization of publics to everyday demands on privacy. The sheer ubiquity of pressures for personal information, the variety of situations where they occur, and the seeming lack of alternatives—all these things apparently conspire to create a sense that resistance is futile.

Consider the "naked machines" contemplated for use in airport security.[13] These are devices that produce quick and precise images of travelers unclothed as they pass through security checks without their actually having to undress. The resulting snapshots leave virtually nothing to the imagination—and thereby supposedly make it impossible to carry guns or bombs on board. Will Americans accept such virtual strip searches as part of normal routines of air travel?

The fact that authorities appear ready to "test drive" these devices on real passengers implies their calculation that air travelers are willing to accept intrusions that would have been out of the question a few years earlier. If they are shrewd, the planners will introduce this highly efficient (but utterly unprivate) form of screening as voluntary—an optional alternative to more time-consuming conventional security routines. In time, exercising a formally existing option for privacy could become about as easy as renting a car without a credit card.

But incremental weakening of our privacy immune systems seems to have been under way well before plans for "naked machines." Reviewing the relatively short history of mass surveillance, one notes a disturbing pattern: ideas and plans rejected in early years as dangerous to privacy seem to evoke markedly less resistance when resurrected a few years later.

In 1966 and 1967, the U.S. Congress held hearings on a proposed National Data Center, a project to assemble personal information held throughout the federal government. Intended mainly to support social science research, such a center would have brought together information held by the Census, the IRS, Social Security, and many other agencies. Officially supported by the heavyweight Bureau of the Budget, the proposed Center was supposedly not to be used for decision making on any individual, but only for research and policy formation. But the idea never withstood widespread mistrust of centralized personal record-keeping. In the words of one Congressional critic, "Good computermen know that one of the most practical of our present safeguards of privacy is the fragmented nature of present information. It is scattered in little bits and pieces across the geography and years of our life. . . . A central databank removes completely this safeguard."[14]

The contrast to present-day efforts under the Patriot Act to centralize personal data from sources ranging from courthouse records to library choices is stunning. Fear of further terrorist violence clearly has provided a major impetus for willingness to accept such measures. But many privacy-watchers also discern a more insidious trend at work—de-sensitization to collection of personal data in seemingly all settings, and a resulting sense of fatalism in the face of such developments.

Policy-makers always seem ready to exploit such changes. In 1974, America's attorney general commissioned a study of false identification, seen as a major problem in fraud, crime, and immigration violations. Two years later, Justice Department researchers produced a weighty and carefully

researched report that specifically rejected creation of a national ID card as a solution to these concerns—on grounds including that any such document might more easily be obtained and used by criminals than by law-abiding citizens.[15]

In the post-9/11 period, by contrast, Congress is pressing states to adopt exacting uniform federal standards for driver's licenses. Only licenses issued by states meeting these standards, which include machine-readability, would be acceptable to identify air travelers or visitors to federal facilities. No one doubts that the ultimate aim is the creation of a national ID card system, despite considerable distaste for the idea from both sides of the political spectrum.

Other countries also show signs of collapse in their resistance against privacy invasion. The courteous British civil servants I interviewed in the 1970s were put off by American-style commercialization of personal information in banking and credit. In the interim, they and their counterparts have certainly had to adjust their attitudes—now that commercialization of personal data from banks, credit card companies, and other businesses has grown virtually as extensive as in the United States. That reversal was at least as complete as the changes being sought by the Blair government in attitudes toward national ID cards.

In France, as well, privacy-watchers complain of decreasing public indignation, or rising fatalism, concerning demands for personal information. There, too, fears of something like America's proposed National Data Center (the SAFARI plan) in 1974 bolstered privacy sentiment and helped inspire creation of the National Commission on Information Processing and Liberties, France's privacy protection agency. By the twenty-first century, however, French citizens are accustomed to having their data electronically harvested nearly as frequently as Americans—at ATMs, in automated toll collections and vehicle license plate recognition, or on the Internet—causing many privacy-watchers to sense decreasing public skepticism, or rising fatalism, about prospects for defending privacy. The CNIL itself, one of the world's stronger and more independent privacy protection agencies, had its powers to block legislation injurious to privacy removed by Parliament in 2004.

Or, consider the growing prerogatives of the French tax collection system regarding social insurance information. For years tax authorities had sought to gain access to people's current addresses from the system administering health care and other benefits—only to have this attractive symbiosis blocked by the CNIL. But in 1998, that body was outflanked by parliamentary

action that effectively made personal data gathered for administration of welfare state benefits available to the nation's tax collection services.

Much public acquiescence to heightened monitoring clearly stems from government exploitation of fears of terrorism and other authentic dangers. But it would be fanciful to imagine that that were the only force involved. Often one simply senses that many people have *given up* trying to control, or even keep track of, the myriad uses of information about themselves. Terrorist threats, after all, have no bearing on the willingness of many Americans to have their daily supermarket choices monitored and traded.

Nor do terrorist dangers play a role in consumers' willingness to subscribe to services like those where one's e-mail exchanges are electronically monitored to generate sidebar ads targeted to the contents of the messages. Nor has the easy revelation of cell phone users' whereabouts apparently undermined consumers' enthusiasm for that seductive technology. Again, public opinion studies register widespread concern over the pervasiveness of surveillance as a fact of public life, both in America and abroad. But perhaps that very pervasiveness has triggered feelings of impotence in the face of a rising tide of claims on personal data. As in environmental affairs, widespread perceptions of a generally degraded situation may foster a sense that the cause is already lost.

Clearly willingness to accept incremental losses of privacy depends utterly on the public *framing* of such choice—that is, on the larger contexts or narratives of which each individual choice is perceived as part. Salient among these of late are frames having to do with struggles against insidious evils. "If just one life is spared from terrorist violence by monitoring of library records, e-mail communications, or cell phone use," one is apt to hear, "it will be worth it." No one, of course, wants to risk innocent life—and no one could ever deny that monitoring some specific form of personal data *might,* conceivably, thwart a terrorist act. But a moment's reflection reminds us that arguments in this form could be used to justify virtually *any* invasion of privacy—or the sacrifice of any number of other public values.

Nevertheless, readiness to yield even intimate personal data has come to be portrayed virtually as a badge of public honor in many settings. Sociologist Gary Marx recounts events in Massachusetts in 2004, where police politely sought DNA samples from all males in a small community in their effort to solve a shocking murder case.[16] Collection—via a mouth swab—was

apparently less objectionable than techniques like lie detectors or blood or urine sampling. Those few males who declined to provide the samples undoubtedly found themselves subjected to special police scrutiny.

And police, in turn, will inevitably prefer to store all identifying DNA data permanently, for use in other crime investigations where DNA evidence is available. The net result is movement toward a world in which the authorities will have at their disposal comprehensive DNA records of the entire population. Such a compilation could make it possible to identify participants in casual sexual encounters, political demonstrations, or off-the-record meetings in any number of settings. Presumably such outcomes were no part of the desires of the volunteers who provided their own samples in hopes of solving a serious crime. But personal data systems, once created, have a way of outlasting their founders' intents.

Still other reasons for willingness to relinquish one's own privacy stem purely from desire for relief from inconvenience. Think of the "Registered Traveler Program," in which Americans are invited to grant continuing access to their personal data in order to speed their way through airport security lines. In the privacy environment that we now inhabit, it is hard to imagine any scarcity of willing takers.

Of course, my learned friend—the one who considers privacy a vaguely attractive but utterly outmoded value—would make total sense of all this. Defense of privacy is simply anachronistic, he avers, in a world where the most basic social and economic processes require easy flow of information. Those who are serious about their dedication to this quaint value, he would likely insist, should show their bona fides by communicating only face-to-face, never relying on credit or debit cards, and traveling only by foot or bicycle.

"Needs," "Purposes," and "Consent"

Most of us still resist drawing such categorical conclusions. We struggle to find ways of making the most of new information possibilities without renouncing meaningful control over information on ourselves. But we do not find it easy to give a simple account of what form that control should take, or what uses of personal data it should address. Indeed, the very language available for thinking about these things makes it hard to identify a point at which losses to privacy cross the line from merely troublesome to quite intolerable.

That language serves more often to obscure than to enlighten. Perhaps most confusing is the view of institutions and the individuals dealing with them as occupying essentially symmetrical positions—both acting in response to mutual "needs." As an individual consumer, in other words, I need a credit card; on the other side of the bargain, the credit card company "needs" my information in order to accept and manage my account.

Like many another myth, this one is not precisely wrong, so much as vastly oversimplified. Certainly some institutional actions literally cannot go forward without reliance on some forms of personal information. No one should expect to subscribe to a publication, without providing an electronic or physical address for its delivery. Nor does it make sense to seek medical treatment without providing at least some information on one's medical history—though patients do often censor what they tell their caregivers. Cases like these involve what law professor Jerry Kang terms "functional" relationships between personal information and specific performances.[17] Were all alleged "needs" for personal data of this type, one might reasonably regard personal information as playing the same indispensable role in institutional action that fuel plays in internal combustion engines.

But in the real world of large institutions and mass surveillance, things are nowhere near this simple. As we have seen, all sorts of organizations stand to *do better in their own terms* by amassing more and more telling personal data. Taxation systems identify more fraudulent returns; law enforcement agencies more effectively track suspects; direct marketers target customers more precisely; sellers of credit and insurance propose more profitable terms to their potential customers—and on and on.

In this sense, institutions' "needs" for information on the people they deal with are infinite. But this is hardly to say that the data in question are indispensable, that leaving "needs" unsatisfied would stop institutions in their tracks. The efficiency gains realized from knowing more and more about people are incremental, not life-or-death propositions.

Similar confusion surrounds ideas of the "purposes" of surveillance systems. A key tenet of the consensus fair information practices is that personal information provided to the systems must be used in ways consistent with the purposes for which individuals provide it. Of course, this uplifting precept is regularly bypassed in practice—especially as today's surveillance systems rely more and more on data drawn from sources beyond the individual's control.

But even where institutions collect personal data directly from the individuals concerned, the "purposes" for which they do so are no open-and-shut matter. Imagine a consumer consulting a website created by a pharmaceutical company to inform herself on sexually transmitted diseases, or incontinence remedies, or psychoactive drugs—matters on which the consumer might well prefer to avoid direct inquiry to human sources. The companies involved, for their part, may well have created the website to capture names and addresses of potential customers—in hopes of marketing products to which the latter are likely susceptible.

Who defines the "purposes" of systems like these? For the creator of the site, the purpose is to identify people suffering from the conditions described on the site. For the consumer, the purpose might be precisely to inform one's self without being identified. Thus the "purposes" of surveillance systems are what philosophers call "essentially contested concepts"—ideas like "liberty" or "equity" that are subject to endless debate and reinterpretation, according to the political values and *partis pris* of those who invoke them.

"Consent" to appropriation of one's own information is another idea that has been so thoroughly pummeled with tendentious interpretations as to lose all meaningful content. One of the most familiar clichés of conventional privacy protection lore is that surveillance ought to operate with the "consent" of the individual—implying that one should be able to "just say no" to privacy-invading practices. But what passes for consent to surveillance is often the only option for accessing things most people would consider elements of any normal life—a bank account, a credit card, or the opportunity to board an airplane.

Certainly there can be justification for requiring some forms of personal data from those seeking these arrangements. But the idea that people "choose" to relinquish their privacy in such situations makes about as much sense as notions of people's "choosing" to flee their burning homes. In both cases, those concerned might well have preferred to avoid altogether the choices they are obliged to make.

What all this equivocal language ignores is *context.* The "purposes" of surveillance; the "needs" of organizations for personal information; and people's "consent" to providing such data—these things make sense only in terms of common understanding of what parties owe one another, of what constitute reasonable demands. Of all the (potentially infinite) "needs" of organizations to know things about people, which should be held legitimate? Who is

to define the "purposes" of collecting personal information? When is "consent" authentic, and when must it be considered a sham? Answers to questions like these are not given in the nature of things—like the bandwidth of a computer connection or the height of Mount Everest. Such understandings can only emerge from thoughtful public deliberation on matters of fundamental value and fairness.

We take as much for granted in many other contexts. Medical care providers clearly have "needs" to be paid for their services—but ethical and legal rules constrain their latitude to satisfy such needs (for example, by refusing treatment in emergency rooms to those unable to pay cash up front). Police often "need"—quite urgently—to compel suspects to provide vital information about crimes—but basic civil liberties constrain them against using torture or from requiring self-incrimination. The point is, we cannot expect definitions of matters such as legitimate versus illegitimate needs to be settled by the parties on the spot. Such definitions have to emerge from some larger collective soul-searching. Where they are lacking—as often in privacy matters—we have no choice but to create them.

Some years back, I did what many Americans did in the 1990s: I re-financed the existing mortgage on my home, hoping to raise some cash and benefit from decreased interest rates. In the endgame to this transaction, I found myself sitting across the table from the lender's lawyer and representatives of other self-interested parties—signing one document after another, and writing checks for processing costs that always seemed to be calculated as last-minute add-ons, at my expense. Inevitably, one's eyes glaze over at the onslaught of papers and the hemorrhage of funds. At the very end, the lawyer passed me a final authorization from the IRS.

Contrary to every inclination, I actually looked at the papers, which seemed to grant the bank access to my tax returns. This struck me as peculiar, since I had (inevitably) already filed recent tax returns with the original mortgage application. On closer inspection, I found that the papers handed me were pre-dated authorizations to the IRS to supply the bank with copies of any *future* tax returns that I might file during the lifetime of the mortgage. Here, notwithstanding dazed consciousness and desperation to conclude the transaction, I balked. Mortgage or no mortgage, I refused to authorize the bank to delve into tax returns that I had not yet compiled, covering years of

my life that I had not yet lived. After token resistance, the other side backed down, and we closed.

But really, I've wondered ever since, why was that the sticking point? Were the principles underlying the demand that I finally found unacceptable any different from those to which I'd already acquiesced? After all, the bank certainly had one sort of "need" for access to my financial affairs after the mortgage was made. If I were to fall behind in my payments, the bank would certainly find it advantageous to base its response on a full understanding of my financial circumstances. They might want to know, for example, whether I had become unemployed (and hence literally unable to pay). Or were missing payments due to a contested divorce or other domestic circumstance?

Always having my full and up-to-date IRS returns on file would certainly make it easier for the bank to offer me new financial services that I might find attractive (and that they would find profitable). And being able to share information from my IRS files with credit reporting agencies would certainly make the bank a more attractive business partner for the latter—presumably reducing the bank's costs and (theoretically) contributing to lower-cost mortgages and other services. At a very minimum, I had to agree that claims on my future tax returns were consistent with the "purposes" of the transaction (at least, from the bank's point of view) and that my "consent" to such access, had I given it, would have been calculated with an eye to my interest in seeing the transaction accomplished. Certainly, too, the bank was being open about its needs and intent—if a little abrupt in springing its demands—so that requirements of due process were served. Was that final straw that broke the back of this consumer's acquiescence really any different from the host of such demands to which I'd already yielded?

Anyone who follows the ever-unfolding fate of personal data collects countless stories of seemingly intolerable demands for personal data that, nevertheless, people end up tolerating. Effective resistance makes itself conspicuous by its rarity. In 2005, the CNIL, France's government privacy protection agency, addressed a novel auto insurance program proposed by Britain's Norwich Union for sale to French motorists. Drivers would have their cars fitted with devices registering speed and location; these "black boxes" would transmit, every two minutes, data on routes being traveled, length of trips, and speed. In a marketing appeal directed particularly to young drivers, Norwich Union promised to bill drivers who remained within legal limits at lower rates than those who did not.

