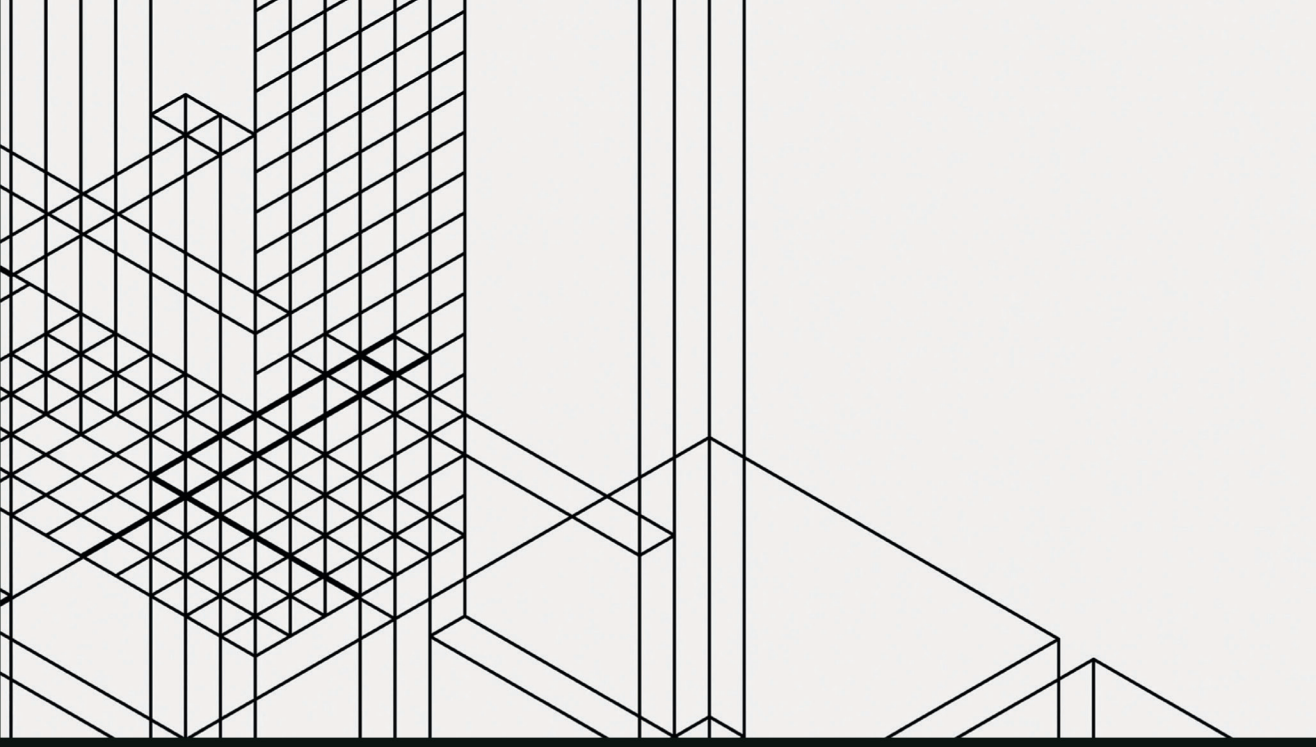
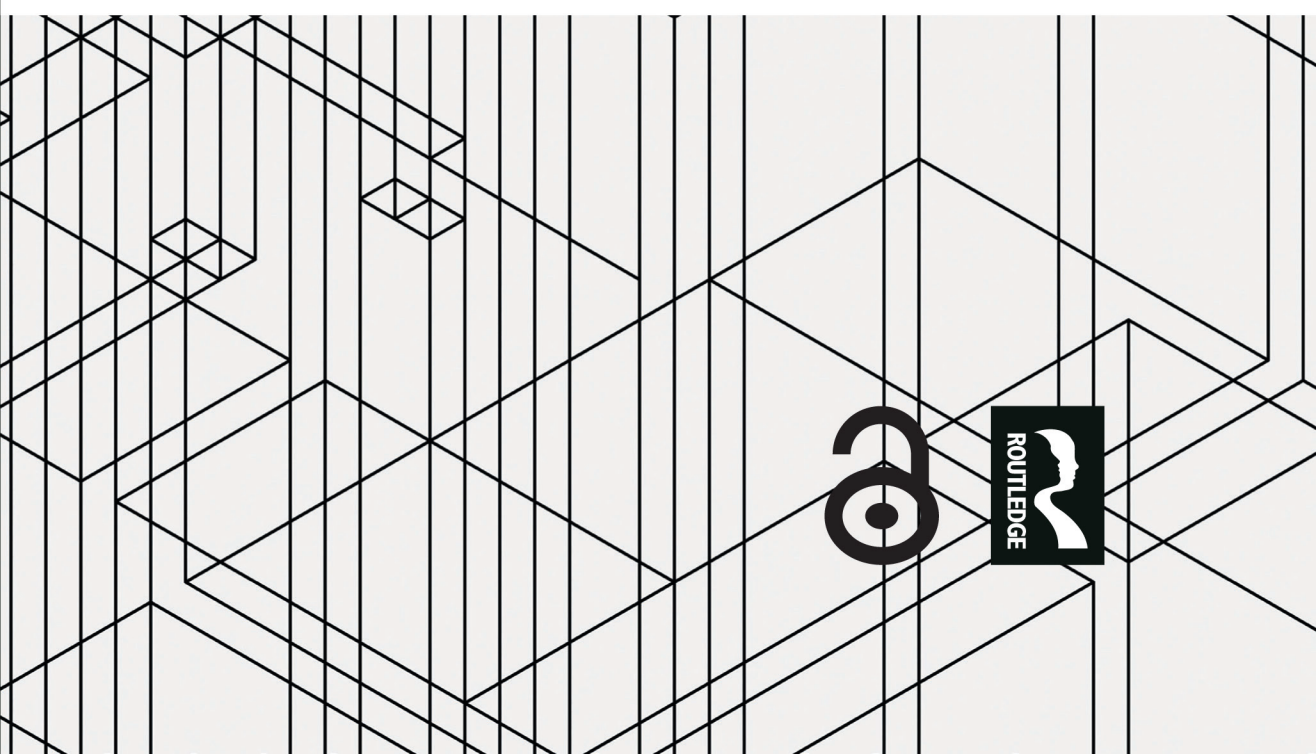


Routledge Studies in Surveillance

TRUST AND TRANSPARENCY IN AN AGE OF SURVEILLANCE

Edited by
Lora Anne Viola and Paweł Laidler



Trust and Transparency in an Age of Surveillance

Investigating the theoretical and empirical relationships between transparency and trust in the context of surveillance, this volume argues that neither transparency nor trust provides a simple and self-evident path for mitigating the negative political and social consequences of state surveillance practices.

Dominant in both the scholarly literature and public debate is the conviction that transparency can promote better-informed decisions, provide greater oversight, and restore trust damaged by the secrecy of surveillance. The contributions to this volume challenge this conventional wisdom by considering how relations of trust and policies of transparency are modulated by underlying power asymmetries, sociohistorical legacies, economic structures, and institutional constraints. They study trust and transparency as embedded in specific sociopolitical contexts to show how, under certain conditions, transparency can become a tool of social control that erodes trust, while mistrust—rather than trust—can sometimes offer the most promising approach to safeguarding rights and freedom in an age of surveillance.

The first book addressing the interrelationship of trust, transparency, and surveillance practices, this volume will be of interest to scholars and students of surveillance studies as well as appeal to an interdisciplinary audience given the contributions from political science, sociology, philosophy, law, and civil society.

