ROUTLEDGE STUDIES IN SCIENCE, TECHNOLOGY AND SOCIETY

Transparency and Surveillance as Sociotechnical Accountability

A House of Mirrors

Edited by
Deborah G. Johnson
and Priscilla M. Regan

Transparency and Surveillance as Sociotechnical Accountability

Surveillance and transparency are both significant and increasingly pervasive activities in neoliberal societies. Surveillance is taken up as a means to achieving security and efficiency; transparency is seen as a mechanism for ensuring compliance or promoting informed consumerism and informed citizenship. Indeed, transparency is often seen as the antidote to the threats and fears of surveillance. This book adopts a novel approach in examining surveillance practices and transparency practices together as parallel systems of accountability. It presents the house of mirrors as a new framework for understanding surveillance and transparency practices instrumented with information technology. The volume centers around five case studies: Campaign Finance Disclosure, Secure Flight, American Red Cross, Google, and Facebook. A series of themed chapters draws on the material and provides cross-case analysis. The volume ends with a chapter on policy implications. This volume was produced as part of a National Science Foundation–funded project bringing together an interdisciplinary team of scholars.

Deborah G. Johnson is Anne Shirley Carter Olsson Professor of Applied Ethics in the Department of Science, Technology, and Society at University of Virginia.

Priscilla M. Regan is Professor in the Department of Public & International Affairs at George Mason University.

Routledge Studies in Science, Technology and Society

1 **Science and the Media**
Alternative Routes in Scientific Communication
Massimiano Bucchi

2 **Animals, Disease and Human Society**
Human-Animal Relations and the Rise of Veterinary Medicine
Joanna Swabe

3 **Transnational Environmental Policy**
The Ozone Layer
Reiner Grundmann

4 **Biology and Political Science**
Robert H. Blank and Samuel M. Hines, Jr.

5 **Technoculture and Critical Theory**
In the Service of the Machine?
Simon Cooper

6 **Biomedicine as Culture**
Instrumental Practices, Technoscientific Knowledge, and New Modes of Life
Edited by Regula Valérie Burri and Joseph Dumit

7 **Journalism, Science and Society**
Science Communication between News and Public Relations
Edited by Martin W. Bauer and Massimiano Bucchi

8 **Science Images and Popular Images of Science**
Edited by Bernd Hüppauf and Peter Weingart

9 **Wind Power and Power Politics**
International Perspectives
Edited by Peter A. Strachan, David Lal and David Toke

10 **Global Public Health Vigilance**
Creating a World on Alert
Lorna Weir and Eric Mykhalovskiy

11 **Rethinking Disability**
Bodies, Senses, and Things
Michael Schillmeier

12 **Biometrics**
Bodies, Technologies, Biopolitics
Joseph Pugliese

13 **Wired and Mobilizing**
Social Movements, New Technology, and Electoral Politics
Victoria Carty

14 **The Politics of Bioethics**
Alan Petersen

15 **The Culture of Science**
How the Public Relates to Science Across the Globe
Edited by Martin W. Bauer, Rajesh Shukla and Nick Allum

16 **Internet and Surveillance**
The Challenges of Web 2.0 and Social Media
Edited by Christian Fuchs, Kees Boersma, Anders Albrechtslund and Marisol Sandoval

17 **The Good Life in a Technological Age**
Edited by Philip Brey, Adam Briggle and Edward Spence

18 **The Social Life of Nanotechnology**
Edited by Barbara Herr Harthorn and John W. Mohr

19 **Video Surveillance and Social Control in a Comparative Perspective**
Edited by Fredrika Björklund and Ola Svenonius

20 **The Digital Evolution of an American Identity**
C. Waite

21 **Nuclear Disaster at Fukushima Daiichi**
Social, Political and Environmental Issues
Edited by Richard Hindmarsh

22 **Internet and Emotions**
Edited by Tova Benski and Eran Fisher

23 **Critique, Social Media and the Information Society**
Edited by Christian Fuchs and Marisol Sandoval

24 **Commodified Bodies**
Organ Transplantation and the Organ Trade
Oliver Decker

25 **Information Communication Technology and Social Transformation**
A Social and Historical Perspective
Hugh F. Cline

26 **Visualization in the Age of Computerization**
Edited by Annamaria Carusi, Aud Sissel Hoel, Timothy Webmoor and Steve Woolgar