The CNIL blocked the project from going forward in France. That country's key 1978 privacy legislation, the agency determined, forbids private interests (with limited exceptions) to monitor compliance with laws. The fact that the drivers concerned gave their consent to such monitoring made no difference. In the words of a CNIL spokesperson, the contract offered by Norwich Union amounted to "trafficking in people's liberty of movement." "Consent does not suffice," the CNIL stated, "to make any use of personal information legitimate."[18]

Britain's information commissioner shows no signs of taking such a position regarding plans for similar insurance contracts in that country, so long as participation remains "voluntary." And it is all but impossible to imagine privacy concerns blocking such an exercise of contractual freedom in the United States. After all, the *aims* of the surveillance are above reproach: to discourage poor driving, especially by young drivers, and to reward those whose records show compliance with that aim.

Indeed, by the logic of standard fair information practices, the *means* for achieving these results should also be held acceptable. After all, data collected would be held in strict confidence; used only for the purposes designated by the company (at least until further notice); and (presumably) subject to correction in case of inaccuracy or arbitrariness. Altogether, this discreet but potentially effective form of monitoring embodies the classic formula for success in the extension of surveillance: an imaginative way of capturing actionable personal data in an effort to control troublesome and destructive conduct. One wonders whether French privacy-protection convictions will continue to withstand the blandishments of such possibilities.

If our look at surveillance in five countries has taught any lesson at all, it is that "needs" for personal information are experienced quite differently across national boundaries. The government of France has apparently for decades experienced needs for virtually unrestricted access to its people's movements, accounts, and communications—needs abundantly satisfied by that country's security services, with hardly a vestige of accountability. Other countries—Canada, notably—have proved far more discriminating in the satisfaction of such needs, while hardly denying the legitimacy of some agencies' requests for discreet investigation of potential terrorist activities. In the private sector, France and Australia drastically constrain businesses' ability to monitor and

report on consumers' "good" credit accounts—all but starving needs that are generously satisfied in other countries. Yet credit services flourish in both these countries, even if not developed to the intensive extremes reached in countries dominated by American credit reporting interests.

One could extend these contrasts at some length. The point is not that institutional "needs" for personal data are not authentic. In every country, institutions almost invariably stand to perform better by knowing more about the people they deal with. Where countries differ is not in the existence of needs, so much as in the public legitimacy accorded such needs in juxtaposition to other, countervailing needs—privacy very much among them. When shopping for a new home or car, we are always aware of the "need" of potential sellers to know how much we are able to pay, or how badly we want to make the purchase. But under these circumstances, we are also acutely aware of our own "needs" to keep such data to ourselves, in order to make the best bargain we can. Which of these countervailing—and equally authentic—needs will be satisfied under prevailing privacy regimes is a matter for political and legal resolution, not a fact of nature.

True, the profiles of all five countries reveal a net shift toward satisfaction of privacy-unfriendly "needs" of institutions. With few exceptions, the last fifteen years have seen shrinkage in the realm of personal information that ordinary citizens in these countries can expect to keep to themselves, in the face of counterclaims by government and private bodies. But this worrisome trend stems from the political ascendance of surveillance interests in our times—not from the inflexible nature of the needs served by surveillance. Life would go on quite adequately, in other words, if the public were to opt for simply leaving significant surveillance needs unmet.

Some Uncomfortable Futures

Clearly any one measure to satisfy such needs represents just a single step in a much larger journey. Privacy advocates find themselves constantly embroiled in resisting such steps. But it helps to look beyond these skirmishes to weigh the long-term prospects of the privacy wars. What further changes in surveillance can we expect in coming years? What forms of human wrongdoing, inefficiency, or wasted effort stand to be corrected through more sophisticated monitoring of individuals' lives?

State monitoring of personal movements. Think of the gains for public order, if only state authorities knew where everyone was at all times. Imagine, then, a world where highly trusted agencies of the state could always determine the exact whereabouts of each citizen or resident in real time. The most obvious advantages would have to do with crime control. Missing-persons cases, kidnappings, and many other particularly dangerous crimes would all but become a thing of the past. Indeed, offenses from murder to overtime parking would immediately reveal themselves—surely leading to drastic reduction in such infractions. In a world where detection would be all but automatic, crime would become an unattractive proposition.

Indeed, resourceful analysis of the endlessly accumulating archive of personal movements generated by a system like this would provide tools for anticipating and forestalling antisocial conduct. Combinations and sequences of movements highly *associated* with wrongdoing would provide grounds for intensified monitoring—much as authorities today attend to loitering in high-crime neighborhoods. Movement patterns associated with drug production, smuggling of illegal aliens, child pornography, or any number of other serious crimes would readily mark the perpetrators—even before they had the opportunity to commit crimes.

Most of the technological and managerial capabilities necessary to support a system like this already exist. In the United States, movements across international boundaries, uses of ATM machines and toll roads and bridges, and countless credit card, debit card, and shopping card transactions already afford tracking of the great majority of Americans. But cell phone technology, more than any other innovation, could make something like total population monitoring feasible in the near future. Though many users seem not to know it, cell phones, when turned on, have the potential to track their users' movements. Providers of cell phone service already devote vast resources to responding to inquiries by police and courts concerning the whereabouts of users. A significant surveillance breakthrough could be realized, if only cell phone use were universal and all phones kept on at all times.

Obviously a project of this scope would require legislative authority and major public investment. Authorizing legislation would have to provide funds for basic cell phone service for every American citizen and resident, along with requirements that the phones be kept on one's person at all times. Perhaps the best way to accomplish this would be to build in some form of automatic alarm that would sound if anyone removed his or her phone. An

efficient alternative might be to implant some element of the cell phone mechanism in each American's body. In either case, to ensure the benefits of universal compliance, stiff penalties would have to be introduced for efforts to break contact between one's device and the central monitors.

To ensure that the system did not infringe on privacy, an impeccably reliable authority would have to be created to guide it. This body would supervise the collection and monitoring of the vast resulting streams of data—and their indefinite retention for use in resolution of crimes not immediately noted. These authorities would be enjoined to ensure that data so collected were used only for authorized purposes. Such purposes would naturally include use by government agencies having legitimate *needs* for the data—which would probably prove to be virtually all government agencies. But the strictest guarantees would dictate that personal information garnered in a system like this would never be used to violate privacy—that is, to satisfy idle curiosity or other unproductive interests.

State Monitoring of Wealth and Transactions

Another messy domain of civic life, ripe for better discipline and enhanced efficiency, is the world of financial transactions. Much destructive and antisocial behavior obviously involves illegal exchanges of money. These range from purchases that should never occur (for sex, political favors, or bodily organs); to money laundering; to failure to pay one's full tax obligations. Nobody disputes that such uses of wealth fly in the face of community values and cost law-abiding citizens dearly. Fortunately, technologies and management ingenuity in the immediate offing could provide a sweeping corrective to these ills.

What we need—or at least, what many will conclude that we need—is a system in which all accounts and transactions are computerized—and where trustworthy state agencies constantly track both in real time, much as in the proposed tracking of personal movements. Cash would be eliminated, making the system a monitor of all financial holdings and exchanges. Every transaction, from corporate transfers to the purchase of groceries, would pass through the system, and the parties would be required to record the purpose of each exchange. To ensure the system's effectiveness, attempts to use cash or barter would bring severe penalties, as would inaccurate representations of goods or services exchanged.

Here, too, strict privacy guarantees would have to govern operation of the system. Only those state agencies with demonstrable needs for information on people's financial affairs would have access to data it generated. These would obviously include law enforcement agencies, tax authorities, all social welfare and social security authorities—in fact, virtually all state agencies. Idle curiosity and useless prying, on the other hand, would be considered serious privacy violations and actively repressed—thus helping ensure public confidence in the system and maximizing ready compliance.

Once the public adjusted to it, a system like this would gain very wide support. With total discretion, it would reassure every citizen that all others were meeting their obligations. Sophisticated analysis of the ongoing stream of data would enable law enforcement officials to identify and curtail countless forms of wrongdoing—from terrorist preparations to drug sales to illegal political contributions—as soon as they occur. Once people experienced the benefits of a world where all taxes were paid, where all employment were on the books, and where improper transactions were impossible, proposals to deal in cash would become about as acceptable as gifts of radioactive waste.

Corporate Scrutiny over Consumption. The benefits of the previous two systems would be apparent above all in improved compliance with civic obligations. But comparable gains would arise from a comprehensive private-sector system for monitoring people's lives as consumers. Such a system would do for financial resources and consumption choices what the two previous systems would do for personal movements and economic exchange.

Viewing the big picture, it is apparent that nearly everyone's consumption patterns involve costly inefficiencies and missed opportunities. People choose products and services that are not right for them. Consumers are exposed to inappropriate advertising and—more important—miss opportunities to experience advertising for products and services for which they are particularly susceptible. A comprehensive system of monitoring all consumer choices, and their resources for further choices, could streamline the realm of consumption to the benefit of all.

The system required to accomplish all this would combine the strengths of today's direct-marketing databases with those of insurance and credit reporting systems. It would monitor not only people's total financial situations—accounts, assets, and obligations—but also the timing and content of every consumer transaction. It would also compile all available data to afford

judgments on consumer susceptibilities, including not only records of past purchases but also social and demographic data known to predict future consumption potential.

Given its scope, a project like this would probably have to be organized as a kind of public utility. All retail businesses would feed all their transaction data into the central system—complete with identifying information on consumers doing the transactions, of course. Public record information; demographic data from the census, postal service, and other sources; and current account data would also be indispensable. The resulting data pool would provide next-to-complete knowledge of all persons' inclinations to purchase and resources for doing so. It would naturally be available for exploitation by any and all businesses, including both those seeking to sell goods and services to any interested party and those (like insurance and credit providers) seeking to *avoid* doing business with the wrong consumers.

Such a system would realize vast efficiencies—above all, by offering each consumer precisely the goods and services he or she would be most likely to choose, at the highest price each could be expected to tolerate. Once perfected, it could make *all* pricing "target pricing," in which the price offered by the seller would be the highest price that particular consumer would tolerate at the moment offered. Direct advertising would be pervasive. Thus one would expect to encounter a steady stream of ads on the screen in front of one's airline seat—which, to maximize its cost-effectiveness, could be turned off only on payment of an additional fee.

In this vein, some far-seeing European entrepreneurs have already proposed to offer phone service, free of charge, to consumers willing to have their conversations interrupted with random ads. In the short run, such suggestions may strike some as intrusive. But such objections would evaporate, once people realized that they were hearing only appeals for precisely the products and services that they most want to purchase—whether they have been aware of their need for them in advance, or not.

Once the public came to appreciate the rewards of measures like these, the whole system could move a quantum step ahead. Outward manifestation of consumer choice could simply be dispensed with. Sellers could supply buyers with things that they were projected to need, notifying them only after the fact—and debiting their credit cards or bank accounts accordingly. Savings would presumably be passed on to consumers in the form of lower prices. In the rare event that the consumer felt a mistake had been made, he or she

would have the option of returning items that had been supplied, on provision of adequate justification for the refusal.

Developments like these would not serve corporate interests exclusively. Comprehensive monitoring of consumption would also open the way for dramatic progress in public health and personal well-being. By tracking the exact detail of people's choices of food, drink, and recreation, a system like this would identify those whose style of life posed a danger to themselves—or to others, via increased costs for health care that all would ultimately share. Those whose supermarket selections revealed consistently high intakes of saturated fats or low-nutrition snacks could receive timely warnings of the health consequences—perhaps through messages distributed or displayed at the checkout counter. The costs of such warnings would happily be borne by industries producing whole-grain foods, fresh vegetables, spring water, and other salubrious alternatives.

At the same time, data generated in a system like this would drastically enhance the efficiency of credit and insurance allocation. Systematic trolling through the logs of consumer choice would reveal associations that, whatever their origin, would identify in advance the most and least desirable credit and insurance applicants. Imagine, for example, the revelation that those who purchased mocha nut ice cream *and* condoms in bulk *and* who typically paid their utility bills at the very last moment were more likely to contest charges appearing on their credit card bills. Since responding to billing disputes raises the cost of any credit operation, it would be only reasonable to charge higher rates to consumers so identified.

These three as-yet-hypothetical systems would do no more than fulfill the promise of surveillance possibilities already in sight. Once people had grown accustomed to them, it would quickly become apparent that each system needed support from the other two. If consumers' supermarket purchases predicted their future credit or insurance use, analysis of the same information could just as readily predict likely future involvement in tax evasion or terrorist activity. By the same token, data on consumers' movements or financial transactions collected by government institutions could prove invaluable for further refinement of precisely targeted direct advertising.

Inevitably, forward-looking planners in both the state and private sector would want to create arrangements for sharing surveillance capacities, thereby

sharpening the efficiency of all three operations. True, critics might object to disclosing data provided to the government to support the quest for private-sector profit. But economists would be quick to point out that everyone stands to benefit by more precise private-sector decision making on consumers. Increased sales volumes from more efficient direct marketing, quicker determinations of eligibility for credit and insurance—all these things would spur the economy, raise tax revenues, and thereby ultimately benefit everyone.

Of course, the list of authorized purposes for which data might be used would grow without limit, given the natural tendency of surveillance systems to spot new connections between forms of personal information and possibilities for enlightened control. But as those possibilities become more extensive, and the impact of the systems on the lives of those monitored became more far-reaching, public confidence would be buoyed by the fact that the systems were operating under the rule of law. People would always be able to view their own data (except where doing so threatened the efficiency of decisions being made) and to contest and correct inaccurate or unfair data. The result would be what many would consider the best of all possible worlds—one where scrupulous observance of privacy principles coexisted with something approaching total surveillance.

Shouldn't those assurances suffice to allay any anxieties about privacy?

No.

Most Americans, and citizens of most other democracies, would find these quantum jumps toward total surveillance intolerable. Much as we may share the desire to combat terrorism, control crime, or combat tax evasion, we are not yet willing to make our movements and financial transactions an open book to the state. Much as we appreciate low prices, quick credit, and easy access to products and services, we are not prepared to share all the details of our consumption lives with the institutions that promise to provide these things. Much as we have all grown inured to providing even the most intimate personal information to bureaucracies in the course of our daily lives, something tells us that the ultimate perfection of systems like these simply goes too far.

But how far is too far? If intolerable invasion of privacy is indeed like the perception of pornography, it will not do simply to assert that we "know it when we see it." Claims on our information that we see as acceptable (if perhaps regrettable) this year would certainly have been unacceptable at earlier

stages. And who would be rash enough to predict the life span of today's standards of tolerability?

By this point, I hope readers have abandoned any idea that some forms of personal information are somehow inherently too personal or private to attract institutional interest. Even the most "personal" data—perhaps especially such data—can provide bases for crucial discriminations that institutions seek to implement. It is undoubtedly true, for example, that all citizens stand to lose, however indirectly, from the bad dietary habits of their fellow citizens—for example, through expensive illnesses and disabilities whose costs everyone feels through higher medical insurance rates or lost productivity. For most of us, this evident connection still does not warrant institutional surveillance over our dietary choices. But how long will this thinking withstand pressures for more public responsibility over diet and health?

There is just one decisive reason for resisting the shift toward a world of total surveillance—and that is that no one really wants to live there. This is not because such a world would be unworkable or inefficient—quite the contrary. Once most people grow inured to monitoring as a normal feature of everyday life, a total surveillance world would work much more smoothly than any alternative.

Few people, if asked whether they wished to exchange such efficiencies for such sweeping loss of privacy in a single stroke, would accept. But will such choices be posed in this dramatic fashion—or incrementally?

In a brilliant and influential article, "The Tyranny of Small Decisions," Cornell economist and planner Alfred J. Kahn challenges some basic ideas on how public decisions get made. May it not be, he wonders, that the accumulating "free" choices of individual consumers in the end give rise to collective outcomes that no one really prefers?