Lora Anne Viola, Ph.D., is Professor of Political Science and Chair of the Politics Department at the John F. Kennedy Institute for North American Studies, Freie Universität Berlin.

Paweł Laidler, Ph.D., is Professor of Political Science at the Institute of American Studies and Polish Diaspora at the Jagiellonian University in Kraków.

Routledge Studies in Surveillance

Kirstie Ball, William Webster, Charles Raab, Pete Fussey

Kirstie Ball is Professor in Management at St Andrews University, UK

William Webster is Professor of Public Policy and Management at the University of Stirling, UK

Charles Raab is Professorial Fellow in Politics and International Relations at the University of Edinburgh, UK

Pete Fussey is a Professor in the Department of Sociology at the University of Essex, UK

Surveillance is one of the fundamental sociotechnical processes underpinning the administration, governance and management of the modern world. It shapes how the world is experienced and enacted. The much-hyped growth in computing power and data analytics in public and private life, successive scandals concerning privacy breaches, national security and human rights have vastly increased its popularity as a research topic. The centrality of personal data collection to notions of equality, political participation and the emergence of surveillant authoritarian and post-authoritarian capitalisms, among other things, ensure that its popularity will endure within the scholarly community.

A collection of books focusing on surveillance studies, this series aims to help to overcome some of the disciplinary boundaries that surveillance scholars face by providing an informative and diverse range of books, with a variety of outputs that represent the breadth of discussions currently taking place. The series editors are directors of the Centre for Research into Information, Surveillance and Privacy (CRISP). CRISP is an interdisciplinary research centre whose work focuses on the political, legal, economic and social dimensions of the surveillance society.

Police on Camera
Surveillance, Privacy, and Accountability
Edited by Bryce Clayton Newell

Trust and Transparency in an Age of Surveillance
Edited by Lora Anne Viola and Paweł Laidler

Surveillance Practices and Mental Health
The Impact of CCTV Inside Mental Health Wards
Suki Desai

For more information about this series, please visit: www.routledge.com/Routledge-Studies-in-Surveillance/book-series/RSSURV

CRISP
CENTRE FOR RESEARCH INTO INFORMATION, SURVEILLANCE & PRIVACY

Trust and Transparency in an Age of Surveillance

Edited by Lora Anne Viola and Paweł Laidler

Routledge
Taylor & Francis Group
LONDON AND NEW YORK

First published 2022
by Routledge
2 Park Square, Milton Park, Abingdon, Oxon OX14 4RN

and by Routledge
605 Third Avenue, New York, NY 10158

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

British Library Cataloguing-in-Publication Data
A catalogue record for this book is available from the British Library

Library of Congress Cataloging-in-Publication Data
A catalog record has been requested for this book

ISBN: 978-0-367-63816-0 (hbk)
ISBN: 978-0-367-63817-7 (pbk)
ISBN: 978-1-003-12082-7 (ebk)

DOI: 10.4324/9781003120827

Typeset in Times New Roman
by Newgen Publishing UK

Contents

List of contributors viii
Acknowledgments x

Introduction 1

1 On the relationship between trust, transparency, and surveillance 3
LORA ANNE VIOLA AND PAWEŁ LAIDLER

PART I
Rethinking transparency's relationship to power and domination 19

2 The limits of transparency as a tool for regulating surveillance: a comparative study of the United States, United Kingdom, and Germany 21
LORA ANNE VIOLA

3 A neo-republican critique of transparency: the chilling effects of publicizing power 47
MATTHEW HALL

4 The dynamics of imposed transparency and its role in deep social conflicts 65
SHAUL A. DUKE

5 Classifying and dividing labor: the political economy of racializing surveillance 85
MARKUS KIENSCHERF

PART II
Transparency and trust as institutional constraints and critical praxis 105

6 Secrecy versus transparency in the US national security surveillance state 107
PAWEŁ LAIDLER

7 Secret surveillance in Poland after Snowden: between secrecy and transparency 127
MATEUSZ KOLASZYŃSKI

8 Legal safeguards and oversight innovations for bulk surveillance: an international comparative analysis 145
THORSTEN WETZLING AND KILIAN VIETH

9 Transparency and surveillance of end users on social media platforms: a view of structural economic factors 165
ABEL REIBERG

PART III
Sources of trust and virtues of mistrust in an age of surveillance 181

10 Trust and surveillance: an odd couple or a perfect pair? 183
FREDRIKA BJÖRKLUND

11 Trustworthy humans and machines: vulnerable trustors and the need for trustee competence, integrity, and benevolence in digital systems 201
SARA DEGLI-ESPOSTI AND DAVID ARROYO

12 Why a militantly democratic lack of trust in state surveillance can enable better and more democratic security 221
MIGUELÁNGEL VERDE GARRIDO

Outlook 241

13 Surveillance, transparency, and trust: critical challenges from the COVID-19 pandemic 243
DAVID LYON

Index 258

Contributors

David Arroyo, Ph.D., is Tenured Scientist in the "Cryptography and Information Security" research group, Institute of Physical and Information Technologies (ITEFI), Spanish National Research Council (CSIC).

Fredrika Björklund, Ph.D., is Associate Professor in Political Science at Södertörn University, Stockholm. Her research interests include trust and surveillance, particularly in an East European context.

Sara Degli-Esposti, Ph.D., is Research Scientist in the Institute of Philosophy (IFS) of the Spanish National Research Council (CSIC), and Honorary Research Fellow in the Centre for Business in Society at Coventry University (UK).

Shaul A. Duke, Ph.D., is a comparative sociologist who earned his Ph.D. from the Department of Sociology at Ben-Gurion University, Israel.

Matthew Hall, DPhil, is a researcher at the Policy, Ethics and Emerging Technologies (POET) research team at Trilateral Research and was previously Economic and Social Research Council (ESRC) postdoctoral fellow at Royal Holloway University, London.

Markus Kienscherf, Ph.D., is an Assistant Professor of Sociology at the John F. Kennedy Institute for North American Studies, Freie Universität Berlin.

Mateusz Kolaszyński, Ph.D., is a member of the Department of National Security at the Institute of Political Science and International Relations at the Jagiellonian University in Kraków.

Paweł Laidler, Ph.D., is Professor of Political Science at the Institute of American Studies and Polish Diaspora at the Jagiellonian University in Kraków.

David Lyon, Ph.D., is Director of the Surveillance Studies Centre, Queen's Research Chair in Surveillance Studies, and Professor of Sociology at Queen's University, Canada.

Abel Reiberg, Dr.rer.pol., is a postdoctoral researcher at the John F. Kennedy Institute, Freie Universität Berlin.

Miguelángel Verde Garrido, Dr.rer.pol., is a political scientist and philosopher who earned his doctorate in global politics and international relations from the Otto-Suhr-Institut at Freie Universität Berlin, Germany.

Kilian Vieth, M.A., is the Project Manager of "Digital Rights, Surveillance and Democracy" at the Stiftung Neue Verantwortung and the Project Manager for the European Intelligence Oversight Network (EION).

Lora Anne Viola, Ph.D., is Professor of Political Science and Chair of the Politics Department at the John F. Kennedy Institute for North American Studies, Freie Universität Berlin.

Thorsten Wetzling, Ph.D., is the head of research on surveillance and democratic governance at the Stiftung Neue Verantwortung, and he directs the European Intelligence Oversight Network (EION).