27 **The Leisure Commons**
A Spatial History of Web 2.0
Payal Arora

28 **Transparency and Surveillance as Sociotechnical Accountability**
A House of Mirrors
Edited by Deborah G. Johnson and Priscilla M. Regan

This page intentionally left blank

Transparency and Surveillance as Sociotechnical Accountability

A House of Mirrors

Edited by Deborah G. Johnson and Priscilla M. Regan

Routledge
Taylor & Francis Group
NEW YORK AND LONDON

First published 2014
by Routledge
711 Third Avenue, New York, NY 10017

and by Routledge
2 Park Square, Milton Park, Abingdon, Oxon OX14 4RN

Routledge is an imprint of the Taylor & Francis Group, an informa business

Library of Congress Cataloging-in-Publication Data

Transparency and surveillance as sociotechnical accountability : a house of mirrors / edited by Deborah G. Johnson and Priscilla M. Regan.
pages cm. — (Routledge studies in science, technology and society ; 28)
1. Electronic data processing—Moral and ethical aspects. 2. Electronic surveillance—Moral and ethical aspects. 3. Government accountability. 4. Corporate governance. 5. Information technology—Moral and ethical aspects. 6. Democracy. I. Johnson, Deborah G., 1945– II. Regan, Priscilla M.
QA76.9.M65T73 2014
004—dc23
2014009886

ISBN: 978-1-138-79073-5 (hbk)
ISBN: 978-1-315-75700-1 (ebk)

Typeset in Sabon
by Apex CoVantage, LLC

Contents

Preface

The earliest thinking behind this volume dates to a paper that we wrote together in 2007 for a workshop on information privacy regulation at the European Consortium for Political Research (ECPR) in Helsinki, Finland. Each of us had written on privacy and information technology for many years, but we had done so from our different disciplinary perspectives—Deborah as a philosopher and STS (science, technology, and society) scholar and Pris as a political scientist and policy analyst. In our paper titled "Privacy Theory: State of the Art and New Frontier," we tried to bring together a sociotechnical systems perspective and our concerns about privacy. The idea that fueled the paper was that privacy policy would be most effective if it took into account all aspects of the sociotechnical systems in which personal data are contained (gathered, stored, processed, and used). Privacy protection cannot be achieved simply through legislation but must take into account multiple and various aspects of the systems in which data flow, including algorithms, personnel policies, user settings, user expectations, and so on.

This paper, and its enthusiastic reception at the workshop, sparked our interest in exploring privacy and surveillance more fully—and doing so explicitly from an STS perspective. At the same time we had the insight that transparency and surveillance have similar structures insofar as they both involve watchers and watched and accounts. The parallel intrigued us since transparency is generally thought of as good and surveillance as bad and since transparency is often seen as a solution to the harms of surveillance. Along with Kent Wayland, at the time a post-doc at UVA, we developed an NSF proposal, "Surveillance and Transparency as Sociotechnical Systems of Accountability," which was funded in the fall of 2008.

We assembled an interdisciplinary team of scholars at the University of Virginia—Siva Vaidhyanathan from the Media Studies Department, Alf Weaver from the Computer Science Department, Kath Weston from the Anthropology Department, and a graduate research assistant, Roberto Armengol, to collaborate with the three of us. Our first meeting was February 26, 2009—and thus began a monthly series of meetings that extended through August 2011. One of our first tasks was selecting the cases to explore in examining

how both surveillance and transparency operated as sociotechnical systems of accountability and how their instrumentation through information technology affected their inner workings and their accounts of individuals. In terms of case selection, we wanted both systems that were generally thought of as surveillance and systems generally thought of as transparency and systems used in different sectors—government, private, and nonprofit. After collective deliberations we agreed on Campaign Finance Disclosure, Secure Flight, American Red Cross, Facebook, and Google.

Once the cases were selected, our conversations centered on readings done in common, on what was currently in the news, on what we were teaching or otherwise researching, on random thoughts, and on paper drafts and, eventually, chapter drafts. Ideas were introduced and debated; through this process, they mutated and evolved into a richer and more extensive understanding of the cases, as well as of the theories and concepts we were using. Although each member of the group brought somewhat different interests and perspectives, through ongoing conversations we developed overlapping views on the cases and the value of thinking about surveillance and transparency together.

