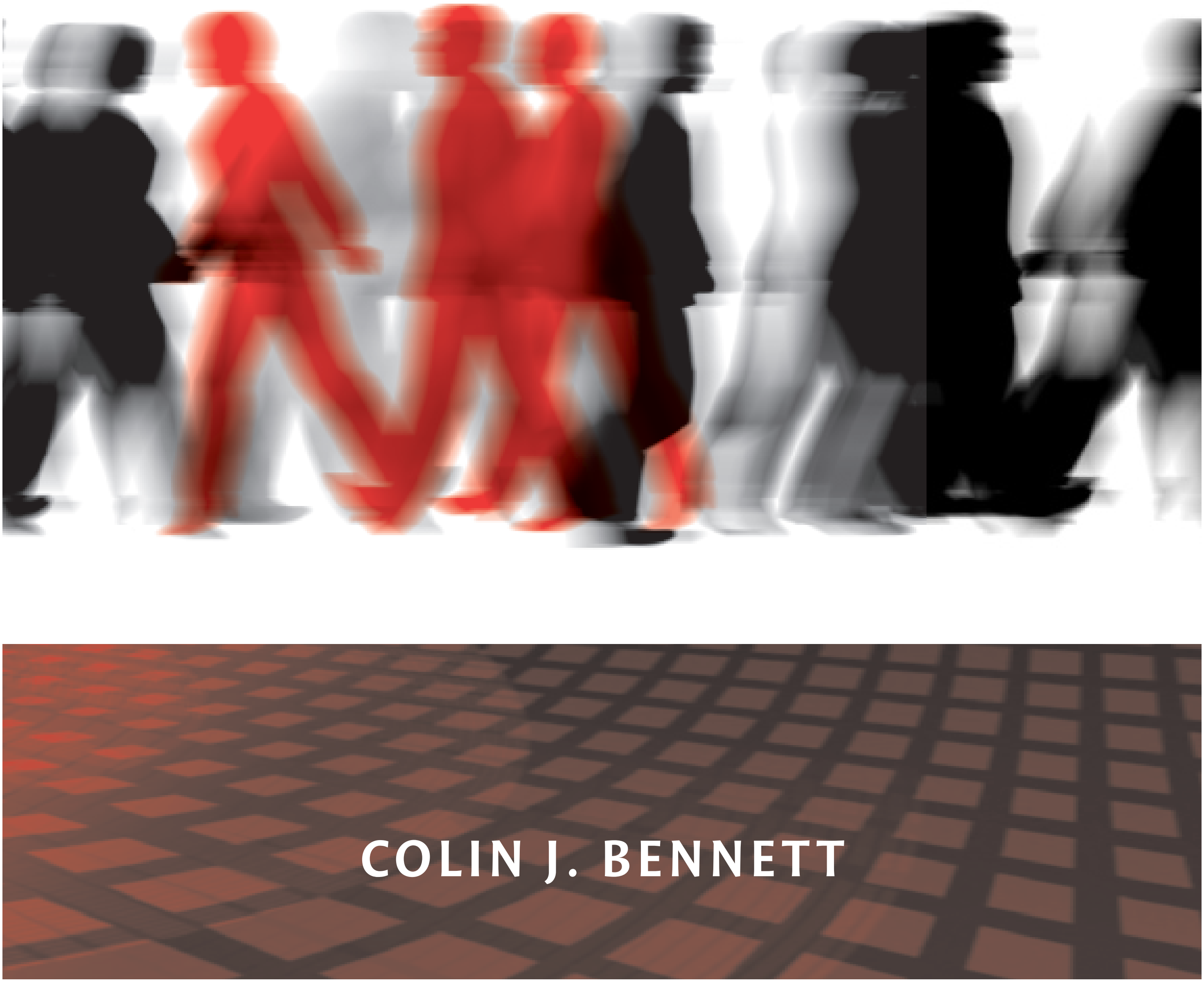
THE PRIVACY ADVOCATES

RESISTING THE SPREAD OF SURVEILLANCE



COLIN J. BENNETT

The Privacy Advocates

Resisting the Spread of Surveillance

Colin J. Bennett

The MIT Press
Cambridge, Massachusetts
London, England

© 2008 Massachusetts Institute of Technology

All rights reserved. No part of this book may be reproduced in any form by any electronic or mechanical means (including photocopying, recording, or information storage and retrieval) without permission in writing from the publisher.

For information about special quantity discounts, please email special_sales@mitpress.mit.edu.

This book was set in Times New Roman and Syntax on 3B2 by Asco Typesetters, Hong Kong. Printed and bound in the United States of America.

Library of Congress Cataloging-in-Publication Data

Bennett, Colin J. (Colin John), 1955–
The privacy advocates : resisting the spread of surveillance / Colin J. Bennett
p. cm.
Includes bibliographical references and index.
ISBN 978-0-262-02638-3 (hardcover : alk. paper) 1. Privacy, Right of. 2. Human rights advocacy. 3. Human rights movements. 4. Human rights workers. I. Title.
JC596.B46 2008
323.44′82—dc22 2008013819

10 9 8 7 6 5 4 3 2 1

To privacy advocates (anywhere and everywhere)—however they are defined

Contents

Introduction

If one enters the term *privacy advocates* into any major Internet search engine, roughly half a million hits arise. In any one week, numerous media stories quote privacy advocates arguing this or protesting that. Privacy advocates are the people who, at least in journalistic parlance, challenge the development of the increasingly intrusive ways by which personal information is captured and processed: identity cards, video surveillance, biometric identifiers, the retention of communications traffic data, the use of cookies and spyware by Web sites, unsolicited marketing practices, data matching and profiling, the monitoring of employees in the workplace, the use of tracking devices in vehicles, the spread of radio frequency identification devices (RFIDs), and a host of other practices. There are a bewildering variety of ways that personal data can be captured, processed, and disseminated. Some people are deeply concerned about these trends and have been trying to do something about them. They tend to be identified as "privacy advocates."

So who are these "privacy advocates"? Who gets mobilized when new surveillance systems rise to governmental and corporate agendas? How do they organize? What do they do? What do they believe? Privacy advocates operate within a range of institutions. They work within nongovernmental organizations (such as civil liberties groups, human rights organizations, and consumer associations). They can also be employed by government, in the case of staff within the official privacy and data protection authorities. They are also found within the corporate sector, as with the chief privacy officers (CPOs) of major corporations, and within some of the major law firms. And sometimes they work on their own.

This book is not about all the people who self-identify as privacy advocates. It is rather about those individuals and groups that have emerged from civil society, spontaneously and without official sanction, rather than about those within the state or the market. This distinction is imperfect, but it will serve to place some initial delimitation around a huge subject matter. Consequently, and unfortunately, some very important individuals within the privacy movement have to be excluded, or at least marginalized, including those who have current employment within either government or the private sector. The decision to assign these "advocates" to the margins and the footnotes should not be read as signifying that they do not play very important roles in promoting the privacy value within their respective organizations and jurisdictions. Rather, the decision is prompted by practical considerations about the scope of the study.

The focus on the more organized and collective forms of social action should also not obscure the fact that resistance to surveillance practices occurs in many less visible ways by ordinary people who would not necessarily identify as privacy advocates. Gary Marx (2003) has explored the many inventive ways that individuals have found to avoid or thwart surveillance, by obscuring their identities, distorting their data, refusing to comply, and so on. The everyday and ubiquitous realities of contemporary surveillance mean that resistance is demonstrated in many locales by ordinary individuals who might quietly, but insistently, refuse to provide personal information, or subtly try to subvert organizational demands. These patterns of everyday resistance are undeniably important elements of antisurveillance politics. By and large, however, these scattered responses have not translated into collective action. And that is one of the central puzzles of this book.

Based on key informant interviews with over thirty advocates in the United States, Canada, Australia, and Europe, as well as on extensive documentary analysis, this research seeks to fill an important gap in the vast literature on privacy. There exists a long tradition of philosophizing about the privacy value, of debating the various legal, technical, and self-regulatory solutions, of warning about the steady slide toward the "surveillance society" and of dissecting nationally and comparatively what mass publics think about the subject. Nobody, however, has attempted to examine the advocacy groups—the disparate individuals and organizations in civil society who have consciously and purposefully attempted to advance the cause for privacy protection. Nobody has asked the question: when surveillance practices emerge, who mobilizes against them, how, and with what effect? Those are my central questions.

The Justification

Many books have been published on privacy in the last twenty years, most of which have claimed a gradual erosion of personal privacy in the face of some relentless social, political, and technological forces (e.g., Sykes 1999; Whitaker 1999; Garfinkel 2000; Rosen 2000; O'Harrow 2005; Rule 2007). As most of the literature notes, privacy is an elusive and multidimensional concept whose meaning is culturally and historically contingent. Yet, it is still the concept that tends to define the policy issue in advanced industrial societies, and it is still the concept around which challenges to excessive surveillance get framed. At root, it has tended to mean the extent to which individuals have control over the circulation of their personal information. Surveillance, broadly defined, challenges that right or interest. It connotes not only visual observation or monitoring but, according to David Lyon, any "collection or processing of personal data, whether identifiable or not, for the purposes of influencing or managing those whose data have been garnered" (2001, 2). Surveillance is, therefore, a routine condition of modern societies to which we are all subjected when we engage in everyday activities. It is also, therefore, a global condition, because personal information can now flow freely and instantaneously across digital networks.