Kahn cites the example of train service to his home in Ithaca, New York—a place whose winter weather often blocks air and road travel. Over the years, rail travel lost market share to the other alternatives, to the point where passenger service was discontinued as unprofitable. The loss stemmed from countless seemingly rational decisions by travelers to choose car, bus, or air travel over the train, for reasons of comfort, schedule, or price. Yet the cumulative result, Kahn argues, was one that no one would have chosen, had the choices been cast appropriately. "The fact is," Kahn writes, "the railroad

provided the one reliable means of getting into and out of Ithaca in all kinds of weather; and this insufficiently exerted option . . . was something I for one would have been willing to pay something to have kept alive."

The mechanism by which this irrational result emerged from apparently rational individual decisions seems clear. Kahn writes, "The cause . . . was the discrepancy between the time perspective of the choices I was given an opportunity to make—deciding, each time I planned to travel, whether or not to go by train—and the relevant decision of the railroad, which was a long-run, virtually all-or-nothing and once-for-all decision, to retain or abandon passenger service."[19] Kahn goes on to re-frame other momentous public choices that have been made in the form of such incremental nondecisions—for example, the rise of automobile ownership and transport. He quotes philosopher Morris Cohen: "Suppose . . . some being from outer space had made us this proposition: 'I know how to make a means of transportation that could in effect put 200 horses at the disposal of each of you. It would permit you to travel about, alone or in small groups, at 60 to 80 miles an hour. I offer you this knowledge; the price is 40,000 lives per year.' Would we have accepted?"

Would we?

"The chains of habit are generally too weak to be felt," wrote Samuel Johnson, "until they are too strong to be broken." Most of us have long since grown accustomed to "choosing" discrete losses of control over our data in exchange for the trappings of normal life in an information-hungry world. In so doing, we incrementally nudge that world toward total surveillance—that is, toward a regime hardly anyone really wants.

Ground to Stand On

But sometimes the choices are dramatic enough that we dig in our heels.

Recall the revolt of parents of schoolchildren in Sutter, California, noted in part I. They were incensed at the attempt to fit each pupil with an RFID tag that would track his or her whereabouts throughout the school day. "Our children are not inventory," they insisted, in a formal complaint to the school board.

Ultimately, this story had a happy ending for privacy advocates. A rash of negative publicity caused the project to be dropped. But can we assume that innovations like this would always spark such opposition? I don't think so.

In this case, no one claimed that needs for the new system stemmed from any special threat or cost. But imagine the response had proponents been able to put forward their measure as a solution to a crisis or emergency? What if there had been a recent history of harm to students on the school grounds—harm that might have been prevented by a system that identified each student's whereabouts? Or for that matter, what if the school stood to lose, say, $100 for each hour a student was at school, but absent from class? Under these conditions, the privacy reflexes of citizens and school board members might have been quite different.

In the absence of gut reactions like the ones that erupted in Sutter, the language available for debate on privacy does not offer many advantages in matters like these. Advocates of incremental ratcheting-up of surveillance would be quick to claim, in this case, that the proposed tracking system did no more than assure that pupils were where they were supposed to be. What possible objection could there be to steps that simply enhanced what had long been accepted as vital functions of all school authorities?

Faced with such challenges, privacy advocates often find little to rely on but a vague language of *balancing*. The advantages of automated attendance-taking, they would hold, must be "balanced" against the losses to privacy exacted by a system that follows every pupil, every moment.

No term in privacy debates has been used to more stultifying effect than this one. Let us agree that we should, and in fact do, somehow weigh conflicting goods in deciding how to treat personal information. But invoking the term "balancing" typically cuts short reflection at precisely the most difficult point—the question of how much "weight" to ascribe to conflicting values at stake in any such assessment. Just how bad are the "bads" involved in monitoring the every movement of school children? How compelling is the need to track movements of ordinary individuals in the hopes of spotting would-be terrorists? Such exacting questions should form the bases of any meaningful privacy debate. But we cannot hope to answer them until we have a way of ascribing weights to the things being balanced. And that is exactly where parties to privacy debates are most dramatically at odds.

Privacy advocates themselves have too often left these questions unaddressed. Their appeals rely heavily on the public's gut reactions against privacy losses, like those that served so well in the Sutter school case—instances

where many people instinctively ascribe more weight to privacy considerations than planners of data systems have done. But in less flamboyant cases, privacy spokespeople often find it difficult to give account of the essential goods and bads at issue.

Perhaps one reason is that what we rather sweepingly bracket as privacy concerns actually involve several distinct values.

One of these certainly is *aversion to dangers of repressive use* of personal data. Many privacy-watchers, whether on the political right or left, share an instinct of classic conservatives that unchecked concentrations of power are inherently suspect. Any system that monitors individual lives, and enables institutions to intervene in those lives, thus demands extreme prudence. Tracking the movements of pupils during the school day may appear an utterly benign activity. Probably, one imagines, no one will ever use the data so garnered in ways that could be prejudicial—probably. But in fact, it is not difficult to imagine how such uses might occur. Do pupils whose records show that they spent longer-than-average periods in the restrooms prove to have high rates of drug use or sexual misbehavior later in life? Do those whose overall attendance logs show long unaccounted-for periods of absence from class prove to have high arrest rates later on? If so, some would hold, perhaps school authorities should be compiling data from schoolyard surveillance and using it to track former pupils in their later lives.

Proponents of schemes like this are always optimists—at least for public purposes. The better informed that government or other major institutions are about people's lives, they hold, the more good they can do—in domains from public welfare to allocation of credit or insurance. The success of public health measures, or social welfare programs, or the consumer economy itself, it would seem, requires *access* to the lives of the people concerned. In this view, dangers of "abuse" of personal information simply require more careful controls of the data systems—like those associated with fair information practices—rather than refusal to create such systems in the first place.

Privacy advocates look skeptically on such confidence. Without necessarily questioning anyone's bona fides, they doubt that anyone is in a position to guarantee the fate of personal data, once compiled, into the indefinite future. Large surveillance systems are enormously expensive to create. The sunk capital that they embody normally outlives the intents of those who create them. And rollbacks of systems that successfully collect and compile personal data in forms lending themselves to institutional action are remarkably rare.

In the United States, we have seen how record systems created for benign bureaucratic purposes—tax collection and Social Security administration, notably—have been mobilized for political repression during the Nixon and Reagan administrations. Even more chilling were the events recounted in part II from the Nazi occupation of Holland—where frantic attempts were made to prevent census data on religious identifications from falling into the hands of the occupiers. No doubt these same records, under the originally intended circumstances, would have served only the most routine administrative uses. But the irreversibility of the effects when such potentials are put to destructive purposes should give everyone pause.

A second value that privacy advocates seek to defend is that of *moderating social inequalities.* Clearly the ultimate purpose of many surveillance systems is to allocate social advantages and disadvantages—ranging from consumer credit and social security benefits to the attentions of police and tax authorities. For many privacy advocates, a key aim is clearly to ensure that such allocations not become *too* punishing to those at the bottom—to ensure that surveillance systems not unduly reinforce or cumulate social disadvantage.

Most of us would endorse some version of such values in everyday behavior—for example, by purposefully "forgetting" about a friend's angry outburst or sexual indiscretion, if she seemed determined to put those moments behind her. Privacy advocates identify the same principle in their opposition to marketing credit scores to insurance companies, or to subjecting people to surveillance solely because they share the same religion or style of life as suspected terrorists. They support the virtues, one might say, of giving a second chance, of not condemning people on the basis of mere association.

But no one holds such values categorically—to the total exclusion of all competing social goods. No privacy advocate I ever encountered, for example, would insist that *no* records of criminal convictions should be kept, or that *no* use be made of such records for dealing with former criminals in the future. Nor have I heard the assertion that overt refusal to meet past credit obligations, or patterns of dangerous driving, should *never* have a bearing on people's future access to credit or driving privileges. For privacy advocates, these issues raise questions of what kinds of records get created, by whom, and of how sweeping the effects of "bad" records should be. The actual implications of privacy values in these connections, then, are matters of degree.

Here willingness to impose surveillance has everything to do with the degree of personal responsibility we attribute to those being monitored. Most

privacy advocates would not hesitate for a second to insist that those convicted of assaults on children should be tracked and prevented from gaining employment in schools, day care centers, or the like. Most would probably also agree that drivers with clear histories of frequent accidents and violations should experience some added costs and constraints in terms of insurance and, ultimately, licensing. By contrast, privacy advocates would be likely to resist monitoring of people's genetic histories so that insurance companies could charge them more for medical or life insurance. Most would resist efforts to subject children of convicted criminals to intensified surveillance, even if it could be shown that these children as a category showed higher rates of criminal behavior. Here a strong privacy position would demand that no one suffer the burden of special surveillance unless and until his or her own choices demonstrably warranted it. The fact that a given principle of discrimination is *efficient* from the standpoint of the institutions monitoring personal information hardly means that the principle is *just.*

But all of these principles have their limits—even for those who embrace them earnestly. Imagine that sophisticated analyses of surveillance databases revealed, say, that persons over six feet tall bearing a specific chromosome had a 99 percent chance of committing offenses against children if employed in their proximity? What if, for example, records showed that most such offenses in the past were committed by such people? Would such strong associations, however purely circumstantial, warrant categorical exclusion of such people from such employment? Such a policy would from all the (hypothetical, in this case) evidence be efficient—but it would certainly not be just. And collecting and screening such data for these purposes would amount to sweeping invasion of privacy, by any reasonable use of the term.

A third, still more subtle set of values pictures *privacy as basic to* ***personhood***. By this I mean to designate those principles, derived from Kant, that distinguish the way we treat human beings from the way we deal with other things—robots, animals, inanimate objects, and the like. Every ethical system makes this distinction—though often in quite different ways. Those with ethical objections to abortion or capital punishment, for example, do not dispute that these things may be effective means to forestalling the birth of, or getting rid of, troublesome people. They simply insist that *eliminating human life* should never serve as a means in these contexts. Such reasoning underlies many people's categorical objections to slavery, to the selling of sex or body

parts, or to experiments with human embryos. To treat human life in these ways, it is held, simply breaks down the barrier between norms guiding treatment of human beings and those governing other things. Similarly, many privacy advocates see certain unauthorized monitoring and use of personal information as eroding rights, held by every human being, to elementary dignity and independence.

Provocative examples are easy to concoct. Imagine a team of medical investigators convinced that a certain form of personal data could yield a dramatic medical breakthrough—but only if collected unobtrusively, without permission from the persons concerned. If secretly monitoring a group of research subjects' sexual behavior, for example, would yield a cure for cancer, would the evident invasion of privacy be justified by the value of the ultimate result? For utilitarians, the problem is no problem. Since the satisfactions of lives saved and sufferings alleviated by curing cancer outweigh the alleged indignities suffered by those under study, the venture is surely warranted. A Kantian rights perspective, by contrast, would forbid any such intervention. People's right to a significant measure of control over information on themselves, in this view, is as basic as their right not to be enslaved, or to control their personal property.

I suspect that nearly everyone accepts some element of rights reasoning in these matters—would agree, in other words, that some uses of personal information simply *go too far* in depriving people control over "their" data, even for the most useful of purposes. Such reactions would underlie objections to a world in which central authorities monitored every movement of every resident, or every purchase or transaction. Such measures could theoretically assure something close to total security and total respect for the law. But a world totally without privacy, and hence without the possibility of individual innovation or resistance to authority, would lack something essential. The costs would not just be reckoned individually, by those whose privacy was curtailed—but also in holistic losses to shared interests in defending a world where individual autonomy and even contrariness remain possible.

This value of privacy as essential to human dignity and personhood is perhaps the most difficult to articulate and defend in a world where utilitarian thinking often reigns supreme. What difference does it really make if the movements of schoolchildren are constantly tracked—if only their safety

and well-being are assured? What difference does it make if all electronic communications and search engine requests are subject to monitoring—if only such measures help secure us from terrorist attack? Why is it wrong for the credit industry to maintain total and unauthorized access to consumers' accounts—if the result is cheaper and quicker credit for the most profitable customers? Privacy advocates must answer that some claims on personal information are simply *bad things* in themselves, even when profitable or expedient.

This was among the principles invoked by CNIL, the French national privacy watchdog, when it ruled against tracking the movements of motorists for insurance purposes. The loss of privacy, the agency held, was a bad thing in itself—and the "bad" was not compensated by any corresponding good. But the notion that watching people too closely involves moral costs, even where those concerned offer no resistance, is a hard sell in our utilitarian public discourse.

These three ways of valuing privacy are logically distinct. One could theoretically uphold any one of them while remaining indifferent about the others. But in practice, they go together. People concerned about misuses of personal data for political repression are mostly inclined to defend privacy as an egalitarian value, and indeed as an end in itself. The several privacy values all appeal to those willing to incur real social costs in the interest of creating or defending a world that offers many opportunities for individual autonomy, innovation, and nonconformity vis-à-vis pressures to fit in. In the real world, all three of these values are implicated in that defense. And the rise of mass surveillance challenges all of them.

The task of privacy advocates is to preach the virtues of a looser, messier, less efficient, but more private world. What makes these arguments especially difficult is that privacy values are typically diffuse and holistic, whereas gains attained through more rigorous surveillance often appear strikingly specific. "If only *one life* can be saved from terrorist violence through monitoring of phone and e-mail traffic," one hears, or "if only *one child* can be protected against abuse by creating a DNA bank of all pupils and school staff," even blatantly privacy-invading measures are held to be justified. Against such urgent and often highly personalized appeals—invoking, for example, names and images of children who might hypothetically have been saved from harm,

if only more intense surveillance had prevailed—privacy values may ring abstract and uncompelling.

But in fact, we accept such trade-offs in many realms of public life. Many policies put individuals at danger in pursuit of diffuse and abstract public values. Physicians administer vaccines and other medicines to large populations, knowing that serious side-effects are certain in very small numbers of cases. Designers of highways follow norms requiring, for example, that curves not be too sharp, in order to minimize accidents. But no one would insist that such designs eliminate *all* dangers to drivers—for example, by proscribing even gentle curves in road designs. Similarly, limitations on the prerogatives of law enforcement agencies—for example, habeas corpus or protection from self-incrimination—surely permit many dangerous felons to go free, in some cases to commit further crimes.

We accept such limitations, with the inevitable tragedies that ensue, to protect values that are often abstract and diffuse—those of not living in a police state, for example. Privacy advocates must invoke similar arguments in response to the steady stream of new surveillance activities that constantly confront us—from the monitoring of our search engine requests, to the archiving of our DNA, to unrestricted tracking of our cell phone use and movements.

Moreover, we permit many utterly deplorable social evils to go uncontrolled, simply because measures necessary to address them would require intolerable invasions of privacy. We enact laws—quite properly, in my view—to monitor and curtail domestic violence of a physical sort. But we do not generally attempt to monitor and repress *symbolic* violence or emotional cruelty within families. A moment's reflection reveals that spouses and children suffer many such wounds at the hands of family members, wounds apt to be far more destructive and long-lasting than physical violence—denial of love, systematic attacks on self-respect, long-lasting humiliation, etc. Certainly preventing such wounds would be a good thing—if it could be accomplished without invading certain private domains. Few if any would advocate the far-reaching surveillance that would be necessary to monitor the everyday content of family communication in order to identify and repress symbolic cruelty in this sphere. It's not that the stakes aren't high—they could hardly be higher—or that the suffering isn't real and long-lasting. It's that we hold the value of leaving the inner lives of families free of such monitoring so great that we are willing to tolerate even terrible evils within the family.

Conclusion: Where Do We Go from Here?

The loss of control over information about one's self often seems seamless and incremental—a slippery slope affording no sticking point for concerted resistance. Like Christopher Robin, we see ourselves on a shrinking island, losing ground to swirling pressures on privacy. How can we best respond?