Acknowledgments

This volume is a result of research carried out between 2018 and 2020 by an international group of scholars in the project *Trust and Transparency in an Age of Surveillance: American, German, and Polish Perspectives* (TATAS) led by Lora Anne Viola and Paweł Laidler. The TATAS project was made possible through the generous financial support of a joint grant from the German and Polish national research foundations, the *Deutsche Forschungsgemeinschaft* (DFG Project #381384607) and the *Narodowe Centrum Nauki* (NCN Project #2016/23/G/HS5/01864). With this grant we were able to bring together a superb set of scholars and practitioners from the surveillance studies community and beyond for two workshops held at the Freie Universität Berlin in November 2018 and at the Jagiellonian University in Kraków in October 2019. In addition, we were able to continue our fruitful discussions at the 2019 *European Workshops in International Studies* (EWIS/EISA) conference and at the 2019 *European Consortium for Political Research* (ECPR) General Conference. These workshops, conferences, and the informal meetings that took place in between, fostered an intense and productive exchange of ideas and expertise based on the knowledge, passion, and engagement of all the contributors. From the initial idea of the book to its completion, these exchanges were crucial for developing interdisciplinary and critical reflections, in both theoretical and practical terms, on the relationship between transparency and trust in the context of surveillance. It has also been a pleasure to have made so many new connections and friendships along the way.

In addition to the contributors whose work appears in this volume, we would like to thank all participants in our workshops and panels, especially Paweł Frankowski, Dominika Furtak, Katerina Hadjimatheou, Eric Láštic, and Ola Svenonius. We are also grateful to have benefited from the insights of civil society actors whose advocacy and activism are so important, especially Andre Meister from netzpolitik.org and Karolina Iwańska from Panoptykon Foundation. Their substantive input to our discussions helped shape the final outcome of the project. Special thanks are reserved for Kirstie Ball and David Lyon who have been exceptionally supportive and helpful throughout

the project, generously sharing their extensive knowledge and experience in surveillance studies as well as their time and energy with us.

For their research assistance and editorial, organizational, and logistical support, we thank Lena Herbst, Jakub Kibitlewski, Penelope Krumm, Abel Reiberg, and Linus Sehn. We also thank Lakshita Joshi from Routledge for helping us to meet all the formalities necessary for the publication, and for her patience. We are grateful to the reviewers of the book for their insightful remarks, critical comments, and valuable suggestions which allowed us to enhance the quality of the volume. Finally, we would like to thank the John F. Kennedy Institute for North American Studies at Freie Universität Berlin and the Institute of American Studies and Polish Diaspora at the Jagiellonian University in Kraków for all their support in carrying out this project. Last but not least, we thank our families for their forbearance and understanding of our professional passions.

The open access license was funded by the Priority Research Area Society of the Future under the program "Excellence Initiative – Research University" at the Jagiellonian University in Krakow.

Introduction

Chapter 1

On the relationship between trust, transparency, and surveillance

Lora Anne Viola and Paweł Laidler

Introduction

Surveillance has become a defining characteristic of twenty-first-century society. Although surveillance, broadly understood as a set of data collection and information processing practices (Lyon 2015), has ancient roots, new information technologies and the advent of big data have created conditions for the pervasive, penetrating, and highly consequential role of surveillance in the everyday lives of individuals, corporations, and governments, leading to what has been called our "surveillance society" (Marx 1985; Gandy 1989; Lyon 1994, 2001, 2004) or, more recently, a "culture of surveillance" (Lyon 2018). While new technologies and big data have enabled both a quantitative and qualitative shift in surveillance, these changes have been accompanied by a range of social, political, cultural, and economic processes that have made surveillance practices appear useful and even necessary. Surveillance appears not as a singular, top-down oppressive force, but rather as something done both to and by us in our everyday activities. On the one hand, surveillance technologies are officially legitimized by the state as tools for enhancing public safety and security. Especially since 9/11 and the so-called "war on terror," the state has enhanced its surveillance powers to enable law enforcement and intelligence agencies to collect and use data in domestic policing and counter-terrorism cases (Wood, Konvitz, and Ball 2003). From CCTV (see e.g., Norris and Armstrong 1999) to bodycams (see e.g., Lippert and Newell 2016), to bulk data collection (Ferguson 2017), the surveillance state is omnipresent (Greenwald 2014; Harris 2011; Gellman 2020; Keller 2017). On the other hand, individuals regularly and more-or-less voluntarily provide massive amounts of private data to states and corporations through our use of smartphones, social media platforms, and other internet-based services (Harcourt 2015; Lewis 2017). This personal data has now become the raw material in the process of data commodification and behavior modification that drives profits in what Shoshana Zuboff has called "surveillance capitalism" (Zuboff 2019).

DOI: 10.4324/9781003120827-2

Even though surveillance is normalized through its ubiquitous presence, growing awareness of the dangers that pervasive state and corporate surveillance pose to freedom, equality, and other rights has also called forth critique and resistance (Lyon 2007). The surveillance studies literature has documented and theorized the ways in which surveillance can reduce liberty, amplify (asymmetric) power, and be a technique of governmentality used to administer, manage, sort, and distribute (Lyon 2003; Richards 2013; Barocas and Selbst 2016). Using arguments of national security and public safety, governments have been expanding surveillance powers and, with them, the potential for violating rights and freedoms (Monahan 2006, 2010; Theoharis 2011; Glennon 2015; Lester 2015;). Furthermore, recent feminist theory and critical race scholarship have begun to investigate the ways in which surveillance practices and technologies are embedded in and further normalize existing systemic inequalities based on race, gender, sexuality, and class (see, e.g., the contributions in Dubrofsky and Magnet 2015 and those in Koskela 2012; Browne 2015; Van der Meulen and Heynen 2016; Selod 2018). Surveillance thus not only presents a threat to individual freedoms, civil liberties, and privacy rights but can also reinforce, reproduce, and create structural inequalities.

Recent events have further exposed the ways in which surveillance is inextricably linked to processes of social ordering and social control. Three contemporary episodes, in particular, have raised public awareness of the dangers and risks of surveillance: the rise of the national security surveillance state in the aftermath of 9/11, especially the secret practices revealed by Edward Snowden;[1] the rise of big tech companies and social media platforms that sell data without consent or regard to privacy rights, especially brought to public attention through the Facebook–Cambridge Analytica data scandal;[2] and, most recently, the COVID-19 pandemic, which has not only introduced a range of new surveillance practices largely accepted because of the public health crisis but has also accelerated the digitization of society and the concomitant expansion of digital surveillance tools in the workplace, schools, and in homes (see Lyon this volume; French and Monahan 2020). One of the main features of contemporary surveillance revealed through these episodes is its secrecy, which makes it difficult, or almost impossible, for citizens to understand the scope, purposes, and effects of surveillance. Furthermore, the asymmetric power and knowledge relationship between the institutions imposing surveillance and the subjects being surveilled gives rise to relations of domination and limits the instruments of accountability available to citizens. Through occasional high-profile scandals, usually thanks to disclosures made by whistleblowers or the press, societies gain knowledge about programs used to collect, store, and process enormous amounts of personal data (Greenwald 2014; Snowden 2019; Stanger 2019). These disclosures, on the one hand, erode trust in institutions and, on the other hand, fuel calls for reforms and remedies, usually centering on privacy protections and greater transparency.