Privacy protection as a public policy question rose to the agendas of advanced industrial states in the late 1960s and 1970s. In those years, there was an abiding assumption that the enactment of law based on a set of common statutory principles, together with credible oversight and enforcement machinery, was both necessary and sufficient to redress the balance between the vulnerable individual and the power of public and private institutions (Flaherty 1989). In the 1990s, however, those assumptions shifted, and experts began to speak of a more complicated inventory of "policy instruments" in addition to properly enforced domestic data protection or privacy legislation: international agreements for the secure processing or personal data when it crosses national borders; the proper implementation of self-regulatory mechanisms, such as codes of practice, standards, and Internet Web seals; privacy impact assessments; and the application of appropriate privacy-enhancing technologies (Bennett and Grant 1999; Bennett and Raab 2006). All are necessary policy instruments; none is sufficient.

At the same time, others have argued that the progress of privacy protection will depend less on policy mechanisms devised and implemented by elites, and more on the extent to which resistance to surveillance practices can be mobilized through social movements (Lyon 2001, 131–135). Some have even contended that instruments for privacy protection often do little more than legitimate existing surveillance practices, rather than stem the seemingly relentless collection and processing of individually identifiable information (Rule et al. 1980). For some of the more radical privacy activists, the progress of the issue depends on the building of a more coherent activist network, which not only uses available means of redress but continuously exposes overly intrusive practices and ‘‘outs’’ the organizations that are responsible for them (Davies 1999).

There is some evidence that the concerted efforts of privacy advocates are producing more frequent and public protests against overly intrusive methods of personal information collection. In the 1970s and 1980s, there were some sporadic protests in Western Europe against certain censuses. And in the late 1980s, the proposed introduction of a national identity card in Australia provoked a storm of controversy. More recently, however, we have witnessed high-profile campaigns against the capture of personal information on the Internet. There have been very visible protests and boycotts against some companies for the use of RFIDs in their products. In Canada, a 1999 controversy over a database managed by Human Resources and Development Canada provoked front-page headlines, a parliamentary uproar, and the near resignation of the responsible Minister. A proposal in Japan for a centralized national identity system (Juki Net) was met with street protests and government embarrassment. In the United Kingdom, the Blair government’s proposals for a national identity card became one of the most controversial and partisan issues of modern British politics. In Germany, there have been high levels of activism against new laws mandating the retention of communications data by telecommunications companies and Internet service providers, including a rally in Berlin in September 2007 in which fifteen thousand people participated. There is at least anecdotal evidence that new private-sector and public-sector schemes for personal information processing can provoke more intense and widespread protest than has occurred in the past.

Whereas there is a sprawling and multidisciplinary literature on the appropriate policy responses to this concern, there has been very little analysis of how demands for privacy protection are articulated and aggregated in different societies and internationally. But who are the privacy advocates, and can they be distinguished from others in the policy community such as consultants, journalists, lawyers, and organizational privacy officers? What do they believe? How do they organize and obtain resources? How do they make decisions about strategies and priorities? Do they direct their appeals to mass publics, or to political and business elites? This book attempts to gain a better purchase on the organization, resources, and strategies of these advocacy groups, and thus to determine whether the conditions are present for a different form of social movement or transnational activist network to develop.

The Organization

Chapter 1 provides a broad historical overview of the nature of the social problem to be confronted. How has the issue been "framed," both by academic research and by the advocates themselves? The definition and scope of the problem has undergone some subtle transformations since the advent of widely available information technology and the coincident concern about personal privacy in the 1960s. This chapter traces the literature from the initial concerns about the "databank society," to the "new surveillance" characteristic of the network society, to more contemporary concerns about the monitoring of location and mobility within the ubiquitous "Internet of things." Along with other analysts, I contend that surveillance is a condition of modern societies, but also that the agents, subjects, and practices have broadened from the early days when the concerns were largely confined to the actions of the omniscient state operating large mainframe databanks. Another dimension of this story, however, is how the actors themselves see the problem. Do contemporary privacy advocates proceed with fixed definitions of "privacy" or deeper philosophical understandings about how to judge when a line has been crossed from the acceptable to the unacceptable, or the ethical to the unethical? Or do they rely more on the "gut instinct"—on the deeper sense that, regardless of technology, institution, and location, some practices are simply wrong and deserve resistance.

Chapter 2 provides a broad overview of the civil society groups through which privacy advocates work. In every advanced industrial society, there exist one or more groups whose self-defined mission is to raise alarm bells about practices that entail unacceptably high levels of surveillance. Sometimes these advocates operate within self-contained groups whose chief mission is to promote privacy. Others are located within larger organizations that try to promote a fuller range of civil liberties or human rights interests. Others are closely related to the consumer movement. Still others have emerged to defend the broad range of digital rights within cyberspace. Many focus on the "single issue." One of the preliminary tasks of the research is to paint a general and contemporary profile of the privacy advocacy network. A listing of the privacy advocacy groups referenced later is provided at the end of this Introduction.

The groups tell one story. The actors within them tell another. Chapter 3 analyzes the various roles played by contemporary privacy advocates. The network is comprised of Advocate-Activists, Advocate-Researchers, Advocate-Consultants, Advocate-Technologists, Advocate-Journalists, and Advocate-Artists. These categories are, of course, flexible and overlapping. Most advocates tend to play multiple roles with sometimes conflicting commitments. Advocates also tend to move from one role to another with speed and ease. And how individuals self-define their roles is often inconsistent with the perceptions that others in the network have of them. The advocacy role is, for most, mediated by other identities—researcher, consultant, technology developer, journalist, or artist.

Chapter 4 discusses the strategies adopted by privacy advocates. Using the framework developed by Margaret Keck and Kathryn Sikkink (1998), this chapter explores how the privacy advocates have engaged in a combination of information, symbolic, accountability, and leverage politics. Much of their activity involves generating politically relevant information about privacy protection and moving it to where it will have the most impact. Thus many privacy advocates perform a range of fairly traditional advocacy functions in relation to the official agencies of the state. They give testimony. They comment on legislative and administrative proposals for new uses of personal information. They generate research and analysis. Privacy advocates also attempt to advance the cause in less public ways, by working with organizations to assist them to improve their practices. Privacy advocates also have to call upon symbols that make sense of these issues within the wider culture. This chapter, therefore, examines the relationship between privacy advocates and the media. On occasion advocates can also attempt to hold powerful governmental and corporate institutions to account, through official complaints or litigation. Standards for privacy protection are inherent in domestic law, international agreements, corporate privacy policies, and other standards. Advocates can, and have, tried to get organizations to live up to their regulatory obligations and public commitments. On occasion they can also exert leverage, mainly through the threat of bad publicity. "Naming and shaming" has a tradition within other areas of social, environmental, and human rights policy. It is increasingly apparent within this area as well.

Chapter 5 examines the dynamics of a number of key conflicts over privacy. The early disputes over the collection of information through the census in certain European countries were the first real examples of highly publicized conflicts over the erosion of privacy. The attempted introduction of identity cards (especially in Australia and the United Kingdom) has also been extremely contentious. Certain marketing schemes, especially over the Lotus Marketplace product, aroused considerable interest in the early 1990s. More recently, conflicts have occurred with respect to intrusive practices on the Internet, such as the development of key-escrow encryption, online advertising through third party cookies, and online authentication mechanisms such as the Microsoft passport. Highly publicized disputes over privacy are rare, but they are increasing in frequency and intensity. I explore the various reasons for this, and I try to establish the common conditions that have accompanied these cases and resulted in apparent victories for privacy advocates and their allies.

Chapter 6 examines the ways in which these various actors do, or do not, network—both online and offline. How do they connect, through privacy conferences and privacy campaigns and privacy coalitions? There is no "umbrella group." When privacy conflicts arise, they tend to be waged by a loose coalition of relatively small groups who come together for specific causes and then disband. An underlining and concluding theme in this chapter is the ways in which the Internet facilitates advocacy networks. Privacy advocacy provides a useful case study of the phenomenon of "net activism." Given the technological sophistication of many privacy activists, the Internet became the locus of some quite early conflicts over issues such as encryption, third-party cookies, and the construction of online databases (Gurak 1997). The Internet has been, therefore, both the object of contention and the means through which intrusive practices could be denounced. The question remains, however, whether the Internet has ushered in a new form of privacy advocacy, unrestrained by traditional constraints of membership, geographic space, and time, or whether it has just introduced a pattern of misinformed and chaotic "electronic panics." This chapter will speak directly to these questions.

The level of activism and media coverage about privacy has clearly risen in the last decade. But it cannot yet be argued that the greater salience of the issue is attributable to the rise of a global social movement devoted exclusively to the advancement of the privacy value. There has been an enormous amount of policy activity: law, codes of practice, international agreements, privacy-enhancing technologies, and so on, contributing to a "trading-up" of international regulation (Bennett and Raab 2006). However, little of this has occurred as a result of concerted grassroots campaigning. There is clearly no worldwide privacy movement that has anything like the scale, resources, or public recognition of organizations in the environmental, feminist, or human rights fields. Rather, the privacy protection issue has yielded a loose, fragmented, and open-ended network of individuals and organizations, most of which have responsibilities beyond this issue.