Begin with a few *negative* conclusions.

First, the fair information practices that constitute the consensus response to surveillance don't address the most pressing issues. At best, they block incorporation of certain forms of data into surveillance systems and provide tools for individuals and public opinion to review and react to the workings of such systems. But they don't help answer that most crucial question: do we want to make the trip in the first place? And many of the most privacy-invasive activities remain beyond the reach of fair information practices—where they are bracketed as "investigative" activities by law enforcement or counter-espionage agencies.

Some alleged privacy codes actually make matters worse—as in the American federal legislation forbidding individual states to adopt more serious protections for data subjects than those afforded at the national level. Indeed, when the last vestige of control over personal information is finally wrested from the last, recalcitrant "private" citizen, the action will doubtless be taken in the name of privacy protection. Privacy codes making demands for personal data more lawful, more open, and more accountable have all too often provided a Trojan Horse for egregiously privacy-invasive practices—for example, credit reporting regulations that afford ordinary consumers no option to "just say no" to monitoring of their current accounts.

True, privacy isn't everything; there are times when even the most earnest privacy advocates will be prepared to forswear it for competing values. But when this occurs, we need to be utterly candid about what is lost. One can make a case for precisely targeted phone- or e-mail-tapping in response to clear and present dangers of terrorist acts or other life-threatening emergencies, for example. But suggesting that massive surveillance sweeps like the Bush administration's NSA surveillance of millions of Americans' telecommunications transmissions can somehow be carried out with respect for privacy does violence to the English language. It brings eerie reverberations of the Party slogans in *1984:* "War is Peace; Freedom is Slavery; Ignorance is Strength."

Second, it won't do to blame "Technology" or other nonhuman agencies for the pressures on privacy. The very technologies now mobilized for privacy-eroding activities could just as well support privacy-friendly practices, if only those in charge approved. In fact, the technological problems of protecting personal data are child's play compared to the sophisticated measures devoted to creating, collecting, transmitting, and using personal data mobilized by surveillance interests. The problem is that sponsors of prevailing information technologies are institutions viewing their mandate as *doing better* in dealing with people by *knowing more* about them. The alternatives to such aggressive uses of personal information are often technologically easy—consisting often of simply not amassing personal data in the first place. What is excruciating is the political, economic, and social costs of renouncing institutional dreams of mastery over human affairs.

Third, there is no reason to conclude that privacy is somehow already definitively "lost." One often hears such laments, even from observers who ought to know better—as though all personal information had somehow irreversibly escaped from individual control, like the troubles from Pandora's box. But in fact, personal data are loose only insofar as their capture and use are held legal and legitimate. If the unauthorized selling of "background reports" on private citizens subjected the sellers to court judgments like those handed down to victims of cigarette smoking or defective drugs, the practices would quickly cease. If snooping into library patrons' reading choices subjected investigators to lawsuits or prosecution, we would see much less of it. Better still, if we could persuade institutions to concentrate as much on *avoiding* collection of personal information as they now do on finding new ways to collect, store, and use it, we would quickly start to inhabit a more privacy-friendly world.

In fact, many of the most sought-after personal data are highly perishable commodities. Even if once discovered, their value for surveillance purposes often declines quickly. Data on income and current accounts for credit determinations, for example, or data on current associations and activities in criminal investigations often has a brief shelf life for surveillance purposes. Our problem is not that our data have lifetimes beyond human control. It is that those in control are free to exploit those data as long as they care to.

Fourth, it is usually futile to hope for either a technological fix or its political equivalent—some intervention that would magically forestall "invasion

of privacy" while still fostering "free flow" of personal data. All too often, the latter are simply two manifestations of the same phenomenon. The problem is precisely that institutions' quest for ever-finer discrimination in dealing with people can only be satisfied by appropriating and using more and more detailed personal data. And though we deplore the invasion of privacy, we seek all sorts of performances from institutions that fuel it—from easy credit to crackdowns on tax evaders to pursuit of terrorists. Candor requires frank recognition that unlimited zeal in pursuit of these efficiencies is simply not compatible with meaningful privacy protection.

This last admission, I have argued, does not come easy to us moderns. Aware of it or not, we are all heirs to potent Enlightenment ideas in matters relating to *control.* If knowledge is good, and informed action preferable to the alternative, why shouldn't we expect institutions of all kinds to maximize their grip on the lives of those they deal with? If government and private organizations are pursuing what are publicly recognized as legitimate ends, why shouldn't they do so as efficiently as possible?

Privacy advocates must enter an unequivocal, emphatic response to such questions: if we're serious about privacy, we can't *afford* to have institutions keep such a tight grip on human affairs. In any long-term view, the only meaningful strategy for privacy protection is to bear the significant costs of knowing less about people's lives.

Privacy advocates have hurt their cause by acquiescing to, or even promoting, notions that privacy is somehow compatible with relentless efficiency maximization in government and private institutions. True, ingenious compromises are sometimes possible between surveillance interests and privacy values. There are, for example, cryptographic billing systems that debit bank and credit card accounts without creating permanent records of the parties and amounts of the transactions. But the broad force underlying pressures on privacy as detailed in this book has been the appetites of institutions to generate and record *more* such detailed personal data, not less. Privacy-friendly technologies are eminently workable—but only to implement willingness to amass less personal data.

When asked what his activists ultimately wanted, the early trade unionist Samuel Gompers is famously said to have replied simply, "More!" Serious privacy advocates could do well to embrace the opposite slogan: "Less!" They

need to advocate urgent programs to identify, and to help implement, ways of dealing with people that simply require less personal data from the start. Instead of investing in more sophisticated and ingenious databases for predicting consumer choices, political inclinations, credit use, tax compliance, and the like, institutions should be investing in less information-intensive alternatives to current practices. We need, in short, to reconfigure institutions as *blunter instruments* for achieving the purposes we attribute to them, so that they may require less personal data.

Such alternatives need not involve Luddite-style rejection of all institutional monitoring of private life. But they do demand systematic determination to deal with people without recourse to all the personal data that might be useful.

This would not mean renouncing all conveniences of consumer credit. But it would mean expecting credit grantors to make do with less personal data than American-style credit determinations now demand. It would not mean refusing to compile information on persons convicted of serious crimes. But it might mean declining to monitor persons merely suspected of criminal tendencies, or those convicted of lesser crimes—even when such renunciation clearly entailed risk. It would not mean turning away from efforts to identify and track terrorists. But it would mean curtailing the more sweeping intakes of personal data now collected on speculative prospects that they might, indirectly, contribute to the strangely named War on Terror. It need not even prevent market researchers and advertisers from using personal data to concoct new products and new ways of publicizing them. But it would require that consumers have absolute, informed choice over such uses.

Obviously these strategies would represent a turn away from what some might consider the modernist project of ever-extending purposeful control over the world. But I hold that they would reflect reasoned judgment—consistent with subtler consideration of Enlightenment values—that control over both natural and human processes has to have limits. Such thinking is now widespread—for example, in environmental issues. Comte, of course, saw all of nature as endlessly ripe for human analysis and exploitation. But a humbler view suggests that some forms of mastery over natural processes simply go too far. Unlimited use of antibiotics may undermine resistance to the diseases we most fear; unlimited intervention in the genetic makeup of life may alter ecosystems in undesirable and irreversible ways; unlimited use of fossil fuels creates climate changes with effects we only now begin to foresee.

Anyone attentive to present-day discourse on the public role of science and technology can extend this list at length. More and more, thoughtful opinion is shifting to the conviction that wisdom lies in not pressing visions of control to their limits.

Proposals to apply this thinking to the use of personal data trigger some predictable rejections. Skeptics inevitably cite the costs of *failure* to control—innocent children who might have been saved from crimes, if only all passersby had been photographed on videotape; terrorists who might have been caught, if only all e-mails had been captured and analyzed; emergency-room patients who might have been saved, if only computer chips containing their medical histories had been implanted under their skin.

These concerns are anything but negligible. Indeed, privacy advocates inevitably—and quite legitimately—differ on where specific dangers or losses are so acute or immediate as to justify even intrusive forms of surveillance. Are there some notably dangerous locations that warrant monitoring by video cameras? Are there some people who *should* carry institutionally relevant personal information in subcutaneous data chips? What categories of convicted felons should be prevented from *ever* working in proximity to children? Even those deeply attached to privacy values—perhaps they especially—are bound to differ in terms of the goodness of the goods, and the badness of the bads, that they attribute in such calculations.

But if privacy advocates do not always agree on the acceptability of specific uses of specific personal data, they might well agree on some ground rules for adjudicating such questions in the public forum. Above all, they might join in calling for new public understandings of the boundaries between public and private. They might insist, for one thing, that all personal data that are "public" at any one moment and for any one purpose must not ipso facto be considered usable for any and all purposes. Or to put it a bit differently, privacy advocates should insist that *mass surveillance* be regarded as a distinctive phenomenon—one warranting special vigilance and restraint. We need to revise assumptions, especially widespread in the United States, that all personal data that is obtainable must be usable for institutional recording and decision making.

No one would want to live in a world without a "public realm." That would mean civic life without the possibility of comment and reflection on

the actions of those around us—from public officials to neighbors to entire communities. Public deliberation, political campaigns, journalistic treatments of human interest, and a host of life-giving processes thrive in a desirable tension between openness and privacy in this domain. For these reasons, even the strongest of privacy advocates should defend the availability of most publicly enacted data for purposes of public discourse.

But mass surveillance—systematic monitoring to support institutional action toward those monitored—has to be different. Harvesting personal data wherever they are publicly available and converting such data to institutional use multiply the effects of the information. The ridiculous ease of compiling data previously evanescent or unavailable challenges us to re-think our very ideas of what is public and private.

The new default condition for public policy should be: no government surveillance without meaningful individual consent or legislative authorization. Some version of this principle has at least received lip service in many countries' privacy codes, though it has often been circumvented. If taken seriously, it would mean that even "public" information—data that might be available to any witness in a public setting—must require express authorization or consent for incorporation into surveillance systems. Thus the mere fact that government agencies find it feasible to obtain data on citizens' supermarket purchases, cell phone use, political expressions, or the like would not suffice to make such collection legal for purposes of institutional surveillance.

For government surveillance, elected officials should be required to authorize each appropriation of personal data in every government surveillance system. Such stipulations would need to name the specific forms of data to be collected—for example, passport applicants' place of birth, but not every place they have ever lived. Blanket authorizations to agencies to collect "any and all data necessary" to achieve their surveillance purposes should be reserved for authentic, short-term emergencies.

The aim would be to *politicize* the working and extension of surveillance—in the positive sense that elected officials would become accountable for the demands on personal data ensuing from their legislative actions. The idea is to ensure that mass surveillance no longer be a taken-for-granted bureaucratic recourse, taken solely at the discretion of government institutions. Even investigative agencies should require specific legislative authority for systematic personal data collection and use. Thus activities like the mass analyses of

ordinary citizens' phone records recently carried out by the NSA in the United States could never go forward without elected representatives' taking responsibility for them.

In the private sector, a parallel precept should apply: no use of personal data for institutional surveillance without meaningful, informed consent from the individual.

Taking this principle seriously would amount to a revolutionary overthrow of practices now prevailing in the United States, and to a lesser degree elsewhere. In America, private entrepreneurs often defend their sweeps of court records, telephone logs, credit card sales, and other sources as recourse to "public" information—and hence beyond challenge on privacy grounds. The idea seems to be that such data, once public for any purpose, must be subject to re-use and commercialization into the indefinite future. Surely this is a rationale for which C. Wright Mills's term "crackpot realism" could have been invented.

Taking privacy seriously would entail that any commercialization of personal data, either from government files or private-sector records, would require active assent from the individual concerned. In the jargon of privacy-watchers, "opt in" would be the rule: no commerce in personal information from any source would be possible without adequate notice and explicit consent from the individual. The result would be to secure individual veto power over commerce in personal information ranging from credit account data to information gleaned from tax returns and prescription sales, to that from periodicals' subscription lists and hotels' guest lists—all of which are now subject to commercial exploitation in the United States.

Note that this stricture would not apply to dissemination of personal data for public discourse and comment. From journalism to gossip, uses of personal data not involving sale or trade would require no consent. But for *commerce* in personal information—activities aimed at creating value for institutional decision making on the people concerned—opt-in requirements would be universal.

Such a change would amount to the creation of a new, privacy-friendly right: a universal *property right* over *commercial exploitation of data on one's self.* Ordinary consumers would *own* data on themselves, much as they might own mineral or water rights to real property. This new right would grant

everyone prerogatives that American law now only confers on celebrities—the right to control trade in the use of one's own name. The ethical basis for such a right is all but self-evident: those whose lives create possibilities for commerce in information on themselves should have the ultimate say over its commercialization.

Absent express consent, such a right would categorically block unauthorized collection and trade in personal data for commercial purposes. By doing nothing, one would avoid exposure to all such activities. "Positive" credit reporting—that is, routine monitoring of all consumers' credit accounts—would be impossible, for example. The blanket "consents" required for this sort of scrutiny as conditions for access to credit in the first place would no longer be recognized. Nor would consent to commercialization of one's data be a valid condition for access to any other relationship.

Of course, those who actually prefer to have their data commercialized would be free to grant permission for such use. By so doing, they would place themselves more or less in the situation of all American consumers today.

A third possibility would also be implicit in any such right. People could discriminate in the commercial uses that they permit of their data—which would now really be "theirs." They could, if they wished, insist on *compensation* in exchange for commercial use of information on themselves. And they could stipulate different conditions for release of different forms of personal information for different purposes.

Some might want to grant permission for direct marketing use of data on themselves, say, to nonprofit organizations but not to corporations. Others might wish to set high fees for use of their data by all organizations that do not publicly subscribe to Christian principles. Still others might grant rights to report their data to prospective creditors, but only those whose credit services they might actually wish to take advantage of. The new right would open a wide array of such possibilities—including always the default condition of doing nothing and thereby foreclosing any and all commerce in data on one's self.

For consumers inclined to discriminate in release of their data—neither refusing all such use, nor offering it *gratis* to all interested parties—a new industry would probably grow up to implement the new right. It would record and enforce individuals' instructions for commercial use of their data, much as ASCAP and BMI represent the interests of composers in the performance of their work. These data rights agencies would maintain records on

the uses each consumer authorized for his or her data and would be quick to act against unauthorized exploitation of such data. Such data piracy would be a tort, and would expose users to both individual and class actions, leading to both compensatory and punitive damages. A corollary right would enable anyone to know the origins of data used commercially on himself or herself. Thus individuals and their institutional representatives would become the first and most potent line of defense against misappropriation of their personal data.

A right like this would hardly be a panacea for exploitative commercial privacy invasion. It would require strong legal context.[20] To minimize bad consequences of ill-considered grants of one's data rights, for example, permission for any specific use should be valid only for short periods—say, six months. Further, to prevent organizations from applying overweening inducements to individuals to yield their data, compensation should only be in cash. This would block pharmaceutical corporations, for example, from presenting websites offering advice on particular diseases but refusing access to the site to those who did not wish to have their data used for commercial prospecting.

Many readers, I imagine, will find such schemes for according citizens veto power over commercialization of "their" data transparently reasonable. Yet this thinking, if taken seriously, will trigger epidemic apoplexy among the industries now appropriating such data as their basic raw material—without constraint and without compensation to consumers. "What?" their spokespeople will demand; "You mean people could censor the negative data out of their credit records or insurance reports? Why then there would be no way of rewarding people with *good* records! Sellers of credit and insurance will have no bases for discrimination over prices and availability of their offerings."