Two broad and shared insights were particularly productive. All members of the working group agreed that the metaphor of a house of mirrors usefully captured the ways in which data move and are transformed in the cases we examined. What went into the system was not what came out! Nor was what went in necessarily used in the way originally intended or expected. Instead, what was originally entered bounced around to a number of parties, was highlighted and shaded by these parties, and then was rendered into an account that was so beyond the original data that the account seemed surreal. The second broad and shared insight has to do with a blurring of the boundaries between surveillance and transparency. Transparency often becomes or necessitates surveillance, and surveillance produces transparency of data subjects for a limited audience. However, neither produces anything like simple or direct access to data subjects. Transparency and surveillance both involve selected data and processes that transform simple data in distinctive ways. We used these insights as the common framework for developing the individual and coauthored analyses of the cases.

Early drafts of our thinking and analyses were presented at a number of conferences. In October 2009, Deborah, Pris, Kent, and Roberto presented a panel titled "The Promises and Perils of Transparency" at the meetings of the Society for the Social Study of Science in Washington, DC. Kent presented a paper on the campaign finance disclosure case, and Pris and Kent presented a paper titled "Facebook Funhouse" at the biannual meeting of the Surveillance Studies Network in London in April 2010 (and were stranded there for several extra days because of volcanic ash). Deborah, Pris, and Kent presented a paper on campaign finance disclosure, privacy, and transparency at the Democracy and Elections Symposium at William

and Mary Law School in October 2010. Pris and Deborah presented a paper on reconfiguring the house of mirrors at the International Workshop on Cyber-Surveillance in Everyday Life at the University of Toronto in May 2011. Pris gave a keynote on privacy and trust in sociotechnical systems of accountability at the International Conference of the PATS project at the Technical University in Berlin in April 2011. Deborah presented a paper on accountability in a house of mirrors at the conference "Information Ethics and Policy" at the University of Washington in April 2013.

Several of these presentations were subsequently published as articles or book chapters. All were extensively updated and revised for this book. The following papers represent early work for the project:

Deborah G. Johnson and Kent A. Wayland. 2010. "Surveillance and Transparency as Sociotechnical Systems of Accountability." *Surveillance and Democracy.* Ed. Kevin D. Haggerty and Minas Samatas. London: Routledge. 19–33.

Deborah G. Johnson, Priscilla M. Regan, and Kent Wayland. 2011. "Campaign Disclosure, Privacy and Transparency." *William and Mary Bill of Rights Journal* 19.4: 959–82.

Priscilla M. Regan and Deborah G. Johnson. 2012. "Privacy and Trust in Socio-technical Systems of Accountability." *Managing Privacy through Accountability*. Ed. Daniel Guagnin, Leon Hempel, Carla Ilten, Inga Kroener, Daniel Neyland. and Hector Postigo. London: Palgrave Macmillan.

Kent Wayland, Roberto Armengol, and Deborah G. Johnson. 2012. "When Transparency Isn't Transparent: Campaign Finance Disclosure and Internet Surveillance." *Internet and Surveillance*. Ed. C. Fuchs, K. Boersma, A. Albrechtslund, and M. Sandoval. New York: Routledge. 239–54.

At the conferences and through the publication process, we received invaluable comments and feedback from a number of colleagues, including Colin Bennett, Danielle Citron, Christian Fuchs, Kevin Haggerty, Chris Hoofnagle, David Lyon, David Phillips, and Charles Raab.

Although two members of the working group were unable to contribute chapters to the book, their contributions to the working group were invaluable and their thinking has significantly influenced the volume.

The working group met regularly for two years, and although the papers presented in this volume are the major products of the project, the two years of discussion will no doubt continue to influence the work that each of us does. In the end, we all agreed that the project was one of the most valuable and rewarding of our academic careers.

Finally, although the research done for this book was supported by the National Science Foundation (Award No. 0823363), any opinions, findings,

and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the National Science Foundation.

Deborah G. Johnson
University of Virginia, Charlottesville VA

Priscilla M. Regan
George Mason University, Fairfax VA

January 2014

1 Introduction

Deborah G. Johnson and
Priscilla M. Regan

In this volume, we bring surveillance and transparency practices together under the same lens. Although each type of practice has been studied extensively on its own, the two are rarely (if ever) examined together. Surveillance and transparency are both significant and increasingly pervasive activities in neoliberal societies. Surveillance is increasingly taken up as a means to achieving security and efficiency while transparency is increasingly seen as a mechanism for ensuring compliance or promoting informed consumerism and informed citizenship. Indeed, transparency is often seen as the antidote to the threats and fears of surveillance. We adopt a novel approach and examine surveillance practices and transparency practices together as parallel systems of accountability.