Is this the way it has to be? The aim of the final chapter is to understand the conditions under which a more coherent international social movement for privacy (and against surveillance) might develop. Is the absence of such a movement inevitable and explicable because of the inherent properties of this issue? Or is it something that might very well arise given the correct agents and strategic choices? It is hoped that the scholarly literature on interest groups and resource mobilization, as well as theories of social movements and transnational activism, will provide some insights into these questions.

Privacy is often considered a highly abstract and subjective issue. Whereas it is possible to observe and measure the direct results of much environmental pollution, arguments against excessive levels of surveillance often have to be pitched in terms of abstract rights, personal perceptions and fears of hypothetical consequences. To be sure, many horror stories about the inappropriate collection and use of personal information can be marshaled to the cause. But still, after over thirty years of advocacy, the privacy movement in every country hears the familiar and quite bogus argument: "If you have nothing to hide, you have nothing to fear." The chapters that follow will give the lie to that argument. The collection, processing, and dissemination of personal data, without the individual's knowledge and consent, are profoundly and increasingly worrying to the individuals concerned. Furthermore, the ability to control the circulation of that information is being eroded with deep consequences for the relationships among the state, the market, and civil society. Surveillance has become a condition of modern societies. Some have tried to challenge and resist these developments. This is their story.

The Methodology

"*Their* story" or "*my* story"? The question is not easy to answer. I do regard myself as a privacy advocate. I appear in the media. I give testimony, and I comment on government and private-sector proposals. I have been a part of the privacy advocacy network both in Canada and internationally for over twenty years. The relationship, therefore, between myself and the people I am studying is not one of the researcher studying his "subjects." Neither, obviously, is it one about which I can be detached, objective, and dispassionate. I believe in this cause, and I am generally sympathetic when privacy advocates succeed and disappointed when they fail. I am also aware that their efforts have been marginalized and regarded as "extreme," "unrealistic," even "lunatic." Those views have occasionally translated into puzzled questions to me about why I am bothering to devote my time and resources to studying a set of actors, perceived by some to be at most an irrelevant irritant on the fringe of the more significant policy community. Obviously, I hope the pages that follow convince these skeptics.

My aim is to hold a mirror up to this privacy advocacy network in a way that has not been attempted before. Thus, I have tried as far as possible to allow these men and women to speak for themselves. I do not agree with everything that the people described in this book do or say; but that is not the point. In presenting the views and voices of privacy advocates, I do so not necessarily because they are correct according to any objective standard. The point is that they hold these views and that they provide a distinctive set of viewpoints on a critically important issue of the day.

One of my respondents, whose anonymity I will protect, offered the insight that "privacy advocates are not normal people." Normal people seek secure paying jobs in government, business, or academia. They do not sacrifice income to work in the nonprofit sector fighting powerful state and corporate interests. Many privacy advocates are euphemistically described as "characters." They are highly visible, somewhat egotistical, very smart, generally unconventional, and extremely interesting. With few exceptions, and paradoxically, they do not lead "private lives." They are extremely social, and they network an enormous amount. Many in this community also joke that the privacy advocates are the biggest gossips out there. So I am not studying here the anonymous foot-soldiers that comprise other social movements. Many of these advocates are "out there" actively trying to shape elite and mass opinion.

All of these realities have had some implications for how I have collected my data and presented my findings. I have to a significant extent relied on "key-informant" interviews with around thirty respondents in the United States, Canada, Australia, and several European countries. The full list of respondents, as well as my interview schedule, is included in the appendixes. The main criteria for selection is current, or former, affiliation with a group one of whose principal missions is to promote privacy protection or to resist excessive surveillance. The vast majority of these individuals are within "not-for-profit" groups, although as we will see, that distinction is sometimes difficult to sustain. I am also not confining my analysis to groups conventionally considered "privacy advocacy groups." More revealing, I have found, is to commence with the simple question: when surveillance practices emerge within a particular society, who resists and in what ways? In most countries, this question leads to some "usual suspects," but not always. As a participant in this network for over twenty years, I was at the outset quite familiar with the various advocates in different countries and naturally tended to commence my research with them. Throughout the initial interviews, others were then suggested and the network, as well as my list of respondents, expanded in ways typical of the "snowball-sampling" methods used within the social sciences.

What is less typical is that most of these interviews have been conducted on an attributed basis. I am aware that this technique is not common within research on social movement politics. Many studies (e.g., Luker 1984) find it important to quote the participants in their own words, but do so anonymously to encourage candor. Furthermore, in many studies, it simply is not important to know the name of the speaker, just that the respondent has a particular identity (national, ethnic, gender, and so on), and that a person with these attributes holds these views. For me, it makes no sense to quote my respondents as, for instance, a "prominent American privacy advocate." In the first place, most informed readers would probably guess the identity from the views expressed and the language used. But second, I make no pretense here that these views are representative of anybody except the person speaking. Hence, the narrative is sprinkled with attributed quotations from my interviews that are simply designed to exemplify or reinforce a larger point that I wish to make. Each of these quotations has been approved by the respondent in question.

I have been able to interview most respondents in person, although travel and resource constraints did necessitate a certain number of telephone conversations. In some cases, the context did not permit formal interviewing techniques. For example, many advocates do not have office space, necessitating more informal meetings in coffee shops and other locations; I have used these interviews more as background information. In a couple of instances, I have been able to engage the groups as a "participant observer." In all cases, I have been able to supplement the interview data with views and opinions expressed in the traditional media, on Web sites and in blogs. By and large, it has not been difficult to find out what privacy advocates think about the questions I am posing in this book.

Time and resource limitations obviously have meant that some individuals and groups have had to be left out. Some of those included might question my categories and my characterization of their roles. I can only plead the perennial scholarly defense that I had to draw the lines somewhere. Many will wonder about my selective presentation of evidence about their views and strategies. Others will see bias. However, and as explained earlier, this project is very much a pioneering study. At the very least, I do hope that this analysis convinces the reader that the privacy advocacy network has been important, that it is becoming more important, and that it deserves to be taken very seriously by policymakers in government and industry, as well as by academics.

Acknowledgments

My first acknowledgment, therefore, is to the men and women who granted me interviews for this project. I am part of their network, and this probably gained me a certain level of trust. But as I proceeded with the research, I began to realize how privileged I have been not only to study this important subject throughout my entire scholarly career but also to be associated with such an extraordinary group of individuals. I am also very grateful to an indeterminate number of advocates whom time and resources did not permit me to interview, including many within the community of international privacy and data protection commissioners. Numerous informal conversations and e-mail correspondence with others within the privacy community—in particular, Ann Cavoukian, Andrew Clement, David Flaherty, Bob Gellman, Ian Kerr, David Lyon, Gary Marx, and Stephanie Perrin—have influenced my views and indirectly found their way into these pages.

As we will see below, privacy advocates attend a lot of conferences. The formal presentations at these events, as well as informal networking, also contributed to my understandings and insights. The annual Computers, Freedom and Privacy (CFP) conference has been particularly valuable. I was also fortunate to participate in two research workshops dedicated to privacy advocacy: the Information Rights Workshop organized by Andrew Clement at the University of Toronto in June 2006; and the Privacy Workshop held at the University of California, Berkeley, School of Law in June 2007.

I am particularly indebted to these colleagues at the University of California, Berkeley. From January to July 2007, I was incredibly fortunate to enjoy a sabbatical leave at the Center for the Study of Law and Society (CSLS) at the UC Berkeley School of Law. The remarkable intellectual and cultural environment of Berkeley permitted me to draft this book, as well as to interact with some of the privacy scholars now there: Paul

Schwartz, Deidre Mulligan, Pamela Samuelson, James Rule, and Chris Hoofnagle. I am also grateful to Rosann Greenspan and Lauren Edelman who currently run the very successful Visiting Scholars program at the CSLS.

The work for this project has been funded by a grant from the Social Sciences and Humanities Research Council of Canada (Award 410–2004–0868). This grant allowed not only travel for research purposes but also the employment of hardworking and talented graduate research assistants from the MA program in the Department of Political Science at the University of Victoria: Meghan McCeachern, Sanda Farcas, and Ben Gonzales. I am especially appreciative of Meghan's transcription of my interviews. Also close to home, I would like to thank the man that runs an indispensable privacy press-clipping service through his Institute for the Study of Privacy Issues (ISPI), Mark Hughes. Charles Raab, Jim Rule, Paul Schwartz, and Warren Magnusson, each read various chapters and gave me valuable and critical feedback. Bob Prior and Alyssa Larose of MIT Press ensured that the publication process was timely and straightforward. And as ever, my lifelong gratitude to my wife, Robin Bayley, for support, encouragement, and tolerance of my moods when the writer's block hit.

The views of many privacy advocates are recorded in the pages that follow. There are many voices, but there is only one responsibility—my own. The book is dedicated to privacy advocates—anywhere and everywhere—however you want to define them.