This book critically assesses one of the most common narratives used to encapsulate current debates regarding surveillance. According to this narrative, greater transparency is one of the most promising remedies for avoiding the negative effects of surveillance on liberty and, at the same time, for restoring the public trust in institutions that is at once necessary for good governance but that has eroded as the details of surveillance practices have become known (e.g., Schneier 2013). It is commonly asserted, for example, that excessive surveillance undermines citizens' trust in governments and businesses and that the loss of trust is socially damaging—something that needs to be avoided (Sullivan 2016). Transparency, meanwhile, has become a mobilizing idea for resisting or overcoming the negative political, social, and economic consequences of surveillance (e.g., Feeney 2017). Harding (2018), for example, argues that the rise of the surveillance society has been enabled by a collapse of democratic oversight and transparency. Dominant in both the scholarly literature and public debate is the conviction that improved transparency can promote better-informed decisions and greater oversight, and that transparency can restore relations of trust damaged by the secrecy of surveillance and the potential abuse that secrecy makes possible (Peters 2013).

The contributions to this volume challenge this conventional narrative by critically investigating the theoretical and empirical relationships between surveillance, trust, and transparency. While trust, transparency, and surveillance have each been studied extensively on their own, their dynamic interaction has received little sustained attention. Moreover, within the context of surveillance the positive relationship between trust and transparency is often taken to be self-evident. Studying trust and transparency in the context of surveillance is particularly helpful in order to question established (usually positively laden) notions of these concepts and to think critically about the conditions under which trust and transparency have the effects usually ascribed to them. This book starts from the observation that an unreflective belief in the virtues of trust and transparency obscures more complex dynamics and runs the risk of promoting not only simplistic but perhaps also counterproductive proposals for remedying the dangers to liberty that accompany surveillance.

Accordingly, the contributions assembled here seek to shed light on urgent questions, such as: under what conditions is more transparency necessary to prevent the negative consequences of surveillance practices? Is transparency of contemporary surveillance practices possible at all? Under what conditions do what kinds of transparency promote accountability and prevent oppression, and when does transparency lead to further obfuscation and concealment? When does transparency help to equalize power relations and when does it serve to entrench inequalities? When and under what conditions does trust facilitate the negative consequences of surveillance practices, and when does distrust need to be fostered? How can (dis)trust be a means of dealing with power asymmetries and of promoting

democratic oversight? How do trust and transparency limit or enable the expansion of surveillance practices? What are the legal tools that legitimize broad state/corporate surveillance with little oversight? How do trust and transparency affect democracy and the rule of law, and specifically, what opportunities do they present for holding powerful actors—governments and corporations—accountable?

What the studies in this book reveal are complex, ambivalent, and sometimes even contradictory pressures in the triadic relationship between transparency, trust, and surveillance. They do so by considering how each in practice is modulated by underlying power asymmetries, by socio-historical legacies, by economic structures, by cultural distinctiveness, and by institutional constraints. The approaches presented in these chapters suggest that the sources and consequences of trust and transparency can only be understood by taking into account how they are embedded and constructed in various social contexts, such as government institutions, market logics, racialized systems, and technological change.

Rethinking the relationship between trust and transparency

Contemporary responses to invasive surveillance practices are typically dominated by demands for greater protection of privacy rights (see, e.g., Solove 2011; Angwin 2014; Kuntze 2018) and calls for greater transparency on the part of government institutions and corporations that collect and use mass data. While demands for privacy protections have been critically examined elsewhere (e.g., Allen 2000; Henry 2013; Weinberg 2017), this book builds on critiques of transparency as an "unconditional virtue" in contemporary society (Bianchi 2013, 2). Transparency is often juxtaposed with surveillance and pointed to as a remedy against its dangers, as captured by phrases such as "sunshine is the best disinfectant."[3] Transparency generally refers to disclosure, defined as a process of seeing through or having access to information about the activities undertaken by others, which in turn allows oversight and legitimation (Davis and Cuillier 2014; Cain 2015). Pozen (2020, 326) notes that "commentators routinely assert or assume that transparency is indispensable to government accountability, democratic deliberation, citizen empowerment, public-spirited regulation, and public trust in the policy process." In theory, by revealing information that exposes discrepancies between rules and practice, transparency allows authority to be held accountable because exposed discrepancies can be punished (e.g., through judicial institutions), in turn providing incentives for cooperative behavior. But the emerging field of critical transparency studies (Koivisto 2019) argues that transparency is not a coherent normative ideal, nor is it a clear legal policy or governance practice (Pozen and Schudson 2018). Instead, the dynamics of transparency can only be understood in the context of specific constellations of power, interests,

and values and thus require a sociological approach (Pozen 2020; Alloa and Thomä 2018; McCarthy and Fluck 2017). In this critical spirit, the chapters in this volume complicate the positive and even "quasi-religious significance" that is often attributed to transparency (Hood 2006, 3).

Transparency is often approached from an epistemological standpoint as a condition that allows truth to reveal itself (Alloa and Thomä 2018, 45). Transparency is thus typically understood as a property of information (McCarthy and Fluck 2017). But this view becomes problematic to the extent that "truth" and "information" never stand alone and are not objectively accessible. As Bianchi argues, transparency can have negative consequences for accountability and cooperation because it is susceptible to the manipulation of information (Bianchi 2013, 10), rendering transparency a political accessory, a convenient "illusion" rather than an accountability mechanism (see also Roberts 2011). Building on this critique, Lora Anne Viola's chapter in this volume shows that by considering transparency as a political practice, rather than merely as the disclosure of information, we can begin to understand how transparency can come to have counter-intuitive effects, such as the legitimation, and even extension, of state surveillance powers. Similarly, Paweł Laidler in this volume discusses the political and legal relationship between secrecy and transparency in the history of US government surveillance, showing how the rhetoric of "national security" enables a cat-and-mouse game between demands for secrecy vs. transparency, making a stable regime of true transparency impossible and leading, instead, to transparency "traps" that appear to offer (partial) disclosure but no true accountability. Mateusz Kolaszyński's chapter, meanwhile, shows how existing political, legal, and institutional contexts in Poland have completely stymied transparency and oversight mechanisms, rendering them too weak to guard against the use of surveillance to curtail rights.

In light of these critiques, we should be cautious about claims that transparency can rebalance power relations and exert a positive influence on cooperation and compliance. New research shows that transparency that successfully exposes the extent to which actors do not comply with rules and expectations can be corrosive of social and political order and even legitimate further noncompliance (e.g., Carnegie and Carson 2018; Curtin and Meijer 2006, 11). As O'Neill notes, transparency can foster a "culture of suspicion" (O'Neill 2002, 77), thus creating societies of control. Research shows, for example, that although many post-Communist societies, such as Poland, used exposure of former informants and surveillance collaborators as a way of enhancing public trust in new democratic institutions, such exposure, in fact, reduced public trust (Choi and David 2012). Transparency, in other words, can have chilling effects for the same reasons that surveillance does. Matthew Hall's chapter in this volume draws on political philosophy to argue that transparency makes individuals more acutely aware of the power held over them but does not help to free them from domination.

Indeed, critical race and feminist theories have shown how transparency can become a technique of domination. Fischer (2019), for example, has shown how visibility can reinforce notions of "deviance" and thus justify state violence against trans people. Rachel Hall (2015), studying transparency practices on the traveler, theorizes the "aesthetics of transparency" as submission to surveillance. Critical race studies have shown how surveillance and transparency practices have been informed by colonialism and racial oppression that depended on policing black life under slavery (e.g., Browne 2015; Rosenthal 2018). In a similar vein, Markus Kienscherf in this volume discusses how contemporary surveillance practices in the United States have their origins in settler colonialism and its system of racialized expropriation. The idea that greater transparency can have outright oppressive effects is underscored in Shaul Duke's chapter on Israeli–Palestinian relations, which shows how imposed transparency can become a tool of social control and a weapon in societal conflicts. With a different focus, Abel Reiberg also explores the relationship between transparency and surveillant control by looking at how market incentives drive social media platforms to push users toward ever greater transparency and self-exposure.