Certainly there are instances in which the public interest requires availability of specific data to be legally mandated for commercial use. Seriously delinquent credit accounts, bankruptcies, and multiple insurance claims for the same forms of loss, for example, should be recorded as red flags to prospective future creditors or insurers. The public interest in these forms of discrimination justifies compilation of these data.

But absent such clear and compelling public interest, ordinary consumers should always have the option of keeping their account histories and other commercial dealings off the surveillance radar. Consumers persuaded of the need to build a good credit record could authorize reporting of a specific

account at the moment that account was opened—provided only that such permission could never be a condition for access to the account in the first place. Those who later preferred to seal an account so compiled from commercial scrutiny, for example, because of billing disputes with the creditor, would be free to do so—perhaps at the cost of noting the existence of the sealed account on some public record.

The immediate result of such privacy-friendly ground rules would be that commercial interests of all kinds would be required to make their attentions attractive to consumers. Consumers insensitive to such attractions would never grant permission to have their accounts and consumption habits monitored—and would accordingly accumulate no records in what would amount to the "default condition." To be sure, credit applicants without records, or those with many records of accounts sealed at their own request, might find themselves at a disadvantage, compared to those with long listings of favorable accounts—accumulated, necessarily, at the consumers' discretion. But competition for consumers' business, as in France and Australia, would provide a continued flow of credit opportunities.

Perhaps the most important benefit of establishing a right like this would be cultural. The idea that businesses—from direct advertisers to insurance companies—should have to pay to use our personal data for their own gain has an intuitive logic than everyone can understand. A right like this, if implemented with the proper supporting guarantees, would help convince people that the loss of control over their personal data is not irrevocable and that privacy was not an outdated concept in an information-oriented world. In short, it would help curtail the fatalism that currently dogs many Americans' expectations of privacy.

That fatalism, I am convinced, constitutes the gravest obstacle to meaningful privacy protection.

In the end, questions of what institutions, policies, or legal forms we adopt to that end may matter less than the attitudes and understandings with which we approach the task. Whether we place our faith in individual rights of action like those envisaged above, for example, or in legislation simply restricting use of specific forms of personal data, may not be the most important thing. What is indispensable is frank recognition of where and how pressures on privacy arise—and what is required to countervail against them. Notions that our

privacy is being lost to vague forces of "technology," "the information society," or other mysterious nonhuman agencies are particular distractions in this connection. These outstandingly bad ideas foster lazy conclusions that the only alternative to endless erosion of privacy is consignment to some sort of informational Stone Age. We know better. Meaningful, active defense of privacy is possible, even in a world that runs on information. But such defenses can never be cost free.

Only by choosing to accept real costs can we hope to fashion a world that keeps a place for privacy in an otherwise information-rich environment. That means accepting that more privacy will often mean less efficiency—less profit, less convenience, more institutional waste, and sometimes even less safety and justice. Inevitably, such costs will fall more heavily on some interests than others, but we would all experience them to some degree. Like proponents of energy conservation, privacy advocates should be frank about insisting that everyone will share both the costs and benefits of less information-intensive modes of institutional action.

The issues involved are ultimately ethical and political, not technological. If we determine to do so, we can readily implement systems that *place the burden of justification on those who would create personal data systems in the first place;* that *grant substantial control over data processes to the individuals described in them;* that *ensure quick elimination of personal information from data systems, once their immediate purposes are served;* that *provide no-cost options for anonymous transactions as an alternative to self-identification;* that *define the purposes of data collection in terms of the interests of individuals rather than of organizations;* and that *limit the amount and variety of personal data allowed to bear on determinations of how organizations will treat individuals.*

Such goals are eminently feasible. But taking them seriously requires that we resolve to leave some forms of control over human affairs untried. Such renunciation runs against the grain of some very deep-rooted public expectations. But so does the destruction of privacy. No one really wants to live in a world where all recordable personal information is effortlessly captured and shared among established institutions. Even the promise of total security and efficiency would not, for most of us, make such a world worth the bargain. I have sought to show that this is exactly the bargain we have to contemplate.

Institutions, wrote political philosopher Karl Popper, are like fortresses: they must be both well designed and well defended. Privacy protection

measures are just such institutions. Without an unsentimental vision of the pressures on privacy, and the political will to confront them, the most ingenious legislation and policy-making will avail little. It is not easy to opt for a messier, less efficient, more dangerous and unpredictable world as the price of authentic privacy. But the alternative is infinitely worse.

This page intentionally left blank

Appendix: Levels of Use of Consumer Credit Australia–USA Comparisons

Australia	USA
Credit cards per adult member of population (2005)[1]	
0.74	2.81
Debit cards per adult member of population (2005)[2]	
1.54	0.97
Unsecured consumer credit per adult member of population (2005)[3]	
$AU6635.*	$US9237
Unsecured consumer credit as per capita percentage of GDP (2005)[4]	
12.4%	17.5%
Percentage of homes owned by occupants with mortgages (2003)[5]	
50.1%	58.7%

*$AU1.00 = approximately $US.81 in 2005

Sources:

[1]www.rba.gov.au/www.abs.gov.au
www.census.gov/posest/states/NST-ann-est.html

[2]Same sources as for [1] above

[3]www.rba.gov.au
www.abs.gov.au
www.federalreserve.gov/releases/g19/current/default.htm

[4]Australian consumer credit: same sources as for [3] above
www.rba.gov.au/Statistics/BulletinG10hist.xls
U.S. consumer credit: same sources as for [3] above
www.federalreserve.gov/

[5]www.abs.gov.au/Ausstats/abs@.nsf/
www.census.gov/hhes/www.housing/ahs/ahs03/ahs03.html
All sources viewed April 2006.

This page intentionally left blank

Notes

Part I. The Making of an Issue

1. News story by Dan Vukelich in the *Albuquerque Tribune*, 24 July 1997.
2. Roger Clarke article in *Privacy Journal* (2005), vol. 31, no. 9.
3. Charles Fried, "Privacy" (1968).
4. Thomas Gregor, "Exposure and Seclusion: A Study of Institutionalized Isolation Among the Mehinaku Indians of Brazil" (1980), p. 83.
5. Helen Nissenbaum persuasively makes this point in "Protecting Privacy in an Information Age: The Problem of Privacy in Public" (1998).
6. Richard Posner, "The Right of Privacy" (1978), p. 404.
7. Samuel Warren and Louis D. Brandeis, "The Right to Privacy" (1890).
8. James B. Rule, *Private Lives and Public Surveillance* (1973), ch. 1.
9. See, for example, Langdon Winner, *Autonomous Technology: Technics-Out-of-Control as a Theme in Political Thought* (1977).
10. E.g., Richard H. Rovere, "The Invasion of Privacy (1): Technology and the Claims of Community" (1958); Vance Packard, *The Naked Society* (1964); Myron Brenton, *The Privacy Invaders* (1964).
11. U.S. Department of Health, Education and Welfare, *Records, Computers and the Rights of Citizens* (1973), pp. xx–xi.
12. *Records, Computers and the Rights of Citizens*, pp. 6–7.

13. When I speak of "national privacy codes," I refer to legislation establishing broad privacy rights over many categories of personal data, rather than measures governing specific *forms* of personal data, like credit records. Thus the U.S. Privacy Act of 1974, applying to administrative records held by federal agencies, counts as such a code, but not the Fair Credit Reporting Act.
14. For thorough discussion of such differences, see David Flaherty, *Protecting Privacy in Surveillance Societies* (1989); Colin Bennett and Charles Raab, *The Governance of Privacy* (2003).
15. See, for example, David H. Flaherty, *Protecting Privacy in Surveillance Societies* (1989), p. 305; Colin Bennett, *Regulating Privacy* (1992), p. 199; Paul Schwartz and Joel Reidenberg, *Data Privacy Law* (1996), pp. 205–14.

Part II. Government Surveillance

Epigraph. Quoted in David J. Seipp, *The Right to Privacy in American History* (1978), p. 108.

1. James Scott, *Seeing Like a State; How Certain Schemes to Improve the Human Condition Have Failed* (1998), ch. 1.
2. Frits W. Hondius, *Emerging Data Protection in Europe* (1975), p. 187.
3. See Sidney Ratner, *Taxation and Democracy in America* (1980), pp. 324ff.
4. John Chommie, *The Internal Revenue Service* (1970), ch. 1.
5. Alan Westin and Michael Baker, *Databanks in a Free Society* (1972), p. 33.
6. U.S. Privacy Protection Study Commission, *Personal Privacy in an Information Society* (1977), pp. 103–6 and 356–63.
7. Paul Schwartz and Joel Reidenberg, *Data Privacy Law* (1996), p. 64.
8. Morton H. Halperin, Jerry J. Berman, Robert L. Borosage, and Christine M. Marwick, *The Lawless State: The Crimes of the U.S. Intelligence Agencies* (1976), pp. 122–31.
9. U.S. Congress, *Legislative History of the Privacy Act of 1974* (1976), p. 9.
10. Privacy Act of 1974, Section 3 (b).
11. Privacy Act of 1974, Section 3 (a)(7).
12. James Dempsey, personal communication, 13 December 2006.
13. U.S. Senate, Select Committee to Study Governmental Operations, *Intelligence Activities and the Rights of Americans, Book II* (1976), p. 290, emphasis in original.
14. Morton H. Halperin et al., *The Lawless State* (1976), pp. 251–53.
15. Peter Swire, "The System of Foreign Intelligence Surveillance Law" (2004), p. 1311.
16. Quoted in Peter Swire, p. 1321.
17. Quoted from the 1978 statute by Peter Swire, p. 1325.
18. Peter Swire, p. 1329.

19. See the Court's annual *Report to Congress*: www.fas.org/irp/agency/doj/fisa/#rept, viewed 14 July 2006.
20. Both quotations from Peter Swire, p. 1325.
21. Peter Swire, p. 1327.
22. For fascinating insight into the pre-9/11 determination of top Bush administration planners to redress limitations on presidential power that took root in the Watergate era, see Jane Mayer, "The Hidden Power: A Secret Architect of the War on Terror," *The New Yorker*, 3 July 2006.
23. Peter Swire, p. 1330.
24. Ibid., p. 1331
25. Ibid., p. 1333.
26. Alison Leigh Cowan story in *The New York Times*, 21 March 2006.
27. *Privacy Times*, vol. 26, no. 8, 17 April 2005, p. 1.
28. *Privacy Journal*, vol. 32, no. 3, January 2006.
29. Department of Justice memo, 27 January 2006, cited in Wikipedia.
30. Regulation of Investigatory Powers Act 2000, Section 6(3).
31. Ian Brown, "Communications Surveillance Briefing," Foundation for Information Policy Research, 18 August 2003. www.fipr.org/030818ripa.html, viewed 29 June 2006.
32. Benjamin Goold, *CCTV and Policing; Public Area Surveillance and Police Practices in Britain* (2004), pp. 1–2.
33. NACRO. "To CCTV or not to CCTV? A review of current research into the effectiveness of CCTV systems in reducing crime" (June 2002). Available from www.nacro.org.uk/data/briefings/nacro-2002062800-csps.pef. Viewed 17 July 2006.
34. Foundation for Information Policy Research. *UK Information Commissioner Study Project: Privacy and Law Enforcement. Combined Papers no 1 and 2: Technology and its effect on privacy & law enforcement* (February 2004), page 41. Available from http://www.cs.ucl.ac.uk/staff/I.Brown/ple-ico.pdf. Viewed 9 December 2006.
35. BBC News story, 13 March 2006, on http//news.bbc.co.uk/go/pr/fr/-/1/hi/England/London/4800490.stm. Viewed 17 July 2006.
36. Nigel Waters, "Government Surveillance in Australia" (2006), pp. 11–12.
37. Senate Legal and Constitutional Legislation Committee: Report into *Provisions of the Telecommunications (Interception) Amendment Bill 2006,* p. 60.
38. *Telecommunications (Interception) Amendment Act 2006,* No. 40, 2006, Schedule 1.
39. Australian Securities and Investment Commission, Policy Statement 175.93.
40. Nigel Waters, "Government Surveillance in Australia" (2006), p. 5.
41. CTV.ca News, 17 February 2006.

42. See http://privcom.gc.ca/media/nr-c/2003/submission_nid_030918_3.asp; viewed 14 December 2006.
43. Jennifer Stoddart, Privacy Commissioner of Canada, "Position Statement on the *Anti-Terrorism Act,"* Submission of the Office of the Privacy Commissioner of Canada to the Senate Special Committee on the *Anti-Terrorism Act*, 9 May 2005.
44. Law of 10 July 1991, Article 3.

Part III. Personal Data in the Marketplace

Epigraph. www.transunion.com/corporate/aboutUs/whoWeAre/publicPolicies.page, viewed 11 November 2006.

1. Paul Schwartz and Joel Reidenberg, *Data Privacy Law; A Study of United States Data Protection* (1996), pp. 321–22.
2. See E. Volokh, "Freedom of Speech and Information Privacy: The Troubling Implications of a Right to Stop People from Speaking About You" (2000).
3. Robert Ellis Smith, *War Stories, Volume II: Accounts of Persons Victimized by Invasions of Privacy* (1997), pp. 52–53.
4. Evan Hendricks, *Credit Scores and Credit Reports*, Second Edition (2005), pp. 251–52.
5. Ibid., p. 231.
6. Ibid., pp. 229–30.
7. Robert Gellman, "Trafficking in Health Information: A Widespread Problem," Version 1.3, 10 July 2006, available from Robert Gellman, Privacy and Information Consultant (2003).
8. University of Miami, Miller School of Medicine, Privacy/Data Protection Project. 2002-05. "Privacy Standard/Rule (HIPAA)." http://privacy.med.miami.edu/glossary/xd_privacy_stds.htm. Viewed 16 June 2006.
9. Rob Stein, "Medical Privacy Law Nets No Fines," *The Washington Post*, 5 June 2006, p. A01.
10. www.abika.com/Report/Samples/Backgroundcheck.htm. Viewed 16 June 2005.
11. Australian Government, Office of the Privacy Commissioner, *The Review of the Private Sector Provisions of the Privacy Act 1988* (March 2005), Section 4.3.
12. E-mail communication from BaycorpAdvantage, 15 December 2004.
13. Personal Information Protection and Electronic Documents Act (PIPEDA), 2000, Part 6, Schedule 1, Section 5. This law was updated in 2006.
14. Story by Jonathon Gatehouse in *MacLean's*, 21 November 2005.
15. "On the Data Trail: A Report on the Canadian Data Brokerage Industry," Canadian Internet Policy and Public Interest Clinic (2006), p. 14.

16. "On the Data Trail," p. 7.
17. PIPEDA Part 6, Schedule 1, 4.2.4.
18. "On the Data Trail," p. 26.
19. HSBC application form, collected from a London branch bank, May 2004.
20. Commission Nationale de l'Informatique et des Libertés, *Les Libertés et l'Informatique: Vingt Deliberations Commentées* (1998), pp. 107–12.
21. *Les Libertés et l'Informatique*: *Vingt Deliberations Commentées*, p. 111.
22. Directive 95/46/EC of the European Parliament and of the Council of 24, October 25, on the protection of individuals with regard to the processing of personal data and on the free movement of such data, *Official Journal L 281, 23/11/1005. P. 0031-0050,* Article 21, 1.