List of Privacy Advocacy Organizations

Organization	Abbreviation	Country
Alfa-Redi		Peru
American Civil Liberties Union	ACLU	United States
Amnesty International	AI	International
Arbeitskreis Vorratsdatenspeicherung (Working Group on Data Retention)		Germany
Arge Daten		Austria
Association Electronique Libre (Electronic Freedom Association)	AEL	Belgium
Association for Technology and Internet	APTI	Romania
Australian Privacy Foundation	APF	Australia
Bits of Freedom	BoF	Netherlands
British Columbia Civil Liberties Association	BCCLA	Canada
Buro Jansen and Janssen		Netherlands
Californians against Telephone Solicitations	CATS	United States
Campaign for Digital Rights	CDR	United Kingdom
Canadian Civil Liberties Association	CCLA	Canada
Canadian Internet Public Policy Clinic	CIPPIC	Canada
CATO Institute	CATO	United States
Center for Digital Democracy	CDD	United States
Center for Democracy and Technology	CDT	United States
Chaos Computer Club	CCC	Germany
Coalition Against Unsolicited Commercial Email	CAUCE	United States
Computer Professionals for Social Responsibility	CPSR	United States (chapters in Canada, Spain, Peru, Africa, Japan)
Consumer Action	CA	United States
Consumer Association		United Kingdom
Consumers Against Supermarket Privacy Invasion and Numbering	CASPIAN	United States

Organization	Abbreviation	Country
Cyber-Rights and Cyber-Liberties		United Kingdom
Derechos Digitales (Digital Rights)		Chile
Deutsche Vereinigung für Datenschutz (German Association for Data Protection)	DVD	Germany
Die Humanistische Union (The Humanist Union)	HU	Germany
Digital Rights Denmark		Denmark
Digital Rights Ireland		Ireland
Electronic Frontier Finland	EFFI	Finland
Electronic Frontier Foundation	EFF	United States
Electronic Privacy Information Center	EPIC	United States
European Civil Liberties Network	ECLN	Europe
European Digital Rights Initiative	EDRI	Europe
FoeBuD		Germany
Förderverein Informationstechnik und Gesellschaft (Association for Information Technology and Society)	FITUG	Germany
Forum Informatikerinnen für Frieden and gesellschaftliche Verandwortung (Forum of Computer Professionals for Peace and Social Responsibility)	FIFF	Germany
Foundation for Information Policy Research	FIPR	United Kingdom
Foundation for Taxpayer and Consumer Rights	FTCR	United States
Frontline		Canada
Fundacion via Libre (Open Source Foundation)		Argentina
Global Internet Liberty Campaign	GILC	International
Health Privacy	HP	United States
ID Theft Resource Center	ITRC	United States
Imaginons un Réseau Internet Solidaire	IRIS	France
International Civil Liberties Monitoring Group	ICLMG	Canada
Internet Society		Bulgaria
Iuridicum Remedium		Czech Republic
Junkbusters		United States
La Ligue des Droits et Libertés (League of Rights and Liberties)		Quebec, Canada
Leave Those Kids Alone	LTKA	United Kingdom
Liberty Coalition		United States
Medical Privacy Coalition	MPC	United States
Motorists Against Detection	MAD	United Kingdom
National Association of State Public Interest Research Groups	US PIRG	United States
National Consumers League	NCL	United States
National Council for Civil Liberties	NCCL	United Kingdom
Netjus		Italy
Netzwerk Neue Medien (Network New Media)	NNM	Germany

Organization	Abbreviation	Country
New York Surveillance Camera Players	SCP	United States
NO2ID		United Kingdom
Patient Privacy Rights Coalition		United States
Privacy International	PI	United Kingdom
Privacy Rights Clearinghouse	PRC	United States
Privacy Ukraine		Ukraine
Privacy Activism		United States
Privacy Journal		United States
Privacy Mongolia		Mongolia
Privacy Times		United States
Private Citizen, Inc.		United States
Privaterra		Canada
Public Interest Advocacy Center	PIAC	Canada
Public Interest Computing Association	PICA	United States
Quintessenz		Austria
Seguridad en Democracia (Security and Democracy)	SEDEM	Guatemala
Statewatch		Europe
Stichtung Waakzaamheid Persoonregistratiie (Privacy Alert)		Netherlands
Swiss Internet User Group	SIUG	Switzerland
Transatlantic Consumer Dialogue	TCD	Europe
UK National Consumer Council	NCC	United Kingdom
Utilities Commission Action Network	UCAN	United States
Verbraucherzentrale Bundesverband (Federation of German Consumer Organizations)	VBV	Germany
Verein für Internet-Benutzer Österreichs (Association for Austrian Internet Users)	Vibe AT!	Austria
World Privacy Forum	WPF	United States

1 Framing the Problem

I give the fight up: let there be an end, a privacy, an obscure nook for me. I want to be forgotten even by God.
—Robert Browning, *Paracelsus* (1835)

We need an electronic bill of rights for this electronic age. . . . You should have the right to choose whether your personal information is disclosed; you should have the right to know how, when, and how much of that information is being used; and you should have the right to see it yourself, to know if it's accurate.
—Vice-President Al Gore, July 31, 1998

We are moving to a Google that knows more about you.
—Eric Schmidt, Google CEO, February 9, 2005

So what is the social problem, and how has it been defined and framed by privacy advocates? The answer is by no means clear as definitions and concerns about privacy have varied over time and according to national, cultural, and academic perspectives. "Privacy" is not a self-defining phenomenon, but a deeply contested concept that frames not one but a series of interrelated social and policy issues. The concept and the discourse can be, and are, molded to suit varying interests and agendas.

For any group that seeks to change public policy, or indeed the structural conditions that give rise to that policy, how issues get "framed" is crucial. Deriving originally from the work of sociologist Erving Goffman (1974), the concept of frames or framing is used to mean patterns of perception or methods of interpretation employed by social movement participants and organizations. A frame might be imagined as a kind of template or filter that organizes how one processes new information. For Sydney Tarrow, issue framing can define the crucial moment when politics expands into sustained interaction with opponents, and creates a social movement. Hence, for Tarrow, social movements should be based on "collective action frames that justify, dignify, and animate collective action." For "framing not only relates to the generalization of grievance, but defines the 'us' and 'them' in a movement's conflict structure" (1998, 21). David Snow has emphasized the importance of "frame alignment," the ability to render problems and events meaningful to a larger audience. There needs to be a resonance, therefore, between a network's interpretive work and the experiences of the broader political culture (Snow 1986, 464).

This chapter tries to trace the various ways that this cluster of issues has been framed in the academic literature and in social and political discourse. There is a framing of the issue around "privacy" and the attempts to draw ethical lines between the realm of the private and that of the social. There is a somewhat narrower framing of the issue around "information privacy," specifically focusing on the processing of personal data. There is also a framing of the problems around the concept of "surveillance" and the collective challenges that are posed when organizational imperatives combine with advanced information technology.

I trace these shifting conceptions in the academic literature, and then in various articulations by privacy advocacy groups. These frames are undoubtedly motivated by technological developments. However, they also reflect some interesting strategic choices about which messages "work" and which don't. For some, their arguments are influenced by the academic debate. Others have an aversion to theorization, preferring to base their activism on a set of basic and visceral instincts, and perhaps a moral authority, that can distinguish the intrusive from the nonintrusive, the acceptable from the unacceptable, and the just from the unjust. Lines therefore get negotiated and drawn—by scholars, by those with economic and political power, and by the advocates themselves.

The Privacy Frame

Although there is no consensus on how to define privacy, even in English-speaking nations, there is common agreement that privacy is something that every human being needs at some level and in some degree. This point is substantiated by a wealth of social psychological and anthropological evidence that has suggested that every society adopts mechanisms and structures (even as simple as the building of walls) that allow individuals to resist encroachment from other individuals or groups (Moore 1984).

As a clear organizational principle to frame political struggle, however, the concept leaves a lot to be desired. Scholars cannot make up their minds whether the problem stems from the fact that it is too narrowly focused on a conception of the individual subject or that it is too broad, vague, and protean. There have been many attempts to carve through the conceptual morass with definitions, taxonomies, and analytical frameworks. Yet after over thirty years of analysis, according to Daniel Solove, the concept is still in disarray: "Privacy seems to be about everything, and therefore it appears to be nothing" (2006, 479).

Let us begin with two sets of distinctions to help focus the analysis and summarize a very complicated and sprawling literature. The first relates to how one might draw the boundary between the public and the private; the second relates to the reasons or motives behind asserting a privacy claim, or why one might want to draw that boundary in the first place. The classic American definition of privacy offered at the end of the last century by Samuel Warren and Louis Brandeis ("the right to be let alone") embodies some subtle and important distinctions concerning what aspects of personal life should, in fact, be "let alone" (1890, 193). Further analysis suggests that there might be privacy of space, privacy of behavior, privacy of decisions, and privacy of information.

Many formulations and discussions of privacy adopt an explicit or implicit spatial dimension, and rest on the assumption that there is a "zone" or "realm" into which other individuals or organizations may not encroach—an "obscure nook" to quote Robert Browning in the epigraph to this chapter. The term "an Englishman's home is his castle" or the principle that the "state has no business in the bedrooms of the nation" (attributed to Pierre Trudeau, among others) are based on a conception of a spatial distinction, or a physical boundary between what is public and what is private. Contemporary concerns about the privacy of the physical person and its protection from various biometric devices are also centered on a notion of a physical or spatial boundary.

For others, the boundary is more properly drawn in terms of the specific behaviors, matters, or actions that should be shielded from intrusion. Take this justification by Charles Fried: "To respect, love, trust, feel affection for others, and to regard ourselves as the objects of love, trust and affection is at the heart of our notion of ourselves as persons among persons, and privacy is the necessary atmosphere for these attitudes and actions, as oxygen is for combustion" (1968, 477). Privacy is, therefore, essential for intimate behavior.