These critiques of transparency do not amount to a wholesale rejection of the idea that transparency can bring benefits to democratic governance, but they do present a strong argument for thinking about transparency more specifically in its particular socio-cultural and political contexts. In this spirit, Thorsten Wetzling and Kilian Vieth's contribution to this volume assesses a wide range of good practice recommendations to provide a more nuanced picture of how and under what conditions specific legal safeguards and transparency mechanisms can produce more effective—rather than illusional—oversight.

One of the central justifications for demanding transparency from governments and corporations is its perceived importance for restoring trust lost through secret, nonconsensual, or invasive surveillance practices. Trust, like transparency, mostly takes on a positive normative valence in current literature (Etzioni 2010, 389; Hardin 2002a). Trust plays a pervasive role in modern social relations and is considered crucial for sustaining social cooperation and democratic governance (Cook 2001; Hardin 2002a; Cook, Hardin, and Levi 2005; Seligman 1997). Trust is seen as facilitating relations between nation states (Kydd 2000), between elected representatives and citizens (Hollyer, Rosendorff, and Vreeland 2019), between government agencies and citizens (Fung 2013), and between individuals. Surveillance practices, in turn, are seen as detrimental to public trust and corrosive of social relations that depend on trust.

Trust can broadly be defined as the belief of one actor that another actor will reciprocate cooperation rather than exploit that cooperation. The "trust giver" cooperates with the "trust receiver" in the belief that he or she will not be taken advantage of and is therefore vulnerable to and dependent on

the reaction of the trust receiver. Trust relations can be further distinguished based on the actor level (e.g., interpersonal or institutional trust) and on the relational distance (e.g., particularized trust or generalized trust). A central feature of any trust relation is that it entails risk, a measurable degree of uncertainty about whether or not the other side will cooperate (Hardin 2002a; Kydd 2000). Beyond these basic points, however, the literature on trust is divided into understandings of trust as a rational, strategic calculus and understandings of trust as a normative, moralistic relationship based on socialization rather than strategic interaction (Nannestad 2008). The rationalist view draws on insights from game theory and Bayesian analysis and sees trust, in Hardin's (2002a) terms, as "encapsulated self-interest" or the result of the rational processing of information about which actors have reasons to act in our best interest (see also Hardin 2002a; Kydd 2000, 2007). But as others have pointed out (Rathbun 2012, 3–7), this conception reduces trust to compliance based on cost assessments. A normative view, in contrast, sees trust as based on the socialized belief that potential trustees will "do what is right" (Uslaner 2002).

The chapters in this volume that focus on trust pick up this debate and examine why a normative or sociological understanding of trust is important in our surveillance society. Fredrika Björklund, for example, argues that a rational explanation of trust fails to explain the contradiction between empirical findings that show a positive correlation between public trust in institutions and acceptance of surveillance practices, and those that show how surveillance leads to a deterioration of public trust. Sara Degli-Esposti and David Arroyo similarly argue that in order for technical systems to earn our trust, digital authentication processes need to go beyond a rational information logic to include an ethic of care built on the integrity and benevolence of the operators of such systems. These contributions go beyond game theory to think about the social contexts that promote or erode trust.

Although the conventional wisdom treats transparency as the currency of trust, there are good theoretical and empirical reasons to see trust and transparency as being in tension with one another. The logic of trust works through social beliefs that the other will cooperate and reciprocate in the absence of monitoring and punishment mechanisms, while transparency works through monitoring and punishment. Transparency aims to eliminate risk and uncertainty and to increase control, while trust is based on accepting a degree of vulnerability. In this sense, trust and transparency can serve as substitutes for one another, rather than as mutually reinforcing complements. Experimental studies on individuals, for example, show that the more trustworthy cooperation partners are perceived to be, the less monitoring is necessary. Conversely, the reliance on monitoring mechanisms, such as among employees, inhibits the creation of trust (Schweitzer, Ho, and Zhang 2018). Shaul Duke's study of pro-Palestinian human rights groups and the Israeli

state in this volume provides an example of how transparency can inhibit trust-building and foster suspicion and hostility.

What makes trust analytically interesting from the perspective of surveillance practices is precisely that it captures willingness to cooperate even in the face of vulnerability to exploitation (Ostrom and Walker 2003). Some scholars have argued that surveillance is conducive to the creation of trust, since it allows actors to ensure that mutually agreed-upon rules of behavior are adhered to (Lombardi and Woods 2008, 723), while others have argued that trust is contrary to surveillance because surveillance is based on a logic of monitoring, whereas trust expects compliance with rules of behavior in the absence of monitoring (Cofta 2007, 20; Neyland 2006, 9). The trust literature has raised a number of important questions in this regard, including whether legal sanctions reinforce or undermine trust, whether too much trust renders the public vulnerable to government corruption or abuse, and whether distrust can be healthy to democratic governance (see, e.g., contributions in Braithwaite and Levi 1998; and in Hardin 2004). Paradoxically, too much trust can enable the very kind of exploitation and abuse that leads to its erosion, and conversely, distrust can enhance the conditions that foster cooperation and trust (Sztompka 1998; Hardin 2002b, 2004). Some studies have shown that trust in government is a crucial permissive condition for allowing the abuse of civil liberties through surveillance because they find evidence that high levels of trust in government make citizens more likely to cede their civil liberty protections and accept government surveillance practices (Davis and Silver 2003, 28–46). Other studies have shown that low political trust leads to greater political activism and involvement (Kaase 1999) or that trust is not necessary for cooperation and democratic governance at all (e.g., Cook, Hardin, and Levi 2005). These insights suggest a complex relationship between trust and distrust that the chapters by Matthew Hall and Miguelángel Verde Garrido in this volume consider in the context of surveillance. In different ways, both these chapters make a case that distrust is crucial for shoring up healthy democratic governance, promoting contestation and deliberation, and avoiding domination in a surveillance society.

The contributions of this volume

This book is intended to expose, illuminate, and go some way toward resolving the contradictions apparent in the triadic relationship between trust, transparency, and surveillance. Building on and integrating insights from existing literature, the chapters in this volume revolve around three overarching insights. First, they share a critique of "naturalistic" approaches to trust and transparency that take these concepts as having a straightforward meaning and emphasize, instead, the ways in which the meaning and implications of trust and transparency are contingent on intersubjective interactions, power relations, and institutional contexts. Second, recognizing

the social construction of these concepts brings into sharper focus their susceptibility to relations of power, and all chapters touch on the ways in which trust and transparency can be tools of power and domination. Third, then, the chapters shed light on the conditions under which trust and transparency, shaped by power relations, technological capabilities, institutions, and socio-historical legacies, facilitate or regulate surveillance practices. Not all of the contributions address the interplay of all three core concepts, but each addresses some combination of them.