Practices of holding and being held to account are deeply embedded in daily life. Calls for individuals and organizations to account for their behavior (e.g., BP Oil, Bernie Madoff, Anthony Weiner) seem to be linked to strongly felt notions of justice, responsibility, and fairness. This sensibility even seems to underlie the impetus toward democracy when, for example, citizens hold nonelected leaders and regimes accountable for their failure to satisfy their basic needs or rights. More prosaically, in democracy, insofar as elected officials serve at the will of the governed, they are accountable to the electorate, and in this respect accountability is essential to the realization of democracy.

Transparency is a practice that is explicitly targeted to achieve accountability. Citizens in a democracy cannot, for example, hold their representatives accountable—they cannot evaluate, complain, or vote them out—unless they know what they are doing. In theory, at least, transparency pressures leaders and institutions to behave as their constituents expect, that is, to both behave lawfully and be responsive to their concerns. The aphorism of transparency discourse is that "sunlight disinfects." Those who are required to be transparent are less likely to violate their public trust, to deflect or neglect their responsibilities.

Surveillance, on the other hand, is only vaguely recognized as a form of accountability; that is, surveillance seems to be used for many purposes not ordinarily thought of as accountability. More important, surveillance is

often seen as a threat to democracy rather than an essential component. Citizens may believe surveillance is not legally justified or fear the revelation of undesirable, albeit not illegal, information when they are tracked and monitored. Hence, freedom may be retarded and rights quietly diminished. Some believe surveillance may even undermine the development of the kind of personalities needed for democratic citizenship (Rule 1974; Flaherty 1989; Reiman 1995; Lyon 2001).

In the past half century, government and civil institutions have increasingly been constituted with computers and information technology.[1] In particular, these technologies have been used to enable and shape transparency and surveillance practices. Each new technological capacity, from simple data collection to the Internet and websites, search engines, social networking sites, Twitter, and YouTube, has been used to reconfigure practices by which various individuals, groups, and organizations reveal information about themselves as well as practices by which they are observed, tracked, and monitored.

Scholars and social commentators have painted a mixed picture of the significance of adopting these new technological capacities. One strain of literature and hype suggests that computers and information technology have the potential to enhance democratic institutions as never before possible. The availability of information and the connectivity of individuals across the globe promote, facilitate, and inevitably lead to democracy (Barber 1984; Bimber 1998; Brinkerhoff 2009). At the other extreme are analyses suggesting information technology will ultimately lead to totalitarian control (Ellul 1964). From the first days of computer usage, some social theorists were concerned about the potential of computers to facilitate centralization of power and autocratic control (Westin 1967; Miller 1971; Burnham 1983); yet others suggest that the significance of computers and information technology for democracy is multidirectional, a mixed and complicated picture (Ferkis 1969; Glaser 1971; Winner 1977; Beninger 1986; Gandy 1993).

To some extent, these seemingly contradictory claims about the implications of information technology for democracy can be explained by the wide-ranging and malleable capacities of technology. For example, claims that information technology will lead inevitably to democracy tend to focus on the Internet and many-to-many communication, while claims about the potential of technology for centralization of power tend to focus on the scale of information gathering and the threat to personal privacy. So the relationship (if we can call it that) between computers and information technology *and* democracy is far from clear; the question is, perhaps, too crude to yield insight into that which is obviously a complicated phenomenon.

In this volume, we make no grand hypotheses about the information technology–democracy connection. Instead, we examine a set of case studies to understand how transparency and surveillance work when they are instrumented through information technology. The challenge is to explore the information technology–democracy connection by framing electronic

transparency systems and electronic surveillance systems as parallel systems of accountability. In this framework, democracy moves to the background as we ask simply: *how do electronic transparency systems work?* And, *how do electronic surveillance systems work?* Our presumption is that American democracy is currently constituted in part by electronic transparency and surveillance systems and that in order to understand the information technology–democracy connection, we must first understand how these systems operate.

Although the case studies we examine are American and our discussion of democracy is primarily focused on the United States, our analysis has implications for surveillance and transparency practices situated elsewhere.