A third way to draw the line is in terms of individual decisions and choices. Privacy is essential for preventing coercive interference with decision making affecting intimate and personal affairs. This concept of decisional privacy has been relied upon, especially in American constitutional law, to protect decision making surrounding abortion, contraception, “lifestyle” choices, the right to choose one’s spouse, the right to follow one’s own sexual orientation and the right to rear one’s children in accordance with one’s own religious convictions (Allen 1988).

Finally, the boundary can be drawn in terms of information. Here the important point is not that certain information is perennially and inherently sensitive and therefore private, but that the individual should have a right to control its circulation. A number of definitions have centered on this informational aspect of the privacy question: “the control we have over information about ourselves” (Fried 1970, 140); “the individual’s ability to control the circulation of information relating to him” (Miller 1971, 25); the “claim of individuals, groups, or institutions to determine for themselves when, how and to what extent information about them is communicated to others” (Westin 1967, 7); and the “interest an individual has in controlling, or at least significantly influencing, the handling of data about themselves” (Clarke 1997). Definitions surrounding the concept of information tend therefore to emphasize the importance of “control” or “choice”—as in the quotation from Al Gore in the epigraph to this chapter.

It is clear that there is no single essential characteristic that all privacy violations share. Moreover, none of these spatial, behavioral, decisional, or informational distinctions can be absolute. Thus the state should have no interest in sexual relations between consenting adults in the privacy of their home, but it may have a significant interest in regulating such behavior in a public place. Decision making on intimate issues can never be wholly private. Neither can the control of personal information. Whether drawn in spatial, behavioral, decisional, or informational terms, each of these boundaries is inherently flexible, contestable, and dependent on context (Nissenbaum 2004). Privacy is not about isolation or removal from society, but about social relations. Social norms about privacy not only protect individuals but also regulate what can and should be done in the public domain (Schoeman 1992).

It is therefore useful to reflect on the purposes for the assertion of privacy claims. In previous work, I have distinguished among three overlapping dimensions of the problem: humanistic, political, and instrumental (Bennett 1992, 22–37). Fundamentally, privacy claims are made for humanistic reasons. Here the essential concern is to protect the dignity, individuality, integrity, or private personality of each and every one of us, regardless of wider implications or consequences. This notion corresponds broadly to what James Rule and his colleagues mean by an "aesthetic" conception of privacy or "the restriction of personal information as an end in itself" (Rule et al. 1980, 22). The fundamental issue is the loss of human dignity, respect, and autonomy that results when one loses control over the circumstances under which one's space, behavior, decisions, or personal information is intruded upon. These conceptions are at the heart of the privacy movement in virtually every democratic state.

A second dimension, however, is explicitly political. Privacy plays important functions within liberal democratic societies by preventing the total politicizing of life; it promotes the freedom of association; it shields scholarship and science from unnecessary interference by government; it permits and protects the use of a secret ballot; it restrains improper police conduct such as compulsory self-incrimination and "unreasonable searches and seizures"; and it serves also to shield those institutions, such as the press, that operate to keep government accountable (Westin 1967, 25). In a similar vein, Paul Schwartz (1999) has advanced a similar theory of "constitutive privacy" to protect the ability of individuals to speak freely and participate in public life on the Internet.

A third, and somewhat different, purpose is an instrumental, functional, or strategic one. The promotion of privacy may also serve to ensure that, in Paul Sieghart's terms, "the right people use the right data for the right purposes" (1976, 76). When anyone of those conditions is absent, critical rights, interests, and services might be jeopardized. This is an explicit concern about information, but it expresses a fundamental assumption that if you can protect the information on which decisions are made about individuals, you can also protect the fairness, integrity, and effectiveness of that decision-making process. In contrast to the first two concerns, this aspect of the problem stems not so much from the collection of personal data as from its use and dissemination. In this view, organizations can collect as much personal information as they like, provided there are adequate procedures in place to make sure that the "right people use it for the right purposes."

Privacy concerns go back centuries. And specific problems about how certain types of personal information in certain contexts, particularly medical contexts, have been the subject of claim and counterclaim, and regulatory and judicial decision making for a very long time. Privacy protection as a public policy question, however, is of more recent vintage. The issue came to the agenda of advanced industrial states in the late 1960s because of two main characteristics of post-industrialism —bureaucratization and information technology. When those forces reached a critical point in the 1960s and 1970s with the expansion of the state and the computerization of state functions, many Western societies then attempted to develop a coordinated public policy approach.

As a public policy question, governments tended to define the problem in informational, rather than in spatial, decisional, or behavioral terms. Even though some laws (such as in Canada, Australia, and the United States) are entitled "privacy acts," statutory protections have historically focused on the informational dimension of the problem, on the assumption that other aspects of the privacy question can be dealt with by the courts, or can be redefined or reduced to informational terms. And in general, policymakers have been more influenced by arguments of instrumental damage, than of aesthetic appeal. The argument that we all deserve privacy on a humanistic level is abstract. The position that individual interests can be harmed when personal information is processed inappropriately, especially if that position is supported by well-chosen horror stories, can have a more direct political appeal. The history of privacy, as a public policy (rather than a legal or ethical) issue has been dominated by a quite particular understanding of how the issue should be framed. Since the 1960s and 1970s, for better or worse, this informational and instrumental conception of privacy has tended to drive policy debate and has set national and international policy choices on a particular trajectory.

The Information Privacy Frame

The concept of informational privacy (sometimes referred to as data privacy) arose in the 1960s and 1970s at about the same time that "data protection" (derived from the German *Datenschutz*) entered the vocabulary of European experts. The notion is closely connected to the information processing capabilities of computers, and to the need to build protective safeguards at a time when large national data integration projects were being contemplated in different advanced industrial states. These projects raised the fears of an omniscient "Big Brother" government with unprecedented surveillance power.

The overall policy goal in every country has been to provide individuals greater control of the information that is collected, stored, processed, and disseminated about them by public and private organizations. This goal was prominent in English-speaking countries, as well as in continental Europe. The concept of *Informationsselbstbestimmung* (informational self-determination) was later developed and given constitutional status in Germany. Control over personal information means rights for the individual, as well as obligations for organizations. It therefore yields a number of basic principles for personal information management. These "fair information principles" can be briefly traced to policy analysis in Europe and the United States in the late 1960s and early 1970s (Bennett 1992, 95–115), and were soon regarded as a logical regime for the protection of information privacy rights. Those experts who were attempting to resolve this issue in national arenas shared a strong desire to draw lessons from their counterparts overseas and produced an international consensus on how best to resolve the privacy problem through public policy. These analytical efforts led to the world's first "data protection" or "information privacy" statutes (Bennett 1992).

The fair information principles (FIPs) can be distilled to the following: An organization (public or private):

- must be accountable for all the personal information in its possession
- should identify the purposes for which the information is processed at or before the time of collection
- should only collect personal information with the knowledge and consent of the individual (except under specified circumstances)
- should limit the collection of personal information to that which is necessary for pursuing the identified purposes
- should not use or disclose personal information for purposes other than those identified, except with the consent of the individual (the finality principle)
- should retain information only as long as necessary
- should ensure that personal information is kept accurate, complete, and up-to-date
- should protect personal information with appropriate security safeguards
- should be open about its policies and practices and maintain no secret information system
- should allow data subjects access to their personal information, with an ability to amend it, if inaccurate, incomplete, or obsolete (Bennett and Grant 1999, 6).

These principles are also conceived in relative terms. Each must be balanced against correlative rights and obligations to the community.

The fair information principles appear either explicitly or implicitly within all national data protection laws, including those in the United States, Australia, New Zealand, and Canada that are called privacy acts, as well as in self-regulatory codes and standards. They have also spread as a result of international agreements. The increasing ease with which personal data might be transmitted outside the borders of the country of origin has produced an interesting history of international harmonization efforts, and a concomitant effort to regulate transborder data flows. In the 1980s, these harmonization efforts were reflected in two international agreements, the 1981 Guidelines from the Organization for Economic Cooperation and Development (OECD 1981), and the 1981 Convention from the Council of Europe. In the 1990s, these initiatives were extended through the 1995 European Union Data Protection Directive, which tries to harmonize European data protection law according to a higher standard of protection and to impose that standard on any country within which personal data on European citizens might be processed.[1] In this decade, there have also been attempts to extend their reach to the Asia-Pacific region (Greenleaf 2005).

Despite this harmonization there are, of course, continuing debates about how the FIPs doctrine should be translated into statutory language (Bygrave 2002). There are disputes for example: about how to regulate the secondary uses of personal data—through a standard of relevance, or through specific provisions about the legitimate custodians of those data; about the limitation on collection principle and to what extent the organization should be obliged to justify the relevance of the data for specific purposes; about the circumstances under which "express" rather than "implied" consent should be required; and about the distinction among collection, use, and disclosure of information, and whether indeed these distinctions make sense and should not be subsumed under the overarching concept of "processing." How these and other statutory issues are dealt with will, of course, have profound implications for the implementation of privacy protection standards within any one jurisdiction.