The book is divided into three parts. The chapters in Part I focus on transparency and its relation to enabling or restraining surveillance. They stress the ways in which the effects of transparency are contingent on the social and political contexts and relationships in which it is deployed. Lora Anne Viola's chapter begins this discussion by identifying and critiquing the arguments that underpin dominant claims about transparency's beneficial effects for regulating surveillance practices. She then introduces three distorting effects of transparency conditioned by a political process that takes place in the context of asymmetrical power relations and conflicting strategic interests. Through a comparative analysis of legislative reforms meant to curtail surveillance abuses in the United States, United Kingdom, and Germany, she shows how transparency can lead to the legitimation and even extension of surveillance powers, rather than their regulation. In Chapter 3, Matthew Hall similarly considers the chilling effects of transparency as it reveals, rather than regulates, the exercise of power. Considering trust and transparency from the perspective of neo-republican political theory, which emphasizes liberty as nondomination and citizen participation, Hall argues that transparency can expose the power of state surveillance but not reduce its harms. Indeed, transparency makes citizens more aware of the power held over them and thus can contribute to domination. He considers, instead, alternative forms of transparency and uses of distrust to avoid state surveillance's infringements upon liberty and to foster public deliberation about the purposes of surveillance. In Chapters 4 and 5, Shaul Duke and Markus Kienscherf pick up on the relationship between transparency and domination in the cases of Israeli–Palestinian relations and neo-colonialism in the United States, respectively. Duke analyses the relationship between imposed transparency and surveillance in the ongoing conflict between the Israeli state and Palestinians living in the West Bank. Transparency, he argues, can become a strategic tool that undermines trust, escalates conflict, and does not empower the weak. Kienscherf considers surveillance practices as central to the accumulation of capital and the formation of race, especially as these practices have been used in the process of expropriating and exploiting black labor in the United States. He argues that continuing contemporary practices of transparency, such as those that monitor workers or track welfare recipients, are part of a neocolonial logic of capital that reproduces racial divisions even under conditions of formal equality. The policy implication of these contributions

is that transparency cannot be blindly relied upon to reduce the harms of surveillance or to restore trust.

The chapters in Part II consider the interactions of trust and transparency in specific surveillance contexts. In Chapter 6, Paweł Laidler considers the evolution of surveillance laws in the US national security state, pointing in particular to the perpetual tension between claims that security requires secrecy, on the one hand, and claims that transparency rules are required for democratic accountability, on the other. By tracing historical and contemporary US policies across the three branches of government, especially in the wake of Snowden's leaks, he argues that the United States has never been able to reach a stable coexistence between demands for secrecy and demands for transparency, as there is a constant tendency to over-correct in one direction or the other. Picking up on the tension between government demands for secrecy and citizen demands for accountability through transparency, in Chapter 7 Mateusz Kolaszyński traces the legal and institutional legacies in post-Communist Poland that have rendered efforts to restrain the surveillance powers of the state futile. Instead, he shows how institutional changes have strengthened the state's surveillance powers even in the face of counterpressures from internal (e.g., civil society) and external (e.g., EU) actors. Almost as if in reply to Laidler and Kolaszyński's concerns, in Chapter 8 Thorsten Wetzling and Kilian Vieth propose a set of concrete best practices taken from real-world examples that can make transparency work to reduce the risks of harm from state surveillance. Sharing with us their think tank expertise, this chapter brings theoretical arguments into dialogue with current policy debates to yield concrete recommendations. In Chapter 9, Abel Reiberg turns to consider the role of transparency and surveillance in social media platforms. Using the example of Facebook, he teases out the market logic by which corporations pressure users to become increasingly transparent while creating incentives for platforms and their data use to remain inscrutable. Reiberg's case study shows how transparency is used to develop "legitimate" regimes of surveillance in capitalist markets. Together, the chapters in this section shed light on the potentials (and pitfalls) of institutional change for achieving an acceptable balance between transparency and secrecy, and between trust and distrust.

The chapters in Part III turn to focus on the issue of trust and distrust by reflecting on the varied sources and types of trust, including mistrust, and their ability to reduce the harms that can be caused by surveillance. The contributions in this section argue that the causes and effects of trust beliefs are contingent rather than immutable and can only be understood as embedded in specific social and political contexts. Fredrika Björklund in Chapter 10 begins by considering the contradiction between the many empirical studies that show a positive correlation between trust in public institutions and acceptance of invasive surveillance practices and the widespread argument that invasive surveillance practices erode trust in society. She argues that

we can go some way to resolving this contradiction by moving away from a rational understanding of trust as the result of good (or poor) performance to think instead about the shared social values and experiences that shape trust relations. By embedding trust beliefs into specific socio-cultural settings, we can better understand how trust relations change over time and space, and across different communities and issue areas. In this same vein, in Chapter 11 Sara Degli-Esposti and David Arroyo consider what trust might mean when we are increasingly dependent on machines and algorithms while having ever more limited knowledge and power to hold them accountable. In thinking about how notions of trust are affected by changing epistemological and technological standards, they argue that digital technology requires us to have mechanisms to ensure that the humans who design and operate digital systems are trustworthy. Rather than base these mechanisms on rational-instrumental motives, they argue for the importance of generating a professional ethics of care among those who design and run digital systems. In Chapter 12, Miguelángel Verde Garrido considers the value of the public's lack of trust for generating trustworthy democratic institutions. Through case study analysis of abusive surveillance practices in the United States, Poland, and Germany, he argues for a "militant democracy" that can ensure and enhance government trustworthiness through institutions of oversight and accountability and citizen engagement. His argument highlights the role of democratic institutions in providing corrections when breaches of trust occur and describes how, through its dynamic nature, healthy distrust can restore trust and support democratic norms. The volume is rounded out with a concluding chapter by David Lyon, providing an outlook that opens the horizon to the larger issues at stake in the book. In particular, Lyon considers how human agency can be mobilized to bring forth an ethics of care and digital justice that allows the technological innovations underpinning surveillance to be used for, and not against, human flourishing.

This book grows out of two workshops, one held at the Freie Universität in Berlin in 2018 and a second at the Jagiellonian University in Krakow in 2019, as well as several conference sections and panels in 2019, through which we brought together a group of scholars from different disciplines interested in exploring the relationship between trust and transparency in the context of surveillance. Funding for our meetings and research was provided by joint grants from the German National Research Foundation (DFG, *Deutsche Forschungsgemeinschaft*) and the Polish National Science Center (NCN, *Narodowe Centrum Nauki*).[4] The participants in this collaborative endeavor come from diverse fields, including surveillance studies, political science, security studies, constitutional law, sociology, and political philosophy. They bring to this volume disciplinary and interdisciplinary perspectives reflecting their academic backgrounds and also their personal expertise and different national contexts. The contributions also display a variety of research strategies, including comparative case studies, country case studies, legal analysis,

policy analysis, and analytical political theory. The multidisciplinary and international character of the volume are key strengths that allow it to address political, legal, economic, historical, and cultural aspects of the relationship between trust, transparency, and surveillance.

This is not to say, however, that we have been able to address all the facets and aspects that deserve consideration. There is much work still to be done and many avenues for research that we have not been able to pursue here, including further work from the perspectives of gender, race, and intersectionality, research on specific technologies, and work on corporate surveillance and big data, especially as these intersect with state surveillance practices. Furthermore, the COVID-19 pandemic began just as this project reached completion, so we have not been able to address the many associated challenges for surveillance, trust, and transparency that will most certainly emerge. Fortunately, however, in the concluding chapter David Lyon reflects on the challenges of the pandemic in the context of thinking about how we can promote human flourishing and justice in an age of surveillance. Especially because of all the work that still needs to be done, and that could not be undertaken here, our hope is that this volume brings attention to the importance of thinking about the compatibilities and contradictions that arise in the interactions among trust, transparency, and surveillance, and that it sheds some light on the contingencies and complexities of these relationships.