THE FRAMEWORK: PARALLEL SYSTEMS OF ACCOUNTABILITY

Why frame electronic transparency and electronic surveillance together? The simple answer is that at their core, both have the same triad of elements. In both, there are watchers, those who are watched, and accounts (of those being watched). Who produces the accounts is different in each case, but in both, accounts are produced and the accounts are used by watchers to hold the watched accountable. The promise is that examining surveillance and transparency together as parallel systems and developing an analysis built on the simple structure of watchers, watched, and accounts will yield a new and deeper understanding of each.

To be sure, the rationales for systems of transparency and systems of surveillance are generally quite different, as are the institutional arrangements that make up each type of system. We generally think of surveillance as being done *by* institutions and *about* individuals for purposes that target the individuals or groups for some sort of action, be it to determine whether the individual is engaging in illegal activity, to provide an individual with a purchasing opportunity, or to stop the individual from boarding an airplane. By contrast, we generally think of transparency as a practice involving individuals or institutions that provide information about themselves in the name of reassuring various constituents by documenting their compliance with legal requirements or shaping opinions by emphasizing certain interpretations of information. In surveillance practices, those who are being watched seem to be passive, while in transparency those who are being watched are active; they control and produce the accounts of themselves.

In both, accounts are focused on a particular domain of activity of interest to the watchers and the lens of watching involves norms for that domain: that is, watchers want to know whether or not those whom they watch fit certain categories (exhibit certain patterns of behavior) or adhere to particular norms. For example, when public officials reveal their financial records, they do so in relation to a norm (a law) that prohibits public officials from engaging in certain kinds of financial arrangements. When

advertisers classify their potential customers into various categories on the basis of their browsing behavior, the categories work as descriptive norms; potential customers are treated according to which category they fit. The norm here is an expectation or prediction that the subject in that category will respond in a particular way to a particular kind of advertisement.

Whatever the domain of activity and whatever the norms, watchers use accounts to make decisions about the watched. Information revealed in the name of transparency may be used by citizens to decide whether or not to vote for a public official in the next election. Security officials use information in an individual's files in deciding whether or not to stop the individual at an airport check-in point. Of course, the decision made depends on what is learned about the watched. Often the decisions made by watchers engaged in surveillance or after reading accounts produced in the name of transparency seem to involve no decision at all, but these are effectively decisions. For example, in the case of a traveler whose name does not match any on the terrorist watch list and whose file does not generate any other flag of concern, the decision is made, in effect, to let the person board the plane. Similarly, the elected official who makes her income tax filing available to the press may be reelected without much fanfare if her constituents find nothing unusual in the filings.

In treating surveillance and transparency as parallel systems, this volume works against the grain of current trends. Surveillance scholarship is increasingly seen as a field of its own, and this body of work has evolved from the social control and the privacy literatures. Surveillance studies might be said to take as their subject matter the practices of those who do the watching, while privacy studies focus on the situation of those who are being watched and especially the effects of the watching on the watched. Surveillance studies focus on institutionalized practices in which data about individuals are gathered, sorted, and used, with or without the subjects' knowledge or consent. Surveillance studies are increasingly seen as a better way to get a handle on privacy issues because attention is focused on institutional practices—social sorting, norms, decision making—rather than on individuals, the threat to their interests, and the elusive notion of an individual "right" to privacy (Lyon 2001; Bennett 2011; Regan 2011; Gilliom 2011).

By contrast, transparency—as a scholarly topic—has been of interest primarily to political scientists and public administration scholars who are concerned with government accountability. Transparency systems are generally understood to be systems in which government agencies, corporations, and (less frequently) individuals reveal information about themselves in the name of accountability to others, such as constituents, stockholders, or the public. Data *about* the subject are intentionally provided *by* the subject. In the context of government, transparency is seen as an essential component of democratic government; in corporate contexts, transparency practices are seen as essential to functioning markets (i.e., consumers need information to make enlightened choices) and to civil society, since corporate activities can create risks to civil society.