The laws have also differed on the extent of organizational coverage—those in North America and Australia have historically mainly regulated public-sector agencies plus selected sectors of private industry, whereas those elsewhere (especially in Europe) encompass all organizations. In recent years this distinction has all but disappeared as countries like Canada, Australia, and Japan have introduced information privacy statutes for the private sector. In most countries (with the notable exception of the United States) these laws are overseen by small privacy or data protection agencies with varying oversight, advisory, or regulatory powers. Some of these agencies have strong enforcement and regulatory authority; others act as more advisory "ombudsman-like" bodies. Some are headed by a collective commission (such as in France), others (such as in Canada and Australia) by a single "privacy commissioner" or "data protection commissioner." One of the effects of the 1995 EU Data Protection Directive has been to extend the process of policy convergence beyond the level of basic statutory principles. This directive also pushes for greater conformity in how these principles are enforced through a "supervisory authority." Moreover, the principle of independent oversight is also regarded as a test of the "adequacy" of data protection in non-European countries. The process of convergence of data protection norms is extending geographically and deepening in meaning and content (Bennett 1997).

Thus, in just forty years, there exists a broad and diverse policy sector embracing a very large number of government officials, lawyers, independent consultants, chief privacy officers, technology providers, academics, and nongovernmental organizations. The "governance of privacy" is a responsibility of many actors operating at different international, national, and local levels. The issue has become institutionalized. As a policy sector, it is not going away. Too many people have a stake in its continuation.

The Surveillance Frame

According to some, however, just as laws are not going to go away, neither are the institutions and technologies of surveillance. At the same time as there has been an undeniable expansion of the policy sector and a "trading-up" of laws and regulations, there has also been a growing body of criticism about whether the concept of privacy, and the policies it generates, are equal to the scale of the social problem (Lyon 2001; Rule et al. 1980; Gandy 1993). For some, privacy is simply not the "antidote to surveillance" (Stalder 2002).

There are several intertwined elements to this critique pitched at different conceptual and practical levels. Philosophically, privacy has its roots in liberal individualism and is perhaps not reflective of the complex subjectivities and identities characteristic of the modern world. Privacy tends to reinforce individuation, rather than community, sociability, trust, and so on. It therefore never challenges the larger questions of categorical discrimination. Individuals are arguably placed at risk because of their membership in certain groups, rather than on the basis of their individual identities and the personal information it generates (Gandy 1993).

As a legal right, some have also pointed out that privacy is plagued with some of the same problems associated with the rights discourse more generally (Haggerty and Erickson 2006, 9). As a legal concept it pushes debate toward experts and authorities and fails to serve the people most at risk (Gilliom 2006, 123). At root, privacy claims tend not to see surveillance as a social question, but as a problem that can be addressed by properly implementing the fair information principles doctrine in relation to the personal data on discrete individuals. Thus contemporary information privacy legislation is designed to manage the processing of personal data, rather than to limit it. From the perspective of those interested in understanding and curtailing excessive surveillance, the formulation of the privacy problem in terms of trying to strike the right "balance" between privacy and organizational demands for personal information does not address the deeper issue and cannot halt surveillance. Information privacy policies may produce a fairer and more efficient use and management of personal data, but they cannot control the voracious and inherent appetite of modern organizations for more and more increasingly refined personal information (Rule et al. 1980).

There have been attempts to realign, rather than abandon, the privacy concept. Priscilla Regan, for instance, has argued that privacy should be seen as a common value, "in that all individuals value some degree of privacy and have some common conceptions about privacy." It is a public value, "in that it has value not just to the individual... but also to the democratic political system." And it is a collective value, "in that technology and market forces are making it hard for any one person to have privacy without all persons having a similar minimum level of privacy" (Regan 1995, 213). She contends that an individualistic conceptualization of privacy does not serve the privacy advocate well. Her analysis suggests that privacy, framed in individualistic terms, is always on the defensive against arguments for the social benefits of surveillance. Privacy will always be in conflict with those social and collective issues, which tend to motivate general publics and their representatives. We must, therefore, frame the question in social terms. Society is better off if individuals have higher levels of privacy.

For others, however, the way to frame the problem is not in terms of protecting privacy, but of curtailing excessive surveillance. In popular parlance, surveillance has historically been associated with the notion of observing, normally by visual means, people under "suspicion."[2] More scholarly definitions tend to be more inclusive. Rule and his colleagues, for instance, suggest that surveillance is "any systematic attention to a person's life aimed at exerting influence over it" (Rule et al. 1983, 223). David Lyon states that surveillance is "any collection and processing of personal data, whether identifiable or not, for the purposes of influencing or managing those whose data have been garnered" (2001, 2). In later work he adds that surveillance is the "focused, systematic and routine attention to personal details for purposes of influence, management, protection or direction" (Lyon 2007, 14).

It has also become evident that surveillance is often as much about classification or "social sorting" as about monitoring (Lyon 2003a). Surveillance therefore discriminates, in both passive and negative senses of that term. It is "Janus-faced"; the same process both empowers individuals but also constrains them. It gives us a variety of advantages (security, convenience, ease of communication, and so on). It also enhances the power of the modern organization to the detriment of individual liberties and to the disadvantage of marginalized groups. Lyon demonstrates how surveillance systems have grown up to compensate for the weakening of face-to-face social relationships in which mechanisms for social integration are increasingly removed and abstract. Surveillance, then, is the necessary glue that builds trust throughout a "society of strangers." The "Invisible Frameworks" of integrated information and communications networks contribute to the "orchestration" of this society of strangers. These same trends have been reinforced in the wake of 9/11 and the global "war on terror" (Lyon 2003b).

For modern sociology, surveillance is a condition of modernity, integral to the development of disciplinary power and new forms of governance (Haggerty and Erickson 2006, 4). It is integral to the development of the nation state, and to the decentered forms of disciplinary power and "governmentalities" inherent within modern neo-liberal societies (Foucault 1991). It is also central to the new order of global capitalism (Deleuze 1992). It is *that* important.

Surveillance therefore now embraces a far broader recognition of the agents and subjects of monitoring. It is not only about powerful organizations controlling hapless subjects. Figure 1.1 attempts to convey the more routine or everyday forms of surveillance in modern societies. It displays a simple four-cell typology distinguishing between the watchers and the watched, and organizations (public and private) and individuals.

		THE WATCHERS	
		Organizations	*Individuals*
THE WATCHED	*Organizations*	1 “Oversight”	3 “Sousveillance”
	Individuals	2 “Surveillance”	4 “Peer Monitoring”

Figure 1.1
A typology of surveillance practices.

Box 1, where the watchers and the watched are both organizations captures an admittedly broad range of practices where organizational accountability is at stake. Surveillance can then occur through a range of oversight mechanisms: auditing, legislative investigation, regulatory accountability, safety inspections, and so on. The word is increasingly used in this sense, particularly within the context of laboratory surveillance by governmental health or environmental protection agencies to enhance safety.[3] The quality assurance inspections conducted in the course of obtaining registration to the ISO 9000 standards are also sometimes called ‘‘surveillance audits.’’

Box 3 embraces a range of practices where the individual monitors the organization. This practice is consistent with what Steve Mann, researcher at the University of Toronto and pioneer of ‘‘wearable computing,’’ calls ‘‘sousveillance,’’ stemming from the contrasting French words *sur*, meaning above, and *sous*, meaning below. Surveillance connotes a kind of omniscient eye-in-the-sky. It is often equated with the notion of ‘‘panopticism’’ whereby the very possibility of observation constructs a set of power relations between the watched and the watchers such that the latter are self-disciplined to conform even though they may not be observed constantly at every hour of the day. Conversely, sousveillance involves the recording of the activities of the observers by the observed.

Sousveillance seeks to decentralize the observation, thus inverting the panopticon and achieving ultimately a state of "equiveillance."[4]

Mann provides several contemporary examples of sousveillance: a taxicab passenger photographs the driver to keep tabs on his behavior; a 1-800 number with "Am I driving OK?" on a truck so citizens can report the behavior of the driver to the trucking company; student evaluations of professors;[5] shoppers keeping tabs on shopkeepers (reporting misleading advertising, unsafe fire exits, etc.).[6] "Sousveillance" is also deeply integrated into Mann's own aesthetic critique of surveillance through the development of "wearable computing" devices.[7] His methods are controversial, especially when they involve the photographing of low-level clerks, security personnel, and others not directly responsible for organizational policy. Other attempts to subvert surveillance technology include, most notably, the New York Surveillance Camera Players (SCP), who have gained a notoriety for their regular performances of such classics as Samuel Beckett's *Waiting for Godot*, Edgar Allen Poe's "The Raven," and, of course, George Orwell's *1984* in front of the video-surveillance cameras on the Manhattan subway.[8]

"Peer monitoring" (included in Box 4) has been the subject of some very interesting recent analysis of how ordinary individuals are increasingly encouraged to keep tabs on their fellow citizens. These forms of surveillance tend to find the most chilling examples in more authoritarian regimes through accounts, in particular, of the reliance on informants of the secret police in Eastern Europe (Ash 1997; Funder 2003). But there also seems to be a trend in more democratic states toward individual-individual monitoring. Voyeurism, of course, is one aspect of this form of monitoring—a practice so brilliantly critiqued in Gary Marx's fictional description of the behavior of his Thomas I. Voire (Marx 2003). Voyeurism has also, of course, reached new levels of intrusiveness with the ready availability of camera phones, and other mobile surveillance toys, used to satisfy the prurient interest.