Notes

1 In 2013, the whistleblower copied about two million classified documents, relating mostly to the operations conducted by the NSA, which revealed several secretive surveillance programs and activities, as well as the scope of data collection by the US government.
2 The scandal, first reported in 2015, involved the company Cambridge Analytica harvesting personal data from millions of Facebook users without consent and then using this data to create targeted political advertising that it sold to political campaigns. The scandal was an example of privacy breaches, the commodification of data, and the use of such data to influence democratic processes (Chen 2018).
3 This phrase, quoted often in the context of surveillance, was famously used by US Supreme Court Justice Louis Brandeis in a 1913 *Harper's Weekly* article entitled "What Publicity Can Do."
4 The project was titled *Trust and Transparency in an Age of Surveillance: American, German, and Polish Perspectives* (TATAS) led by Lora Anne Viola and Paweł Laidler, and was funded by grant numbers: DFG Project #381384607 and NCN Project #2016/23/G/HS5/01864.

References

Allen, Anita. 2000. "Privacy-as-Data Control: Conceptual, Practical, and Moral Limits of the Paradigm." *Connecticut Law Review* 32: 861–75.

Alloa, Emmanuel, and Dieter Thomä, eds. 2018. *Transparency, Society and Subjectivity: Critical Perspectives*. London: Palgrave Macmillan.

Angwin, Julia. 2014. *Dragnet Nation: A Quest for Privacy, Security, and Freedom in a World of Relentless Surveillance*. New York: Times Books.

Barocas, Solon, and Andrew D. Selbst. 2016. "Big Data's Disparate Impact." *California Law Review* 104(3): 671–732.

Bianchi, Andrea. 2013. "On Power and Illusion: The Concept of Transparency in International Law." In *Transparency in International Law*, edited by Andrea Bianchi and Anne Peters, 1–20. Cambridge: Cambridge University Press.

Braithwaite, Valerie, and Margaret Levi. 1998. *Trust and Governance*. New York: Russell Sage Foundation.

Browne, Simone. 2015. *Dark Matters: On the Surveillance of Blackness*. Durham: Duke University Press.

Cain, Bruce. 2015. "The Transparency Paradox." *The American Interest* 11(2), www.the-american-interest.com/2015/10/10/the-transparency-paradox/.

Carnegie, Allison, and Austin Carson. 2018. "The Spotlight's Harsh Glare: Rethinking Publicity and International Order." *International Organization* 72(3): 627–57.

Chen, Adrian. 2018. "Cambridge Analytica and Our Lives Inside the Surveillance Machine." *The New Yorker.* March 21, 2018, www.newyorker.com/tech/annals-of-technology/cambridge-analytica-and-our-lives-inside-the-surveillance-machine.

Choi, Susanne Y.P., and Roman David. 2012. "Lustration Systems and Trust: Evidence from Survey Experiments in the Czech Republic, Hungary, and Poland." *American Journal of Sociology* 117(4): 1172–201.

Cofta, Piotr. 2007. *Trust, Complexity and Control: Confidence in a Convergent World*. Chichester: Wiley.

Cook, Karen. 2001. *Trust in Society*. New York: Russell Sage Foundation.

Cook, Karen, Russell Hardin, and Margaret Levi. 2005. *Cooperation without Trust?* New York: Russell Sage Foundation.

Curtin, Deirdre, and Albert Meijer. 2006. "Does Transparency Strengthen Legitimacy?" *Information Polity* 11(2): 109–22.

Davis, Charles N., and David Cullier. 2014. *Transparency 2.0: Digital Data and Privacy in a Wired World*. New York: Peter Lang Publishing.

Davis, Darren W., and Brian D. Silver. 2003. "Civil Liberties vs. Security: Public Opinion in the Context of the Terrorist Attacks on America." *American Journal of Political Science* 48(1): 28–46.

Dubrofsky, Rachel E., and Shoshana Magnet, eds. 2015. *Feminist Surveillance Studies*. Durham: Duke University Press.

Etzioni, Amitai. 2010. "Is Transparency the Best Disinfectant?" *Journal of Political Philosophy* 18(4): 389–404.

Feeney, Matthew. 2017. "When It Comes to Surveillance, Watch the Watchmen." *The New York Times*. October 23, 2017, www.nytimes.com/2017/10/23/opinion/police-surveillance.html.

Ferguson, Andrew G. 2017. T*he Rise of Big Data Policing: Surveillance, Race, and the Future of Law Enforcement*. New York: New York University Press.

Fischer, Mia. 2019. *Terrorizing Gender: Transgender Visibility and the Surveillance Practices of the U.S. Security State*. Lincoln: University of Nebraska Press.

French, Martin, and Torin Monahan. 2020. "Dis-ease Surveillance: How Might Surveillance Studies Address COVID-19?" *Surveillance & Society* 18(1): 1–11.

Fung, Archon. 2013. "Infotopia: Unleashing the Democratic Power of Transparency." *Politics & Society* 41(2): 183–212.
Gandy, Oscar H. 1989. "The Surveillance Society: Information Technology and Bureaucratic Social Control." *Journal of Communication* 39(3): 61–76.
Gellman, Barton. 2020. *Dark Mirror: Edward Snowden and the American Surveillance State*. New York: Penguin Press.
Glennon, Michael J. 2015. *National Security and Double Government*. Oxford: Oxford University Press.
Greenwald, Glenn. 2014. *No Place to Hide: Edward Snowden, the NSA, and the U.S. Surveillance State*. New York: Metropolitan Books.
Hall, Rachel. 2015. *The Transparent Traveler: The Performance and Culture of Airport Security*. Durham: Duke University Press.
Harcourt, Bernhard E. 2015. *Exposed: Desire and Disobedience in the Digital Age*. Cambridge: Harvard University Press.
Hardin, Russell. 2002a. *Trust and Trustworthiness*. New York: Russell Sage Foundation.
Hardin, Russell. 2002b. "Liberal Distrust." *European Review* 10(1): 73–89.
Hardin, Russell. 2004. *Distrust*. New York: Russell Sage Foundation.
Harding, James M. 2018. *Performance, Transparency, and the Cultures of Surveillance*. Ann Arbor: Michigan University Press.
Harris, Shane. 2011. *The Watchers: The Rise of America's Surveillance State*. New York: Penguin Books.
Henry, Aaron. 2013. "The Perpetual Object of Regulation: Privacy as Pacification." *Socialist Studies/Etudes Socialistes* 9(2): 94–110.
Hollyer, James R., B. Peter Rosendorff, and James Raymond Vreeland. 2019. "Transparency, Protest and Democratic Stability." *British Journal of Political Science* 49(4): 1251–77.
Hood, Christopher. 2006. "Transparency in Historical Perspective." In *Transparency: The Key to Better Governance?*, edited by Christopher Hood and David Heald, 3–23. Oxford: Oxford University Press.
Kaase, Max. 1999. "Interpersonal Trust, Political Trust and Non-Institutionalized Political Participation in Western Europe." *West European Politics* 22(3): 1–21.
Keller, William. 2017. *Democracy Betrayed: The Rise of the Surveillance Security State*. Berkeley: Counterpoint.
Koivisto, Ida. 2019. "Towards Critical Transparency Studies." *Res Publica* 25(3): 439–43.
Koskela, Hille. 2012. "'You Shouldn't Wear that Body': The Problematic of Surveillance and Gender." In *Routledge Handbook of Surveillance Studies*, edited by Kirstie Ball, Kevin Haggerty and David Lyon, 49–56. Abingdon: Routledge.
Kuntze, Jan-Hendrik. 2018. *The Abolishment of the Right to Privacy? The USA, Surveillance, and the Spiral Model.* Baden: Nomos.
Kydd, Andrew. 2000. "Overcoming Mistrust." *Rationality and Society* 12(4): 397–424.
Kydd, Andrew. 2007. *Trust and Mistrust in International Relations*. Princeton: Princeton University Press.
Lester, Genevieve. 2015. *When Should State Secrets Stay Secret? Accountability, Democratic Governance, and Intelligence.* Cambridge: Cambridge University Press.
Lewis, Randolph. 2017. *Under Surveillance: Being Watched in Modern America*. Austin: University of Texas Press.