Part IV. The Future of Privacy

1. *Privacy Times* (11 October 2005), p. 3.
2. Colin Bennett, Charles Raab and Priscilla Regan, "People and Place: Patterns of Individual Identification within Intelligent Transportation Systems" (2002), p. 128.
3. U.S. Department of Health, Education and Welfare, *Records, Computers and Rights of Citizens* (1973), p. 5.
4. Directive 95/46/EC of the European Parliament and of the Council of 24 (October 1995).
5. "Civil Liberties Issues in Public Databanks" in Alan F. Westin, ed., *Information Technology in a Democracy* (1971), p. 310.
6. James Dempsey, personal communication (13 December 2006).
7. Associated Press (23 May 2005).
8. David J. Phillips, "Cell Phones, Surveillance and the State" (2004), p. 57.
9. Statement of Louis J. Freeh, Director, Federal Bureau of Investigation, before the Subcommittee on Technology and the Law of the Committee on the Judiciary, U.S. Senate, and the Subcommittee on Civil and Constitutional Rights of the Committee on the Judiciary, House of Representatives (18 March 1994).
10. Quoted in *Privacy Journal* (March 2006), p. 7.
11. Edgar Whitley, research coordinator. *The Identity Project: An Assessment of the UK Identity Card Bill and Its Implications*, *Interim Report* (2005).
12. James B. Rule, *Private Lives and Public Surveillance* (1973), pp. 38–40.
13. Associated Press story by Leslie Miller (28 June 2003); Jeffrey Rosen, *The Naked Crowd* (2004), Prologue.
14. U.S. House of Representatives. *The Computer and the Invasion of Privacy* (1966), p. 6.

15. U.S. Department of Justice, Federal Advisory Committee on False Identification, *Report on the Criminal Use of False Identification* (1976), pp. 73ff.
16. Gary Marx, "Soft Surveillance: Mandatory Voluntarism and the Collection of Personal Data" (2005).
17. Jerry Kang, "Information Privacy in Cyberspace Transactions," *Stanford Law Review* (1998), vol. 50, no. 4, April, p. 1249.
18. *Ornet*, story by Arnaud Devillard (22 December 2005).
19. Alfred J. Kahn, "The Tyranny of Small Decisions"; following quotation from page 30.
20. More detail of the legal and procedural architecture required to implement this right is given in James B. Rule, "Toward Strong Privacy: Values, Markets, Mechanisms, and Institutions" (2004).

Bibliography

Agre, Philip E., and Marc Rotenberg, eds. 1997. *Technology and Privacy: The New Landscape.* Cambridge, MA: MIT Press.

Arendt, Hannah. 1951. *The Origins of Totalitarianism.* New York: Harcourt, Brace and Company.

Bennett, Colin J. 1992. *Regulating Privacy: Data Protection and Public Policy in Europe and the United States.* Ithaca, NY: Cornell University Press.

Bennett, Colin, and Rebecca A. Grant, eds. 1999. *Visions of Privacy: Policy Choices for the Digital Age.* Toronto: University of Toronto Press.

Bennett, Colin J., and Charles D. Raab. 2003. *The Governance of Privacy: Policy Instruments in Global Perspective.* Burlington, VT: Ashgate.

Bennett, Colin, Charles Raab, and Priscilla Regan. 2002. "People and Place: Patterns of Individual Identification within Intelligent Transportation Systems," in David Lyon, ed., *Surveillance as Social Sorting: Privacy, Risk and Automated Discrimination.* New York: Routledge.

Bigo, Didier. 1996. *Police en Reseaux; l'experience europeenne.* Paris: Presses de la Fondation Nationale des Science Politiques.

Brenton, Myron. 1964. *The Privacy Invaders.* New York: Coward, McCann.

Brown, Ian. 2006. "UK Government Powers to Access Personal Information." Research Report, University College London.

Bunyan, Tony. 1976. *The Political Police in Britain.* New York: St. Martin's Press.

Canadian Internet Policy and Public Interest Clinic, Faculty of Law, University of Ottawa. 2006. "On the Data Trail: A Report on the Canadian Data Brokerage Industry."

Carey, Peter. 2004. *Data Protection: A Practical Guide to UK and EU Law,* second edition. Oxford: Oxford University Press.

Chommie, John C. 1970. *The Internal Revenue Service.* New York: Praeger Publishers.

Clarke, Roger. 1988. "Information Technology and Dataveillance." *Communications of the ACM,* vol. 31, no. 5.

Cohen, Stanley A. 2005. *Privacy, Crime and Terror: Legal Rights and Security in a Time of Peril.* Markham, Ontario: LexisNexis.

Commission Nationale de l'Informatique et des Libertés. 1998. *Les Libertés et l'Informatique: Vingt Deliberations Commentées.* Paris: La Documentation Française.

Electronic Privacy Information Center and Privacy International. 2005. *Privacy and Human Rights 2005; An International Survey of Privacy Laws and Developments.* Washington, DC: Electronic Privacy Information Center.

Flaherty, David H. 1989. *Protecting Privacy in Surveillance Societies.* Chapel Hill: University of North Carolina Press.

Foucault, Michel. 1979. *Discipline and Punish: The Birth of the Prison.* New York: Vintage Books.

Fried, Charles. 1968. "Privacy." *Yale Law Journal,* vol. 77.

Gellman, Robert. 2006. "Trafficking in Health Information: A Widespread Problem," Version 1.3, July 10, 2006, available from Robert Gellman, Privacy and Information Consultant, 419 Fifth Street, SE, Washington, DC, 20003.

Gilliom, John. 2001. *Overseers of the Poor: Surveillance, Resistance, and the Limits of Privacy.* Chicago: University of Chicago Press.

Goold, Benjamin J. 2004. *CCTV and Policing: Public Area Surveillance and Police Practices in Britain.* Oxford: Oxford University Press.

Greenawalt, Kent. 1975. *Legal Protections of Privacy: Final Report to the Office of Telecommunications Policy.* Washington, DC: U.S. Government Printing Office.

Gregor, Thomas. 1980. "Exposure and Seclusion: A Study of Institutionalized Isolation among the Mehinaku Indians of Brazil," in Stanton Tefft, ed., *Secrecy: A Cross-Cultural Perspective.* New York: Human Sciences Press.

Hagel, J., and J. F. Rayport. 1997. "The Coming Battle for Customer Information." *Harvard Business Review,* vol. 75, no. 30.

Halperin, Morton H., Jerry J. Berman, Robert L. Borosage, and Christine M. Marwick. 1976. *The Lawless State: The Crimes of U.S. Intelligence Agencies.* New York: Penguin Books.

Hendricks, Evan. 2005. *Credit Scores and Credit Reports: How the System Really Works, What You Can Do.* Second edition. Captain John, MD: Privacy Times, Inc.

Hentoff, Nat. 2003. *The War on the Bill of Rights and the Gathering Resistance.* New York: Seven Stories Press.

Hondius, Frits W. 1975. *Emerging Data Protection in Europe.* New York: Elsevier.

Hunter, Larry. 1985. "Public Image: Privacy in the Information Age." *Whole Earth Review,* vol. 32.

Kahn, Alfred J. 1966. "The Tyranny of Small Decisions: Market Failures, Imperfections, and the Limits of Economics." *Kyklos,* vol. 19, no 1.

Kang, Jerry. 1998. "Information Privacy in Cyberspace Transactions." *Stanford Law Review,* vol. 50, no. 4, April.

Kerr, Orin S. 2003. "Internet Surveillance Law after the USA Patriot Act: The Big Brother That Isn't." *Northwestern University Law Review,* vol. 97, no. 2.

Laudon, Kenneth. 1996. "Markets and Privacy." *Communications of the ACM,* vol. 39, no. 9.

Lyon, David. 2001. *Surveillance Society; Monitoring Everyday Life.* Philadelphia: Open University Press.

Marx, Gary. 2005. "Soft Surveillance: Mandatory Voluntarism and the Collection of Personal Data." *Dissent,* Fall.

Mayer, Jane. 2006. "The Hidden Power: A Secret Architect of the War on Terror." *The New Yorker,* 3 July.

McCahill, Michael, and Clive Norris. 2002. *CCTV in Britain.* Working Paper No. 3, Center for Criminology and Criminal Justice, School of Comparative and Applied Social Sciences, University of Hull, Hull HU6 7RX.

Michael, James. 1994. *Privacy and Human Rights: An International and Comparative Study, with Special Reference to Developments in Information Technology.* Paris: UNESCO.

Miller, Margaret J., ed. 2003. *Credit Reporting Systems and the International Economy.* Cambridge, MA: MIT Press.

Nissenbaum, Helen. 1998. "Protecting Privacy in an Information Age: The Problem of Privacy in Public." *Law and Philosophy,* vol. 17.

Noiriel, Gerard. 1996. *The French Melting Pot: Immigration, Citizenship, and National Identity.* Minneapolis: University of Minnesota Press.

Nouwt, Sjaak, Berend R. de Vries, and Corien Prins, eds. 2005. *Reasonable Expectations of Privacy? Eleven Country Reports on Camera Surveillance and Workplace Privacy.* The Hague: T.M.C. Asser Press.

O'Harrow, Robert, Jr. 2005. *No Place to Hide.* New York: Free Press.

Orwell, George. 1949. *1984.* London: Penguin Books.

Packard, Vance. 1964. *The Naked Society.* New York: McKay.

Phillips, David J. 2004. "Cell Phones, Surveillance and the State." *Dissent,* Spring.
Posner, Richard. 1978. "An Economic Theory of Privacy." *Regulation,* May/June.
Posner, Richard. 1978. "The Right of Privacy." *Georgia Law Review,* vol. 12, no. 393.
Ratner, Sidney. 1980. *Taxation and Democracy in America.* New York: Octagon Books/Farrar, Straus and Giroux.
Regan, Priscilla. 1995. *Legislating Privacy: Technology, Social Values, and Public Policy.* Chapel Hill: University of North Carolina Press.
Roberts, Alasdair. 2006. *Blacked Out: Government Secrecy in the Information Age.* New York: Cambridge University Press.
Rosen, Jeffrey. 2004. *The Naked Crowd: Reclaiming Security and Freedom in an Anxious Age.* New York: Random House.
Rotenberg, Marc. 2005. *The Privacy Law Sourcebook.* Washington, DC: Electronic Privacy Information Center.
Rovere, Richard. 1958. "The Invasion of Privacy (1): Technology and the Claims of Community." *The American Scholar,* vol. 27.
Rule, James B. 1973. *Private Lives and Public Surveillance.* London: Allen Lane.
———. 2004. "Toward Strong Privacy: Values, Markets, Mechanisms, and Institutions," *University of Toronto Law Journal,* vol. 54.
Rule, James B., Doug McAdam, Linda Stearn, and David Uglow. 1980. *The Politics of Privacy.* New York: Elsevier.
Rule, James B., and Lawrence Hunter. 1999. "Toward Property Rights in Personal Data," in Colin J. Bennett and Rebecca Grant, eds., *Visions of Privacy: Policy Choices for the Digital Age.* Toronto: University of Toronto Press.
Schwartz, Paul M., and Joel R. Reidenberg. 1996. *Data Privacy Law: A Study of United States Data Protection.* Charlottesville, VA: Michie.
Scott, James C. 1998. *Seeing Like a State: How Certain Schemes to Improve the Human Condition Have Failed.* New Haven, CT: Yale University Press.
Seipp, David J. 1978. *The Right to Privacy in American History.* Cambridge, MA: Program on Information Resources Policy, Harvard University.
Smith, Robert Ellis. 1997. *War Stories, Volume II: Accounts of Persons Victimized by Invasion of Privacy.* Providence, RI: Privacy Journal.
Solove, Daniel J. *The Digital Person: Technology and Privacy in the Information Age.* 2004. New York: New York University Press.
Swire, Peter P. 2004. "The System of Foreign Intelligence Surveillance Law." *The George Washington Law Review,* vol. 72, no. 6, April.
Swire, Peter P., and Robert E. Litan. 1998. *None of Your Business: World Data Flows, Electronic Commerce, and the European Privacy Directive.* Washington, DC: The Brookings Institution.

Thomas, L. C., J. N. Crook, and D. B. Edelman, eds. 1992. *Credit Scoring and Credit Control.* Oxford: The Clarendon Press.

Thompson, Catherine, and Ian Kerr. N.D. "Tailgating on Spyways: Vanishing Anonymity on Electronic Toll Roads."

Torpey, John. 2000. *The Invention of the Passport: Surveillance, Citizenship and the State.* Cambridge: Cambridge University Press.

U.S. Department of Health, Education and Welfare. 1954. *Vital Statistics of the United States 1950, Volume I.* Washington, DC: U.S. Government Printing Office.

———. 1973. *Records, Computers and the Rights of Citizens; Report of the Secretary's Advisory Committee on Automated Personal Data Systems.* Washington, DC: U.S. Government Printing Office.

U.S. Department of Justice, Federal Advisory Committee on False Identification. 1976. *Reporton the Criminal Use of False Identification.* Washington, DC: U.S. Government Printing Office.

U.S. Privacy Protection Study Commission. 1977. *Personal Privacy in an Information Society: The Report of the Privacy Protection Study Commission.* Washington, DC: U.S. Government Printing Office.

U.S. Senate. 1976. *Intelligence Activities and the Rights of Americans; Final Report of the Select Committee to Study Governmental Operations with Respect to Intelligence Activities, Book II.* Washington, DC: U.S. Government Printing Office.

U.S. Senate, Committee on Government Operations, U.S. House of Representatives Committee on Government Operations and Subcommittee on Government Information and Individual Rights. 1976. *Legislative History of the Privacy Act of 1974.* Washington, DC: U.S. Government Printing Office.

Vitalis, Andre. 1988. *Informatique, Pouvoir et Libertés.* Paris: Economica.

Volokh, E. 2000. "Freedom of Speech and Information Privacy: The Troubling Implications of a Right to Stop People from Speaking About You," *Stanford Law Review,* vol. 52.

Warren, Samuel, and Louis D. Brandeis. 1890. "The Right to Privacy," *Harvard Law Review,* vol. 4.

Waters, Nigel. 2006. "Government Surveillance in Australia," research report commissioned by James B. Rule.

Westin, Alan F. 1967. *Privacy and Freedom.* New York: Atheneum.

———. 1971. "Civil Liberties Issues in Public Databanks," in Alan F. Westin, ed. *Information Technology in a Democracy.* Cambridge, MA: Harvard University Press.

Westin, Alan F., and Michael A. Baker. 1972. *Databanks in a Free Society: Computers, Record-Keeping, and Privacy; Report.* New York: Quadrangle.

Whitley, Edgar, research coordinator. 2005. *The Identity Project: An Assessment of the UK Identity Card Bill and Its Implications. Interim Report.* London: LSE Department of Information Systems.

Winner, Langdon. 1977. *Autonomous Technology: Technics-Out-of-Control as a Theme in Political Thought.* Cambridge, MA: MIT Press.

Zamiatin, Eugene. 1924. *We.* New York: E. P. Dutton and Co.