More interesting perhaps are the ways in which individuals become the watchers, either through a subtle process of cooptation or through clever marketing. Recent empirical work suggests that there are a host of "peer-monitoring" or "lateral surveillance" examples from neighborhood watch schemes, to landlord/tenant monitoring, to citizens groups that publicize the vehicle license nos. of those suspected of soliciting prostitutes, to Web cams for the surveillance of children, teenagers, domestic employees, to the locational devices that can be embedded in automobiles to monitor speed, safety procedures, drug/alcohol use, and so on (Wood 2004). Peer-to-peer monitoring was also institutionalized in the United States after 9/11 through Operation TIPS, a program that allows ordinary Americans, such as mail carriers, meter readers, and repair service persons, to act as informants about any suspicious terrorist activity that they might encounter in their professional capacities. Inevitably, somebody then set up a Web site for "Operation TIPS-TIPS" through which people could report on the alleged informants.[9] There is nothing new about this kind of peer-to-peer monitoring in the United States. From 1915 to 1917, the American Protective League boasted around a quarter million badge-wearing members, who proudly informed the Justice Department about any suspicious activity, especially among those citizens of German origin.

Despite these interesting examples, the vast majority of surveillance literature has centered on the monitoring of individuals by organizations (Box 2), and this is the meaning most commonly understood in the literature and implied in the various definitions. Lyon stresses the systematic and the routine, but he also concedes that "surveillance in the end directs its attention to individuals" (Lyon 2007, 14). It is also about how ordinary people in their roles as citizens, workers, travelers, consumers, and so on, interact with surveillance—how they comply, negotiate, and perhaps resist.

This idea that advanced industrial societies are creeping inexorably toward an unacceptable level of surveillance has influenced writers from a number of disciplinary and national backgrounds. David Flaherty, a Canadian scholar of legal history, ended up calling his comparative analysis of the operation of data protection laws in Germany, Sweden, the United States, France, and Canada, "Protecting Privacy in Surveillance Societies." He begins: "The central theme of this volume is that individuals in the Western world are increasingly subject to surveillance through the use of databases in the public and private sectors, and that these developments have negative implications for the quality of life in our societies and for the protection of human rights" (1989, 1).

In the 1970s and early 1980s, the general assumption was that privacy problems stemmed from the centralized and coordinated control of personal information held by governments in discrete, mainframe "databanks." To the extent that private-sector organizations were a matter of concern, advocates tended to focus on the most visible and monopolistic corporations and on the subject of the majority of complaints—namely, the consumer credit industry. This industry was also the first to be subject to regulation for its personal data processing practices. Throughout the 1980s and 1990s, however, it was either obvious that the private sector deserved as much attention as the public, or that it was increasingly difficult to tell the difference between the two.

The notion of "monitoring" also comes under critical scrutiny in the 1990s. These and other trends lead Philip Agre (1994) to the conclusion that a "capture" model is just as evocative as a "surveillance model" to represent the new commodification of personal information. This model is built upon linguistic rather than visual metaphors and has its roots in the disciplinary practices of applied computing rather than in the historical experiences of the "surveillance state." Others have written about "surveillance by design" and how the capacity to capture personal information can become embedded within the architecture of information systems (Samarajiva 1996). More recently, however, Haggerty and Erickson have pointed out that this "capture model" also has its shortcomings because the ongoing politics of surveillance more often involves the provision of "inducements and enticements at the precise threshold where individuals will willingly surrender their information" (2006, 12). Thus privacy is not "invaded," "breached," or "violated"; it is surrendered within the many transactions and relationships that constitute modern life.

Roger Clarke (1988, 1997) found it necessary to coin a new word—"dataveillance"—to describe these new forms of surveillance that are facilitated, not by direct visual or audio monitoring, but by the manipulation of personal data. He contends that the "Big Brother" scenario has not arrived because it is unnecessary. Besides, dataveillance, according to Clarke, is more efficient, whether from a technical, economic, or political standpoint. There is a wide, and imperfectly understood, range of practices for the analysis of personal data currently used by modern institutions. Dataveillance practices vary along five different dimensions: (1) whether personal or mass dataveillance is being conducted; the former involves the analysis of the records of individuals who have already attracted attention, the latter begins with no a priori knowledge of the subjects who may warrant attention; (2) whether the dataveillance is internal or external to the agency that initially collected the data; (3) whether the analysis is upfront or post facto, that is whether the check is made before or after an individual receives a government benefit of service; (4) whether the analysis is conducted on a single variable, or a multiple number of variables (such as when profiling occurs); and (5) whether the practices have a negative or positive impact on individuals (Bennett 1996). Dataveillance, therefore, facilitates the integration of surveillance capabilities across institutional, technological, and national boundaries.

As technology has become smaller, less expensive, and more decentralized, analysts have argued that a "new surveillance" is at work that transcends distance, darkness, and physical barriers: "The awesome power of the new surveillance," Marx summarizes, "lies partly in the paradoxical, never-before-possible combination of decentralized and centralized forms" (1988, 217). Philip Agre and Marc Rotenberg observed a "new landscape" for privacy and technology "that is more variegated, more dangerous, and more hopeful than before" (1997, 1). Haggerty and Ericson (2000) coined the term the "surveillant assemblage" to capture the ability of various institutional actors to integrate, combine, and coordinate various personal information systems to extend and intensify processes of social control. They paint a picture of complex and intertwining flows of personal data that are abstracted from humans and their territorial locations. These flows are then reassembled in different locations as discrete and virtual "data doubles." They emerge to the surface in rather the same way that a rhizomatic root structure produces different manifestations above the surface of the earth.

Hence, when we observe the nature of surveillance in the first decade of the twenty-first century, a number of trends have been at work producing the many and various practices that in turn have animated the actions of privacy advocates. First, surveillance trends have completely eroded traditional distinctions between public and private sectors. The flows of personal data now percolate through systems that are more porous, and less discrete. Second, it is also commonly agreed that we need to concentrate on a further dimension of the privacy problem—not only who we are and what we are doing but also where we are doing it. We are now a "mobile" society, and there is extraordinary potential for "mobile" surveillance (Bennett and Regan 2004). Third, surveillance targets not only "suspects" but everyone. It is about the "monitoring of everyday life" (Lyon 2001). Contemporary surveillance has developed largely through the uncontrolled decisions of thousands of decentralized organizations and individuals, all making supposedly rational decisions that one more incremental invasion of privacy is a price worth paying for greater efficiency, security, profit, and so on. Surveillance has become everyday, routine, and mundane. Finally, the tools of surveillance are becoming more decentralized, culminating in the visions of ubiquitous computing, and the Internet of things, realized through the spread of radio frequency identification devices (RFIDs). Each of these themes will resurface during our later discussion of privacy advocacy.

In summary, the literature on surveillance leaves us with the overwhelming message that the quantity and quality of monitoring have changed. It is not just that we have less "privacy" but that these new surveillance practices have produced qualitative changes in how we subjectively experience our interactions with institutions and technologies. As Haggerty and Erickson put it: "Privacy invasions now often *feel* different than they did in the past" (2006, 11).

Perhaps all these trends suggest that the lines articulated in the heuristic framework of figure 1.1 have all but broken down. However, there is now some critical debate about the breadth and inclusiveness to the concept of surveillance, which has been expanded to embrace any capture of personal information, whether identifiable or not, and whether having positive or negative implications for the individual. It too, therefore, is a concept that carries a lot of theoretical baggage, and is in danger of being stretched so far that it, like "privacy," might mean everything and nothing.

In particular, there is arguably an important distinction between the collection of personal data and the subsequent analysis of that data for the purposes of making a decision about that person. The routine capture of personal data is a feature of modern societies whenever we book an airline ticket, make a credit card purchase, reserve a hotel room, surf the Internet, or make a cellular phone call. But, as I have contended elsewhere (Bennett 2005), the everyday capture and storage of such data is qualitatively different from the use of that data to determine whether the person should or should not fly, would or would not be a credit risk, will or will not be able to pay his hotel bill, may or may not be downloading child pornography, or is or is not a terrorist threat. The analysis of the risks of surveillance needs to be sensitive to the distinction between the routine capture of data and the subsequent use of that data. The concept of "surveillance" conflates many processes and motivations.

Framing Dilemmas

Hence, surveillance is everywhere and it is getting more complex, latent, and subtle. It is a central feature of modern life. It is challenged by a value that has also been impossible to define and that many scholars regard as inadequate—conceptually, legally, and practically. This incomplete sketch of a sprawling literature suggests, therefore, that the people who might want to challenge these developments face some profound dilemmas about how the social and political problem (or problems) might be "framed." It is one thing for academics to analyze and frame understandings of how these issues have developed, and how they should be framed. It is another thing for those who actively press for social change.

The last portion of this chapter looks at the way these various themes have played out in the stated motivations and goals of contemporary privacy advocates. For the social and political activist, the breadth and complexity of the problems produce a number of tricky strategic dilemmas, through which they have to navigate. These dilemmas are manifested on two levels, within the formally stated mission statements of the various organizations, as well as in the more informal perceptions of the individual activists.

Very few people within the privacy advocacy network operate within any fixed and guiding definition of what privacy means. Organizations have tended not to waste valuable time parsing the many definitions, and arguing about concepts and doctrine. The term "privacy" is used over and again, but it is rarely given a clear definition within the various mission statements of privacy organizations. There does tend to be a pervasive "I don't know what it is, but I know it when I see it" assumption. At the same time, there are some different approaches to issue framing.