Not only have surveillance studies and transparency studies been separate from one another, as mentioned earlier, but transparency is often seen as the solution to surveillance. The literature on surveillance is rife with suggestions about countering the negative effects of surveillance by requiring those who gather information to make their activities transparent to those being surveilled (Lyon 2007: 181–83). Danna and Gandy, for example, have argued that data-mining companies should simply inform the public of their activities so that the "bright light of publicity" might regulate their activities (Danna and Gandy 2002: 384). Others have argued that transparency might be a remedy for addressing the injustice of government data-mining efforts (Rubinstein, Lee, and Schwartz 2008). Weitzner questions the utility of simple "notice and consent" transparency policies for Google, favoring instead a more inclusive transparency system in which Google discloses its surveillance tactics to groups of outside experts for evaluation (Weitzner 2007). Indeed, "transparency" is one of the key concepts in the statement of Fair Information Principles put forth by the Organization for Economic Cooperation and Development (OECD).

Whatever the reasons for keeping surveillance studies and the transparency literature separate, they are brought together by the recognition that in both kinds of systems, there are watchers, those who are watched, and accounts used to make decisions about the watched. Moreover, both are generally thought to—even intended to—shape the behavior of the watched. That is, the rationales for both surveillance and transparency systems generally involve some sort of presumption about how the watching will affect the watched. For example, in many systems involving financial transparency such as campaign finance disclosure, the presumption is officials will be less corrupt because they have to reveal what they are doing. Similarly in the classic panoptic prison, the presumption is that prisoners will adjust their behavior to fit the expectations of the guards in the guard tower. Interestingly, some contemporary surveillance seems to go counter to this presumption; those who track the behavior of online consumers, for example, want them simply to behave unfettered by any awareness that they are being watched so that the watchers can better decipher what consumers want. For example, Google wants its customers to reveal their preferences so that they can identify how to provide better search results. Just how watching affects or should affect the behavior of the watched is a complicated matter.

ACCOUNTABILITY

In addition to involving watchers, watched, and accounts, surveillance and transparency can be brought together under the same lens by recognizing they are both *systems of accountability*. Transparency is, of course, commonly viewed as a form or mechanism of accountability; surveillance is not. In transparency, watchers and watched are aware that accounts are produced, and there is the expectation that there will be consequences

depending on what the account reveals. Modern surveillance systems are not as explicitly or intentionally presented as systems of accountability; that is, surveillance systems are more often than not presented as if they are designed to achieve some other public value. Airline passengers are monitored in the name of security; Google searches are tracked in the name of providing better search results; blood donors are scrutinized to ensure the safety of blood transfusions.

Minimally, surveillance is accountability in the sense that it involves the production of "accounts" of individuals or groups, but, more important, it involves "accounts" being used to make decisions about those who are observed and involves consequences of various kinds being meted out on the basis of the accounts. In being held accountable for their behavior, the subjects of surveillance are being judged and treated accordingly. Of course, it is not just punishment that is meted out in surveillance systems; the watched may be rewarded with special opportunities, such as a lower interest rate on a loan or a special offer (because the individual has "achieved" a very high credit score), or decisions may be made to do nothing to a subject of surveillance.

Framing surveillance as accountability has the promise of new insights into surveillance. More often than not, one's behavior is observed and judged and consequences are meted out *without one's knowledge* that a "trial" was being held, without one's knowledge of the norms by which one is being evaluated, and without recourse, except of course if one experiences the consequence and takes the trouble to ferret out who has done the judging, what criteria were used in the judging, and what, if any, system of recourse there is. The obvious examples here are being turned down for a loan or being prevented from boarding an airplane.

Recognizing that surveillance involves accountability helps us to understand why individuals so often react negatively to surveillance. One is being held to account and judged in "trials" that are effectively secret. Judgments are made in places and through processes that are inaccessible to those on trial and protected from public scrutiny. Arguing for a shift in the overarching metaphor used by privacy scholars, from George Orwell's *Big Brother* to Kafka's *The Trial*, Solove (2001) begins to capture the idea that surveillance involves accountability. However, Solove does not dwell on the "trial" aspects of the metaphor. Instead, he emphasizes that the *Trial* metaphor captures the sense of powerlessness, vulnerability, and dehumanization "created by the assembly of dossiers of personal information where individuals lack any meaningful form of participation in the collection and use of their information." That individuals are being held to account is, of course, the precursor to the feeling of powerlessness, vulnerability, and dehumanization. One might not care so much about the operations of surveillance systems were it not that they render judgment and mete out consequences on the basis of the judgment.