Index

Abika, 113
Access Card, 73
accessibility of data, 26
accuracy of information, 26
actionable information, 15–17, 157
activism for privacy rights, 5, 29, 143–44
Acxiom, 107, 113, 114, 118, 130
Administrative Appeals Tribunal, 70
administrative investigations, 81–82, 83
administrative records, 24, 148
administrative wiretaps, 79–80
advertising, 132. *See also* marketing industry
advocacy for privacy issues, 139–41, 143–47, 192, 200
"affiliate organizations," 139–40
AGIRA (Association pour la Gestion des Informations sur le Risque Automobile), 131
air travel, 60, 86, 89, 144, 164–65
Alaska, 62
ALF (insurance company), 131
American Direct Marketing Association, 124
American Library Association (ALA), 56
anachronistic nature of privacy, xiii
anonymity, 7, 61
Anti-Terrorism, Crime and Security Act, 66, 74
anti-terrorism legislation, 66, 74, 79. *See also* Patriot Act
Argentina, *30*
arms, right to bear, ix
Association pour la Gestion des Informations sur le Risque Automobile (AGIRA), 131
Australia
  banking industry, 135
  and commercial use of data, 199
  compared with France, 130

Australia (*continued*)
compared with the U.S., 37, 69–74, 114–19, 133
and credit reporting, 136
and marketing of data, 96
and national ID cards, 83–84, 152, 164
and needs for surveillance, 173–74
and privacy codes, 29, *30,* 151, 152
and privacy organizations, 143–44
restrictions on data collection, 141
"Australia Card," 115
Australia Finance Conference (AFC), 135
Australian Federal Privacy Commission, 117
Australian Privacy Charter (APC, 1992), 25, 26–27
Australian Privacy Foundation, 144
Australian Secret Intelligence Organization, 70
Australian Transaction Reports and Analysis Centre (AUSTRAC), 71
automation, 83
automobile insurance, 21, 107, 130–31

background checks, 113–14, 191
balancing privacy priorities, 183–84
Bali terrorist attacks, 70
banking
competition among banks, 134–35
in France, 128
and IRS inspections, 48
and justifications for surveillance, 171–72
and symbiotic data, 22
ubiquity of, 158
Banque de France, 130, 135
Baycorp Advantage, 118
Belgium, *30*
benefits of surveillance, 91, 163
Bentham, Jeremy, 11
Bill of Rights, 43–44
biometric data, 68–69, 72, 77, 89
birth registration, 45, 157
Blair, Tony, 68–69, 153, 162, 166
Brandeis, Louis D., 1, 10, 13, 22
Brazil, *30*
Britain. *See* Great Britain
British Callcredit, 125
Brown, Ian, 65
Bulgaria, *30*
Bureau of Alcohol, Tobacco, Firearms and Explosives, 60
bureaucratic surveillance, 17, 41
Bush, George W.
and California privacy laws, 141
and data centralization, xiii, 47, 90
and domestic communications monitoring, 62, 84
and Total Information Awareness scheme, 164

California, 5, 107, 140, 141, 182
cameras, 67–68, 76–77
Canada
compared with the U.S., 37, 74–78, 83, 119–24, 133
and expansions of surveillance, 36
and needs for surveillance, 173
and privacy codes, 29–31, *30,* 155
and privacy organizations, 143–44, 145
and privacy victories, 139
and restrictions on data collection, 141
Canadian Charter of Rights and Freedoms, 74
Canadian Marketing Association, 124
Canadian Security Intelligence Service (CSIS), 74–75

Canadian Standards Association Model Code (CSA, 1996), 25, 29–30
capacity of surveillance systems, 163
CAPPS II, 152
cash, 176
Catholic Church, 40
cell phones. *See* communications surveillance; mobile phones
censorship, 36
census data, 42
Center for Democracy and Technology, 51, 143, 154
Central Intelligence Agency (CIA), 60
Central London Congestion Charging, 68
CGI, 122
checkpoints, 58–62, 83–84, 86–87
checks, 48
Children's Online Privacy Protection Act, 153
child-support, 46
China, 32
ChoicePoint, 57, 107–8, 113–14, 118, 122, 130
Church, Frank, 51
Church of England, 40
Citizens' Action Network, 143
civic life, 8, 194–95
civil liberties, 5
civil rights workers, 49
civil servants, 93–94
Civil War, 45
classification of risk groups, 128
Clinton, Bill, 137–38
CLUE reporting system, 108
CNIL. *See* Commission Nationale de l'Informatique et des Libertés (CNIL)
Coderre, Denis, 77
Cohen, Morris, 182
COINTELPRO program, 49
commercialization of personal data, 97, 102–5, 196. *See also* marketing industry
Commission Nationale de l'Informatique et des Libertés (CNIL). *See also* France
  and banking information, 128
  described, 78
  and the EU Privacy Directive, 129
  and financial surveillance, 81
  and the insurance industry, 131, 172–73
  legislative provisions weakened, 166–67
  and privacy activism, 144
  and state surveillance, 154–55
  and travel surveillance, 172–73, 188
common-law tradition, 64
Communications Assistance for Law Enforcement Act (CALEA), 161
Communications Security Establishment, 75
communications surveillance
  in Australia, 70, 74
  and the Bush administration, 84
  in Canada, 74–75, 123
  and constitutional privacy protections, 47–48
  and expansions of surveillance, 33–34, 158
  in France, 78, 81
  in Great Britain, 64–65
  and technology issues, 160–61
  and terrorist threats, 167
  and travel surveillance, 175
  and wiretapping, 79–80, 160, 190, 196

communism, 49
compartmentalization of data, 36
competition, 134–35
Composite Portrait of Fair Information Practices, 26
comprehensiveness of surveillance, 96
computing
  computer-readable ID cards, 77, 87, 161–62, 166
  and credit surveillance, 99–100
  and insurance industry, 107
  personal data on computers, 158
  and privacy losses, 14, 17, 18–22, 160
  and supplementary data, 17–18
Comte, Auguste, 156, 193
confidentiality, 109–10
conflicts of interest, 16
Congress, 46
connection data, 65, 70–71, 78, 79–80
consent issues
  in Canada, 123–24
  and consumer needs, 168–74
  and credit reporting, 126
  and direct marketing, 126
  and the Fair Credit Reporting Act, 139
  and fair information practices, 26
  in France, 129
  and the logic of surveillance, 35
  and monitoring devices, 172–73
  and "opt-out" procedures, 140
  and PIPEDA, 121
  and symbiosis among surveillance systems, 113
conspiratorial view of surveillance, 158–59
Constitutional Council, 81
constitutional privacy protections, 47–49
constraints on mass surveillance, 34–38. *See also* activism for privacy rights
consumer credit. *See* credit surveillance
consumers and consumption data, 19–20, 28, 71, 103, 130, 177–79
content data, 79–80
convenience, 145
corporate affiliates, 139–40
cost of surveillance systems, 184–85
Council of Europe Convention (C of E, 1981), 25, 27
court decisions, 36, 47–48
credit surveillance. *See also* financial surveillance
  and actionable information, 16–17
  in Australia, 71, 115–17, 117–18
  and banks, 134–35
  in Canada, 120–22
  constraints on, 35
  and credit cards, 100, 130
  and credit inquiries, 115–16
  and credit scores, 108–9, 159
  and debt data, 171
  in France, 81, 129–30
  in Great Britain, 93–94, 124–27
  and insurance, 108–9, 112
  and justifications for surveillance, 174
  longevity of, 185
  and marketing, 101
  and necessary data, 198–99
  and payment histories, 28
  and positive credit reporting, 98, 102, 120, 126, 129–30, 133, 134–36, 151–52, 197
  and privacy codes, 150, 190
  and profit motive, 95
  and safe harbor, 137
  and technology, 19, 99–100

and transparency, 28–29
ubiquity of, 158, 193
and the U.S., 33, 97–102
CRIF (data processing company), 127
crime and crime control. *See also* law enforcement; terrorism
and criminal records, 88–89
and espionage, 52–57
and longevity of personal data, 185
and organized crime, 80
sex offenders, 88, 90, 153
and tax evasion, 41–42
and travel surveillance, 67–68, 76–77, 130–31, 175–76
Czech Republic, *30*

Damaged Lives Register, 127
data brokers, 123
data mining, 103
Data Protection Act, 66, 67
Data Retention Directive, 66
data rights agencies, 197–98
Davis, Deborah, 61, 87
Davis, Gray, 140
death registration, 45, 157
debit cards, 130, 158
debt. *See* credit surveillance
"declarations of suspicion," 80–81
democracy, 11, 35
Dempsey, James, 51, 154
Denmark, *30*
Department of Motor Vehicles, 85
direct marketing. *See also* marketing industry
in Australia, 117
in Canada, 123
Direct Marketing Association, 103, 105
and discrimination, 102–5
and Do Not Call Registers, 105, 117, 127, 141–42
in France, 131–32
in Great Britain, 127
and opt-in rules, 197
and privacy codes, 150, 153
in the U.S., 141
disclosure of private information, 6–13
discrimination
and actionable data, 15–17, 157
and credit reporting, 115, 121
and direct marketing, 102–5
and expansion of surveillance, 192
as goal of surveillance, 18, 94–96
in insurance, 107
and opt-in rules, 197–98
and personal data, 181
and taxation, 41
dismantling of surveillance systems, 141
DNA data, xiv, 90, 167–68, 186
Do Not Call Registers, 105, 117, 127, 141–42
domestic violence, 189
driver's licenses, 17, 61–62, 166
driving records, 107, 186
drugs and pharmaceuticals, 2
due process, 148
Dun and Bradstreet, 115

eavesdropping, 47
E.C. Privacy Directive, 104
"An Economic Theory of Privacy" (Posner), 1
economics. *See* market economics
efficiency
and actionable data, 157
justice contrasted with, 186
and justifications for surveillance, 172
and marketing, 178–80

efficiency (*continued*)
and privacy advocacy, 192, 200
and privacy losses, 33–34
and technological advance, 21
and utilitarianism, 27
Electoral Registers, 125
Electronic Communications Privacy Act, 52
Electronic Frontier Foundation, 143
electronic monitoring, 83. *See also* communications surveillance
Electronic Privacy Information Center, 143
e-mail, 74, 158, 190
employment data, 33
encryption, 80
Enlightenment, 192
entrepreneurship, 107, 113, 196
Equifax, 97–98, 125
EquifaxCanada, 120
espionage, 52–57
Estonia, *30*
ethical issues, 27, 186, 200
ethnicity, 9
Europe and the European Union (EU). *See also* European Community; Privacy Directive (1995)
and British privacy practices, 126
and Canada, 77, 119
and the CNIL, 129
and direct marketing, 104
and marketing of data, 96
and money laundering, 66–67
and privacy codes, 31, 152
privacy protests in, 29
and safe harbor, 136–39, 153
and the welfare state, 14
European Commission, 138
European Community, 31–32, 137, 148–49. *See also* Europe and the European Union (EU)
European Court of Human Rights, 79
European Parliament, 138
evolution of mass surveillance, 20, 133
expansions of surveillance
and Canada, 36
and communications surveillance, 33–34, 158
and France, 36
and Great Britain, 36
and the IRS, 36, 162
and medical data, 34
and political dimensions of privacy, 200
and privacy codes, 35, 36, 151
and public opinion, 180–83
resistance to, xv, 5, 29, 143–44, 180–83
and social welfare, 36, 162
and terrorism, 38, 154
expectations of privacy, 7
expense of surveillance systems, 184–85
Experian, 97–98, 125, 127
extradition, 59, 88

Factual Service Bureau, 110
Fair and Accurate Credit Transactions Act (FACTA), 100–101
Fair Credit Reporting Act (1970), 29, 50, 100, 111–14, 139–41, 206n. 13
fair information practices, 23–26, 57, 111–12, 190
false identifications, 165
fatalism, 199–200
federal buildings, 89
Federal Bureau of Investigation (FBI), 39, 49–51, 54, 78–79, 88, 160–61

Federal Communications Commission (FCC), 105
Federal Intelligence Security Court, 53
Federal Privacy Commission (Canada), 69, 121
Federal Trade Commission (FTC), 105
fiber-optic lines, 160–61
Fichier des Incidents de Credit aux Particuliers (FICP), 130
Financial Crimes Enforcement Network (FINCEN), 58
financial surveillance. *See also* credit surveillance
  in Australia, 71
  in Canada, 76
  and cash, 176
  and consolidation of surveillance data, 83
  in France, 80–81
  and globalization of surveillance, 155
  in Great Britain, 66
  and justifications for surveillance, 171–72
  and lending data, 171–72
  and state monitoring, 176–82
Finland, *30*
FINTRAC, 76
Ford, Gerald, 50, 52
Foreign Intelligence Surveillance Act (FISA), 52–57, 76, 79
foreign nationals, 72
fourth amendment, 43–44, 47
France. *See also* Commission Nationale de l'Informatique et des Libertés (CNIL)
  and the banking industry, 135
  and commercial use of data, 199
  compared with the U.S., 37, 78–82, 83, 128–32, 133, 135
  and consent issues, 172–73
  and credit reporting, 136
  and expansions of surveillance, 36
  and marketing of data, 96
  and national privacy codes, *30*
  and needs for surveillance, 173–74
  and positive credit reporting, 135–36
  and privacy codes, 151, 154–55
  and privacy organizations, 143–44
  and public opinion, 166
  and restrictions on data collection, 141
free speech, 64
Freeh, Louis, 161
Fried, Charles, 6
functional relationships, 169

gag rules, 56
Gellman, Robert, 110
genetic information, xiv, 5, 90, 167–68, 186
Germany, *30*
global nature of surveillance programs, xvi
Gompers, Samuel, 192–93
Goold, Benjamin, 67
Government Accountability Office (GAO), 57
Great Britain
  civil servants, 93–94
  compared with the U.S., 37, 64–69, 83, 124–27, 133
  and consent issues, 172–73
  and expansions of surveillance, 36
  and national ID cards, 153, 162, 166
  national privacy codes, *30*
  and privacy victories, 139
  restrictions on data collection, 141

Greece, *30*
Gregor, Thomas, 6–7

health care. *See* medical care and data
health care providers, 1–2, 90
Health Insurance Portability and Accountability Act (HIPAA), 110–12
health maintenance organizations, 110
Hendricks, Evan, 57, 108
Henry VIII, 40, 42
Hitler, Adolf, 42
HIV status, 18, 89, 90, 106, 111
Hobbes, Thomas, 11
holistic privacy values, 6
Homeland Security, 59, 60–61
Hong Kong, *30,* 152
Hoover, J. Edgar, 39, 49, 54
HSBC Group, 126
Hungary, *30*

Iceland, *30*
identity card systems
  in Australia, 69, 73, 83–84, 152, 164
  in Canada, 77
  and checkpoints, 87–88, 89–90
  and false identification, 165–66
  in France, 82
  in Great Britain, 68–69, 153, 162, 166
  machine-readable ID cards, 77, 87, 161–62, 166
  National Identity Register, 68–69
  and public opinion, 164
  radio frequency identification (RFID) tags, 5, 182–83
  "Real ID Act," 61–62
  and travel surveillance, 89–90
illegal activities, 66–67, 126. *See also* law enforcement
Imaginons un Reseau Internet Solidaire (IRIS), 143
Immigration and Naturalization Service (INS), 86
Impaired Lives Register, 127
income taxes. *See* taxes and taxation
inferential data, 108–9
Information and Privacy Commissioner, 77
Information Commission, 94
information resellers, 57
information technology, 14
"inherent authority," 62
insurance industry
  and actionable information, 16
  automobile insurance, 21, 107, 130–31
  and credit information, 63, 112, 118, 159
  and discrimination, 198
  in France, 130–31
  and genetic data, 5, 186
  in Great Britain, 127
  and health data, 90
  and HIV status, 90
  and life insurance, 106, 131
  and monitoring devices, 172
  and necessary data, 198–99
  and symbiotic data, 22
  and travel surveillance, 21, 130–31, 186, 188
  in the U.S., 105–12
intelligence agencies, 24, 148
Internal Revenue Service (IRS)
  and constitutional privacy protections, 48
  and debt-related data, 171–72
  and expansions of surveillance, 36, 45, 162
  and the Patriot Act, 154

and personal consumption data, 4–5
and the proposed National Data Center, 165
international travel, 59, 86, 158, 175. *See also* travel surveillance
Internet usage data, 158
Interpol, 82
intimacy, 3
investigative companies, 57, 110
Ireland, *30*
Israel, *30*
Italy, *30*

Japan, *30*
Johnson, Samuel, 182
Jospin, Lionel, 80
judicial review, 83
justice, 21, 186
justifications for surveillance, 169–71, 195. *See also* law enforcement; terrorism

Kahn, Alfred J., 181–82
Kang, Jerry, 169
Kant, Immanuel, 11, 12–13, 27, 186–87
Katz decision, 48
Kennedy, Edward, 60