First, there is a dilemma about whether to regard privacy in its fullest manifestations, and thus broader than information privacy or data protection. When Privacy International (PI) was founded in 1990, the founder, and current director general, Simon Davies, argued forcefully for the need for a broader approach:

> Privacy should not be regarded merely as data protection. Data protection appears to be quite clearly a sub set of privacy, and for the sake of maintaining clarity of the issues it should remain so. If all privacy matters were interpreted as data protection, solutions would generally be juridical and legal rather than being subjected to the broader range of influences. In addition, data protection surely cannot exist where there is no obtainable data, and those familiar with Foucault's principle of the panopticon representing the surveillance state will understand that privacy must surely have wider parameters.[10]

In a similar vein, British Columbia's Freedom of Information and Protection of Privacy Association (FIPA) defines privacy as "the ability or right to have a 'private life'—to be left alone, free from illegal or unwanted scrutiny and intrusions. Privacy rights include informational privacy—the right to control or limit the collection, use, and disclosure of one's own personal information by other agencies, whether they are part of government or the private sector."[11]

Yet others seem to be more comfortable with focusing on the information privacy aspects, and thus mirroring and overshadowing the work of the official data protection agencies. For example, there is an Austrian organization called ArgenDaten, and a Deutsche Vereinigung for Datenschutz (German Association for Data Protection). A focus on digital technology also tends to be accompanied by an emphasis on the informational dimensions of the issue. The Center for Digital Democracy's (CDD) specific reference to the fair information principles and its attempt to justify privacy as a necessary condition for the enjoyment of other democratic rights resonates with some of the themes discussed earlier:

> Information privacy is the right to control the collection and use of personal information. And Fair Information Practices provide that control. A concept developed in the 1970s, Fair Information Practices provide individuals with the right to have information collected only with consent, updated and maintained accurately, collected for a specific purpose, secured from unauthorized access or alteration, used only with knowledge of what will be done with the data, provided with the ability to view and correct data after collection, and ensured a means to hold the data collector accountable.[12]

Similarly, the Global Internet Liberty Campaign advocates: "Ensuring that personal information generated on the GII [global information infrastructure] for one purpose is not used for an unrelated purpose or disclosed without the person's informed consent and enabling individuals to review personal information on the Internet and to correct inaccurate Information."[13]

A second dilemma relates to whether or not privacy is justified in universal or national terms. Many American groups, for example, take pains to stress how the value is rooted in their own constitutional traditions. The Electronic Privacy Information Center (EPIC), for example, contextualizes its goals in terms of bedrock American principles: "[EPIC] was established in 1994 to focus public attention on emerging civil liberties issues and to protect privacy, the First Amendment, and constitutional values."[14] As does the Privacy Coalition (coordinated through EPIC): "Privacy is one of America's most fundamental values. The Fourth Amendment states that 'The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated.' In addition, the U.S. has adopted many laws protecting Americans from privacy invasive practices by both the public and private sectors."[15] One of the strongest national privacy groups exists in Australia. The Australian Privacy Foundation (APF) "is the primary association dedicated to protecting the privacy rights of Australians. The Foundation aims to focus public attention on emerging issues that pose a threat to the freedom and privacy of Australians. The Foundation has led the fight to defend the right of individuals to control their personal information and to be free of excessive intrusions."[16]

A third tension exists with respect to the relationship between privacy and related human rights and civil liberties. For some groups, privacy protection is justified and contextualized within a broader suite of civil liberties, especially in relation to the Internet and a wider conception of "digital rights." The Center for Democracy and Technology (CDT), for instance, "works to promote democratic values and constitutional liberties in the digital age.... Our mission is to conceptualize, develop, and implement public policies to preserve and enhance free expression, privacy, open access, and other democratic values in the new and increasingly integrated communications medium."[17] The Electronic Frontier Foundation (EFF) has a similar identity: "EFF continues to confront cutting-edge issues defending free speech, privacy, innovation, and consumer rights today. From the beginning, EFF has championed the public interest in every critical battle affecting digital rights."[18]

A fourth tension is also observed over the question of whether privacy is a fundamental or an instrumental value. The Center for Digital Democracy explains how "privacy is important to enhance other rights such as free speech or freedom of association. By withholding identity, some may be more willing to voice political or controversial speech—thus promoting diversity in civil discourse."[19] Similarly, and in the case of the Health Privacy Project: "A substantial barrier to improving the quality of care and access to care is the lack of enforceable privacy rules. Individuals share a great deal of sensitive, personal information with their doctors.... Without adequate privacy protections, individuals take steps to shield themselves from what they consider harmful and intrusive uses of their health information often at significant cost to their health.[20]

Yet other groups frame the issues in larger sociological terms about surveillance. The American Civil Liberties Union (ACLU), for instance, notes the "the tremendous explosion in surveillance-enabling technologies, combined with the ongoing weakening in legal restraints that protect our privacy have us drifting toward a surveillance society. The ACLU's Technology and Liberty Project fights this trend and works to preserve the American tradition that the government not track individuals or violate privacy unless it has evidence of wrongdoing."[21]

A Dutch group, Bits of Freedom (BoF), gets a little more specific:

> During the past 6 years both governments and companies have initiated many measures and activities that have endangered civil rights. Governments have extended their powers in many ways. Instead of dedicated investigations into the activities of people suspected of serious crimes, law enforcement authorities silently but massively revert to data-mining techniques to examine the daily behaviour of innocent citizens.... But besides government, industry also plays a very important role in the increasing control of the behaviour of citizens and consumers. This tendency is illustrated by developments such as mandatory data retention, the proposed central storage of biometric passport data and the central storage of travel-data created by the new national public transport chip card.[22]

And then there are groups that take a more radical posture, regarding the advancement of privacy rights as a way to control, perhaps dismantle, the "surveillance state." The Surveillance Camera Players, for instance, are: "completely distrustful of all government.... We protest against the use of surveillance cameras in public places because our cameras violate our constitutionally protected right to privacy.[23] The International Campaign Against Mass Surveillance argues:

> This new "security" paradigm is being used to roll back freedom and increase police powers in order to exercise increasing control over individuals and populations. Under the public's radar screen, a registration and surveillance infrastructure of global reach is quietly being constructed. It includes the convergence of national and international databases, the creation of data profiles for whole populations, the creation of a global ID system, the global surveillance of movement, and the global surveillance of electronic communications.... Governments around the world must abandon the intrusive and discriminatory measures inherent in the practice of mass registration and surveillance, and put the genuine protection and development of citizens—in the fullest sense, including the protection of our rights—at the centre of any approach to "security."[24]

For some groups, therefore, privacy is simply not the issue, but the nexus among the state, capitalism, and new information technology producing unprecedented surveillance capabilities. The issue is simply about power.

Conclusion: Privacy, Surveillance, and Power

I will paint a more comprehensive picture of the entire range of groups that advocate for privacy in the next chapter. The above statements, strategies, purposes, and rhetoric simply offer a preface to the groups and themes discussed in this book.

Earlier, I drew a distinction among humanistic, political, and instrumental motivations behind privacy protection, each of which is expressed in the quotations above. Some groups see the issue in terms of promoting and protecting an essential human dignity. Others emphasize political dimensions, seeing privacy as one value that can be advanced to control the worst effects of power (public and private). Others view it in instrumental terms—to advance better health care, to promote a free and unregulated Internet, to advance consumer protection, and so on.

It is also instructive how some advocates stress individual protection, while others see the value in a social framework. The word "surveillance" is explicit in the framing of the issue by some groups, thus posing the question in more collective terms: "is this the kind of society we wish to live in?" The distinction is important, and we will return to it. New technologies—video surveillance, for instance—can be used in ways that are detrimental to individual privacy rights; tapes can be inappropriately accessed, individuals might be victims of mistaken identity, they might be recognized in contexts that they would rather keep confidential, and so on. At an individual level, we have plenty of evidence that informational privacy rights can be violated by this technology, occasionally inspiring complaints and litigation. But the issue can also be framed in social terms: "do we wish to live in a society in which cameras are monitoring our every move?" Some groups tend to see the issue in this broader framework; others are directed by the desire and need to resolve the individual grievance.

Some groups see the issues in international, perhaps global, terms. Others tend to be more focused on specific countries. Some have a very broad technological span. Others prefer to concentrate their efforts on a selection of the more intrusive practices. Some see their mandate as to protect individuals as "citizens"; others focus on "consumers." For some groups, privacy is the central focus. For others it is one of a suite of civil liberties and rights necessary for the protection of liberal democracy. For some, whether surveillance is offline or online is immaterial. For others it is crucial; privacy rights are one frontier over which the essential structure of the Internet is being fought.

These are merely tendencies, and we should not read too much into differences of emphasis, nor of course infer that these statements have been carefully considered, debated, and ratified as accurate expressions of organizational purpose. Nor should it be inferred that these various justifications actually motivate the individual activists. One very powerful theme that animates privacy advocates is the abuse of power. Many, as we will see, get their batteries recharged when they force a powerful organization on the defensive, or embarrass an arrogant minister or CEO, or catch those organizations in a lie. Privacy is one vehicle, among many, for redressing the balance between the powerful and the powerless.

After we have examined the organization, networking, and strategies of privacy advocacy groups in the pages that follow, it will be possible to address in a more sustained manner the central question about whether, in Tarrow's terms, there is a "generalization of grievance" that defines the "us and them" in the conflict structure. It is clear that privacy is a multidimensional and often subjective value. It can mean a lot of things, and it can mean different things to different people. But, despite the conceptual confusion, for better or worse, privacy is still the concept around which the major policy issues have been framed (at least in the English-speaking world) for more than forty years. And "privacy advocates" have learned to live with it.