When the operations of institutionalized surveillance are covert, the consequences meted out may be experienced (by the subject) as bizarre. Why

am I being stopped at the airport? What could I possibly have done? Or, why is Google sending me an advertisement for Detroit Tigers paraphernalia? I have never been to Detroit and have no interest in baseball. The surveillance subject merely behaves and has no idea that his or her behavior will trigger judgment and consequences; the subject has no idea that criteria are being used in an evaluation and no idea what criteria are being used.

The language of accountability is apt for surveillance practices because norms of behavior are so central to what goes on. Governments, corporations, and individuals are accountable for behaving (or not behaving) in certain ways. Often, the rationale cited for both kinds of systems is that the watching and the production of an account may change the behavior of the watched. This dynamic is most readily seen in transparency regimes. The expectation is that requiring government officials or corporations to be transparent about their activities will help to ensure that they adhere to expectations, that is, formal or informal norms. For example, asking corporations to produce financial reports increases the likelihood they will adhere to the laws regulating their financial activities. Asking employees to reveal any conflicts of interest will reduce the likelihood that they will act in situations in which they have a conflict of interest. Transposed to surveillance, this effect is precisely what Bentham believed the panoptic prison would produce. Seeing the guard tower or believing the guards were watching, inmates would adjust their behavior to conform to norms they expected the guards to enforce. According to Foucault (1977), they would adjust their behavior as well as their understanding of themselves. Of course, as a number of scholars have noted, much of modern surveillance is done without the awareness of the watched, so the effect on behavior is far from clear.

INFORMATION TECHNOLOGY

Transparency and surveillance systems are parallel not just insofar as they involve watchers, watched, and accounts, and not just insofar as they are both systems of accountability. They are also alike insofar as they are increasingly instrumented with information technology. Watchers, watched, and accounts are digitally constituted. In recognizing this commonality, it is tempting to ask what the role of information technology is in modern surveillance and transparency practices. How has information technology reconfigured surveillance and transparency?

Accountability has traditionally not been viewed as a technological endeavor, and one of the important ideas of this project is to recognize that accountability is sociotechnical, that is, that accountability practices are sociotechnical endeavors. However, this means not just that information technology is an important part of surveillance and transparency but that other technologies constitute and have in the past constituted accountability practices. Think here of CCTV, swipe cards, workplace monitoring, and

wiretaps. Shifts in technology have implications for accountability practices, and each shift is different.

Thus, again, it seems tempting to ask how information technology has reconfigured surveillance and transparency. This is a good question but one that we have resisted trying to answer; we have resisted for several reasons. First, the question seems to call for generalizations that might get in the way of "letting the cases speak." Indeed, the question seems to call for a temporal, historical, comparative perspective: how are surveillance and transparency different today (with information technology) than in the past (before information technology), and why? That was not the perspective we took in analyzing the case studies. Rather, we sought to understand how surveillance and transparency practices operate. As will be explained later, we did find a commonality in the loose sense that we were able to fit each case to the metaphor of a house of mirrors.

Another reason for resisting questions that call for the historical, comparative perspective is that information technology is no longer new, no longer an exogenous element of life in modern industrial societies. It may be better treated as an ordinary component of contemporary practices. Thus, we treat information technology as a seamless part of the practices we examined, trying to understand what is produced and less interested in which component of the system contributed what—except where a contribution is striking or obvious. For example, the wide available of information on donations to political campaigns would not be possible were it not for the Internet. Similarly, were it not for the enormous storage and processing capacities of computer technology, Google would not be able to keep track of every one of a user's searches.

Rather than theorizing about the role of information technology across cases, we have treated each case as a sociotechnical system. This means we recognize both that technology is an important component of each system and also that the systems are produced through the intricate interactions and combinations among elements, so much so that it is impossible to disentangle what is due to the technology and what is due to a human decision, a market force, or a legal constraint. Yes, Google could not do what it does without information technology and the Internet, but what Google does results from the working together of technology, Google's economic model, its understanding of itself, legal constraints, market forces, and much, much more.

So, in the case studies and the themed chapters that follow, we treat information technology as a seamless part of the systems we examine. We do not address whether a result or aspect of a practice results from the technology or the social arrangements except when this is strikingly clear or essential to the analysis. Understanding just what goes on in electronic or digital surveillance and transparency is the challenge of this book. And the ultimate question is whether or how these systems can be better constituted to protect and achieve democratic values.