LaBonte, Mark, 106
labor interests, 45
Latvia, *30*
law enforcement
and access to personal data, xiv
and communications surveillance, 160–61
and DNA data, 167–68
and financial surveillance, 177
and health data, 18, 90
and justifications for surveillance, 15, 171
and privacy protection, 24
and symbiotic data, 22
and travel surveillance, 175–76
and utilitarianism, 12
laws, 96. *See also* privacy codes and legislation
lawsuits, 52
legality of data collection, 26
legislation. *See* privacy codes and legislation; *specific pieces of legislation*
lending data, 171–72. *See also* financial surveillance
Levi, Edward, 52
Lewis, Sinclair, 7
liberal democracy, 35
library records, 191
license plates, 67, 72–73, 76–77
life insurance, 106, 131
Lithuania, *30*
lobbying, 119
London School of Economics (LSE), 162
longevity of personal data, 70, 72, 76, 80, 83, 185. *See also* storage of surveillance data
Louis XIV, 42
Lovelace Health Systems, 1–2, 3, 34
Luxembourg, *30*

machine-readable ID cards, 77, 87, 161–62, 166
MacLean's, 122–23
Malta, *30*
market economics
and insurance, 110
and personal data, 10–11, 97, 114

market economics (*continued*)
pressures on privacy, 133
and profit motive, 95, 109, 159
marketing industry
and consumer credit, 101, 136
and consumption surveillance, 177–79
and direct marketing, 102–5, 117, 123, 127, 131–32, 141–42, 150, 153, 197
and efficiency, 178–80
and insurance, 159
marketing of personal data, 96, 129
and medical care, 103
marriage registration, 157
Marx, Gary, 167–68
mass surveillance, xi, 14–15, 20, 21, 34–38. *See also specific forms of surveillance*
media, 10
medical care and data
and actionable information, 16
and centralization of data, xiii–xv, 4
and commercialization of data, 97
and consent issues, 170–71
and consolidation of surveillance data, 47
and direct marketing, 103
and expansions of surveillance, 34
and financial surveillance, 179
genetic information, xiv, 5, 90, 167–68, 186
in Great Britain, 127
and HIV status, 18, 88, 89, 90, 106, 111
and the insurance industry, 1–2, 109–12
and law enforcement, 18
as personal information, 11–12
and public health, 179
and symbiotic data, 22
Mehinaku tribe, 6–7
MIB (insurance company), 106, 121–22, 131
military service, 45, 90
Mills, C. Wright, 196
Minister of the Interior (France), 82
Ministry of Transport (France), 131
mobile phones, 160–61, 167, 175. *See also* communications surveillance
mobility, 100. *See also* travel surveillance
money laundering, 66–67, 126
motives for privacy, 4
movement surveillance. *See* travel surveillance

"naked machines," 164–65
National Commission on Information Processing and Liberties. *See* Commission Nationale de l'Informatique et des Libertés (CNIL)
National Control Commission for Security Interceptions (CNCIS), 79
National Data Center, 165
national identity cards. *See* identity card systems
National Identity Register, 68–69
national privacy codes. *See* privacy codes and legislation
national security, 12, 18, 151. *See also* law enforcement; terrorism
National Security Agency (NSA), 62–63, 190, 196
National Security Letters, 56
Nazism, 185
necessary data, 198–99

negative credit reporting, 151–52
Netherlands, *30*
New Hampshire, 62
New York City, 84
New York State Comptroller's Office, 159
The New York Times, 2, 56, 62–63, 145
New Zealand, *30*
1984 (Orwell), 42–43, 190
Nixon, Richard, xii, 50, 64, 185
No Fly Lists, 60, 88
nongovernmental organization (NGOs), 143–44
North Dakota, 140, 141
Norway, *30*
Norwich Union, 172
Nunez, Stephen, 117

Office of Intelligence Review and Policy (OIRP), 54
Olmstead decision, 47
Omnibus Crime Control and Safe Streets Act, 52
oppression, 42, 64, 184–85, 188
opt-in policies
  and Canada, 121, 123–24
  and France, 131, 132
  and HEW principles, 25
  and North Dakota, 140
  scope of, 196
Option Consommateurs, 143
opt-out policies
  and the Australian Privacy Charter, 26–27, 117
  and definition of privacy, 3
  and demands for information, xv
  and the Fair Credit Reporting Act, 29
  and France, 131
  and Great Britain, 127
  and HEW principles, 25
  and North Dakota, 140
  and privacy code failures, 190
  and public interest, 198
  and resale of personal data, 124
Organization for Economic Co-operation and Development (OECD), 25, 29, 31
organizational goals, 13
organized crime, 80
origins of personal data, 198
Orwell, George, 42–43, 190
ostracism, 7
ownership of personal data, 196
Oyster Card, 68

Parent Locator Service (PLS), 46
passenger data. *See* travel surveillance
passports, 44, 46, 59, 67, 72, 162
Patriot Act
  and Australia, 70
  and Canada, 76
  and expansions of surveillance, 33, 154
  and FISA, 52–55, 55–57
  and judicial checks, 83
  and the Privacy Act of 1974, 51
  and the proposed National Data Center, 165
  and secrecy of surveillance, 151
pensions, 45
Personal Information Protection and Electronic Documents Act of 2000 (PIPEDA), 74–75, 119–22, 123, 139, 163
personal responsibility, 185–86
Phillips, David J., 160–61

Poland, *30*
police. *See* law enforcement
policy issues, 22–32, 189
political dimensions of privacy
  and combating surveillance expansions, 200
  fluctuations in, 44
  and justifications for surveillance, 195
  and political repression, 42, 64, 184–85, 188
  and sharing of information, 61
  and the War on Terror, 62–63
The Politics of Privacy (Rule), 36
Popper, Karl, 200
populist privacy protections, 114–19, 140
Portugal, *30*
positive credit reporting
  in Canada, 120
  and consent issues, 197
  and credit scores, 102
  and efficiency, 98, 133
  in France, 129–30
  in Great Britain, 126
  political support for, 135–36
  and privacy codes, 151–52
Posner, Richard, 1, 8–9, 10–11
Privacy Act of 1974
  and data sharing, 139, 163–64
  and fair information practices, 111–12
  and for-profit surveillance, 57
  and the HEW Report, 29
  as national code, 206n. 13
  and the Patriot Act, 154
  and privacy activism, 144–45
  and Watergate, 50–51
Privacy Act of 1982, 74, 119
Privacy Act of 1988, 69, 71–72
Privacy and Freedom of Information Office, 144–45
Privacy and Freedom (Westin), 22
privacy codes and legislation
  in Australia, 29, *30,* 117
  background of, 22–27
  in Canada, 29–31, *30,* 74
  controversies surrounding, 28–29
  cost and benefits of, 150–56
  by country, *30*
  and data sharing, 163–64
  and expansions of surveillance, 35, 36
  in France, *30,* 78
  national codes, 28–32, *30,* 206n. 13
  negative effects of, 190
  and Northern Europe, 42–43
  South Korea, 29, *30*
  Sweden, 29, *30*
  and the Watergate era, 51
Privacy Directive (1995)
  described, 31
  effects of, 31–32
  and France, 129, 132
  and Great Britain, 126
  and the OECD Guidelines, 29
  preamble, 148–49
  and safe harbor, 138–39
Privacy International, 143
privacy organizations, 143–44
privacy regimes, 7, 13–18, 19
Privacy Rights Clearinghouse, 143
Privacy Times, 57, 108
Private Lives and Public Surveillance (Rule), xii, 163
private sector, 94, 147–48. *See also* market economics
probable cause, 53
profit motive, 95, 109, 159
protests. *See* activism for privacy rights

public access to information, 26
public goods, 8
public health, 179
public information, 8–9, 94, 194
public interest, 198–99
public opinion
  in Australia, 69–70
  cyclical nature of, 84
  in France, 166
  and national ID cards, 164
  and privacy codes, 152
  and public information, 8–9
  support for privacy protections, xv, 145, 146, 180–83
  and technological advance, 21
  and terrorism, 155, 167
public policy, 22–32, 189
public record data, 158
Public Safety Act, 75, 78
purposes of surveillance, 169–71

radio frequency identification (RFID) tags, 5, 182–83
Reagan, Ronald, 64, 185
"Real ID Act," 61–62
"reasonable expectations of privacy" standard, 48–49
Records, Computers and the Rights of Citizens (report), 23, 29, 50, 148
Registered Traveler Program, 168
Regulation of Investigatory Powers Act (UK), 65
Reidenberg, Joel, 48, 104
reporting agencies, 147–48
repression, 42, 64, 184–85, 188
resellers of information, 57. *See also* marketing industry
resistance to surveillance expansions, xv, 5, 29, 143–44, 180–83
responsibility for information security, 26
retail transaction data, 33
retention of surveillance data, 70, 72, 76, 80, 83
right to privacy, 11–13, 27
"The Right to Privacy" (Warren and Brandeis), 1
Roman Empire, 42
Royal Air Force (RAF), 42
rules regarding privacy issues, 147–50. *See also* privacy codes and legislation

SAFARI plan, 166
safe harbor, 136–39, 153, 164
safety and security. *See also* law enforcement; terrorism
  and airport security, 164–65
  and data sharing, 35
  and discriminating treatment, 41–42
  and incremental privacy losses, 167
  and investigative activities, 151
  responsibility for information security, 26
  and total security, 200–201
sale of personal data, 113, 123, 129, 132–33. *See also* marketing industry
Sara Lee Corporation, 2
Schwartz, Paul, 48, 104
scientific worldview, 156
Scott, James, 41
Second Amendment, ix
secrecy of surveillance efforts, 24, 187
security. *See* law enforcement; safety and security
self-ostracism, 7
self-regulation provision, 138

September 11 terrorist attacks, 38, 55, 66, 70, 155
sex offenders, 88, 90, 153
sexual information, 6–7, 18. *See also* HIV status
sharing of surveillance data, 118, 163–64. *See also* symbiosis of surveillance programs
Singapore, 31–32, 137
Slovak Republic, *30*
"smartcards," 72, 73
social costs of surveillance, 188–89
social justice, 119, 185
social relations, 3, 19, 32
social welfare and Social Security
  and actionable information, 16
  and benefits of surveillance, 163
  and consolidation of surveillance data, 45–46, 87
  development of, 157–58
  in Europe, 14
  and expansions of surveillance, 36, 162
  and financial surveillance, 177
  and France, 81
  and medical data, 90
  and the National Data Center, 165
  and the Patriot Act, 154
  and repression, 185
  and state monitoring, 177
  welfare institutions, 14, 16, 36, 73, 81
South Korea, 29, *30,* 143–44, 152
Spain, *30*
Specially Designated Nationals, 88
sponsorship of information use, 20
Stalin, Joseph, 42
standards for privacy issues, 147–50
state authority, 20
states' rights, 190
Statewatch, 143
statistical records, 24
Stoddart, Jennifer, 77–78, 122–23
storage of surveillance data, 70, 74, 76, 80, 83, 185
strategic view of privacy, 4, 9, 11
subscriber data, 76
supermarkets, 103
supplementary data, 17–18
"Suspicious Activity Reports" (SARs), 58, 66–67
Sutter, California, 5, 182
Sweden, 29, *30*
Swire, Peter, 53–57
Switzerland, *30*
symbiosis of surveillance programs, 17–18, 22, 112–13, 163–64. *See also* sharing of surveillance data

Taiwan, *30*
taxes and taxation
  and benefits of surveillance, 163
  and consolidation of surveillance data, 46–47
  and expansions of surveillance, 35
  and financial surveillance, 177
  in France, 81
  income taxes, 45
  and the Internal Revenue Service, 4–5, 36, 45, 48, 154, 162, 165, 171–72
  and justifications for surveillance, 171–72
  and personal documentation, 86–87
  and record keeping, 14
  and repression, 64, 185
  and state revenues, 84–85, 107
  and tax farming, 40–42, 91
  and travel surveillance, 85–86
  in the U.S., 157–58

technology
and blame for privacy losses, x, 18–22, 191
and communications surveillance, 160–61
and credit surveillance, 99–100
and travel surveillance, 175
and trends in privacy rights, 200
telecommunications. *See* communications surveillance
telemarketing, 105, 141–42. *See also* marketing industry
terrorism
and actionable information, 15
and Australia, 70
and balancing privacy priorities, 183–84
and Canada, 74
and communication surveillance, 79–80
and expansions of surveillance, 35, 38, 82–83, 91–92, 193
and FISA, 55
and France, 79
and globalization of surveillance, 155
and the Patriot Act, 154
and public opinion, 152, 167
and wiretapping, 190
Thailand, *30*
Thatcher, Margaret, 124
third-party payors, 110
Title III searches, 56, 65
toll roads, 76–77
Total Information Awareness (TIA) Program, 152, 164
total surveillance society, 162–64
totalitarianism, 42
Tracfin, 80–81
tracking data, 161, 184–85
traffic cameras, 67–68, 76–77
Transportation Security Administration (TSA), 60–61, 88
TransUnion, 93, 97–98, 101, 120
travel surveillance
air travel, 60, 86, 89, 144, 164–65
in Australia, 72
in Canada, 76–77
and checkpoints, 60
and consolidation of surveillance data, 44, 46
in France, 82
globalization of, 155
infrastructure for, 175
and international travel, 59, 86, 88, 158, 175
and license plates, 67, 72–73, 90
and national ID cards, 89
and No Fly Lists, 60, 88
and privacy activism, 144–45
and privacy losses, 33
Registered Traveler Program, 168
and repression, 184
and symbiotic data, 22
and traffic cameras, 67–68, 76–77
and the TSA, 60–61, 88
and vehicular surveillance, 67–68, 85–86
and visas, 88
Treasons Act, 40
Treasury Enforcement Communications System (TECS), 59, 61, 77, 158
trends in privacy rights, 199–200
triangulation, 104
"The Tyranny of Small Decisions" (Kahn), 181

UK Information Commissioner, 66, 125–26
uncertainty, 105–6
United Kingdom. *See* Great Britain
United States
  and consumer credit information, 97–102
  and foreign policy, 119
  and free market economics, 97–114
  insurance industry in, 105–12
  lack of privacy commissioners, 83
  and marketing industry, 96, 141
  and national privacy codes, *30*
  and privacy losses, 33, 37
  privacy organizations, 143–44
  and safe harbor, 136–39
Universal Declaration of Human Rights, 23
U.S. Census Bureau, 165
U.S. Congress, 165, 166
U.S. Constitution, 43–44
U.S. Customs Service, 59
U.S. Department of Health, Education and Welfare, 23–26, 29
U.S. Department of Health and Human Services, 111
U.S. Department of Homeland Security, 152
U.S. Department of Justice, 52, 54, 165
U.S. Department of State, 88
U.S. Department of the Treasury, 58, 60, 67, 88
U.S. Supreme Court, 47, 48
USA PATRIOT Act. *See* Patriot Act
utilitarianism, 10–12, 27, 187–88
vehicular surveillance, 67–68, 76–77, 85–86
verification of data, 17
victories for privacy advocates, 139–41
video surveillance, 67–68, 72, 76–77
Vietnam War, 49
visas, 88

War on Terror
  and consolidation of surveillance data, 91–92
  and data sharing, 164
  and expansions of surveillance, 154
  and FISA, 54
  and for-profit surveillance, 57
  global impact of, 43
  and "inherent authority," 62
  and medical data, xiv
  and privacy losses, xii
  and public opinion, 84, 152
  and surveillance levels, 193
Warren, Samuel D., 1, 10, 13, 22
watch lists, 60, 88
Watergate, xii, 49–52
Waters, Nigel, 74
welfare and the welfare state. *See* social welfare and Social Security
Western Europe, 14
Westin, Alan, 22, 50, 149–50
wiretapping, 78–80, 160, 190, 196
World War II, 42