Lippert, Randy K., and Bryce Clayton Newell. 2016. "Debate Introduction: The Privacy and Surveillance Implications of Police Body Cameras." *Surveillance & Society* 14(1): 113–6.

Lombardi, Domenico, and Ngaire Woods. 2008. "The Politics of Influence: An Analysis of IMF Surveillance." *Review of International Political Economy* 15(5): 711–39.

Lyon, David. 1994. *The Electronic Eye: The Rise of the Surveillance Society*. Cambridge: Polity Press/Blackwell.

Lyon, David. 2001. *Surveillance Society: Monitoring Everyday Life*. Buckingham: Open University Press.

Lyon, David. 2003. *Surveillance as Social Sorting: Privacy, Risk and Automated Discrimination*. London: Routledge.

Lyon, David. 2004. "Globalizing Surveillance: Comparative and Sociological Perspectives." *International Sociology* 19(2): 135–49.

Lyon, David. 2007. *Surveillance Studies: An Overview*. Cambridge: Polity Press.

Lyon, David. 2015. *Surveillance after Snowden*. Cambridge: Polity Press.

Lyon, David. 2018. *The Culture of Surveillance: Watching as a Way of Life*. Cambridge: Polity Press.

Marx, Gary T. 1985. "The Surveillance Society: The Threat of 1984-Style Techniques." *The Futurist* 6: 21–26.

McCarthy, Daniel R., and Matthew Fluck. 2017. "The Concept of Transparency in International Relations: Towards a Critical Approach." *European Journal of International Relations* 23(2): 416–40.

Monahan, Torin. 2006. *Surveillance and Security: Technological Politics and Power in Everyday Life*. London: Routledge.

Monahan, Torin. 2010. *Surveillance in the Time of Insecurity*. New Brunswick: Rutgers University Press.

Nannestad, Peter. 2008. "What Have We Learned About Generalized Trust, If Anything?" *Annual Review of Political Science* 11: 413–36.

Neyland, Daniel. 2006. *Privacy, Surveillance and Public Trust*. New York: Palgrave Macmillan.

Norris, Clive, and Gary Armstrong. 1999. *The Maximum Surveillance Society: The Rise of CCTV*. London: Routledge.

O'Neill, Onora. 2002. *A Question of Trust: The BBC Reith Lectures 2002*. Cambridge: Cambridge University Press.

Ostrom, Elinor, and James Walker. 2003. "Introduction." In *Trust and Reciprocity: Interdisciplinary Lessons from Experimental Research*, edited by Elinor Ostrom and James Anthony Walker, 3–18. New York: Russell Sage Foundation.

Peters, Anne. 2013. "Towards Transparency as a Global Norm." In *Transparency in International Law*, edited by Andrea Bianchi and Anne Peters, 534–607. Cambridge: Cambridge University Press.

Pozen, David E. 2020. "Seeing Transparency More Clearly." *Public Administration Review* 80(2): 326–31.

Pozen, David, and Michael Schudson. 2018. "Introduction." In *Troubling Transparency: The History and Future of Freedom of Information*, edited by David Pozen and Michael Schudson, 1–10. New York: Columbia University Press.

Rathbun, Brian. 2012. *Trust in International Cooperation: International Security Institutions, Domestic Politics and American Multilateralism*. Cambridge: Cambridge University Press.

Richards, Neil M. 2013. "The Dangers of Surveillance." *Harvard Law Review* 126(7): 1934–65.

Roberts, Alasdair. 2011. "Wikileaks: The Illusion of Transparency." *International Review of Administrative Science* 78(2): 116–33.

Rosenthal, Caitlin. 2018. *Accounting for Slavery: Masters and Management*. Cambridge: Harvard University Press.

Schneier, Bruce. 2013. "The Only Way to Restore Trust in the NSA." *The Atlantic*. September 4, 2013, www.theatlantic.com/politics/archive/2013/09/the-only-way-to-restore-trust-in-the-nsa/279314/.

Schweitzer, Maurice E., Teck-Hua Ho, and Xing Zhang. 2018. "How Monitoring Influences Trust: A Tale of Two Faces." *Management Science* 64(1): 253–70.

Seligman, Adam. 1997. *The Problem of Trust*. Princeton: Princeton University Press.

Selod, Saher. 2018. *Forever Suspect: Racialized Surveillance of Muslim Americans in the War on Terror*. New Brunswick: Rutgers University Press.

Snowden, Edward. 2019. *Permanent Record*. New York: Henry Holt.

Solove, Daniel. 2011. *Nothing to Hide: The False Tradeoff Between Privacy and Security.* New Haven: Yale University Press.

Stanger, Allison. 2019. *Whistleblowers: Honesty in America from Washington to Trump*. New Haven: Yale University Press.

Sullivan, Margaret. 2016. "Yahoo Helps the Government Read Your Emails. Just Following Orders, They Say." *The Washington Post*. October 6, 2016, www.washingtonpost.com/lifestyle/style/yahoo-helps-the-government-read-your-emails-just-following-orders-they-say/2016/10/05/05648894-8b01-11e6-875e-2c1bfe943b66_story.html.

Sztompka, Piotr. 1998. "Trust, Distrust and Two Paradoxes of Democracy." *European Journal of Social Theory* 1(1): 19–32.

Theoharis, Athan G. 2011. *Abuse of Power: How Cold War Surveillance and Secrecy Policy Shaped the Response to 9/11.* Philadelphia: Temple University Press.

Uslaner, Eric M. 2002. *The Moral Foundations of Trust*. Cambridge: Cambridge University Press.

Van der Meulen, Emily, and Robert Heynen. 2016. *Expanding the Gaze: Gender and the Politics of Surveillance*. Toronto: University of Toronto Press.

Weinberg, Lindsay. 2017. "Rethinking Privacy: A Feminist Approach to Privacy Rights after Snowden." *Westminster Papers in Communication and Culture* 12(3): 5–20.

Wood, David, Eli Konvitz, and Kirstie Ball. 2003. "The Constant State of Emergency? Surveillance after 9/11." In *The Intensification of Surveillance: Crime, Terror and Warfare in the Information Era*, edited by Kirstie Ball and Frank Webster, 137–50. London: Pluto Press.

Zuboff, Shoshana. 2019. *The Age of Surveillance Capitalism*. London: Profile Books.

Part I

Rethinking transparency's relationship to power and domination

Chapter 2

The limits of transparency as a tool for regulating surveillance

A comparative study of the United States, United Kingdom, and Germany

Lora Anne Viola

Introduction

In an interview with *The Guardian*, Edward Snowden explained that his disclosure of the massive scale of government surveillance was motivated by the conviction that greater transparency was necessary in order for citizens to properly hold government to account. Snowden was clear that "harming people isn't my goal. Transparency is" (Greenwald 2013). Since Snowden's revelations, greater government transparency has been touted as the only way to restore the trust so damaged by the secrecy of surveillance and the potential abuse that secrecy makes possible (see, e.g., Schneier 2013, 2015). Indeed, along with "privacy," "transparency" has become a mobilizing idea for resisting or overcoming the negative consequences of surveillance. While the extent to which privacy should be protected and the best means for doing so are intensely debated, the idea of transparency is invoked almost reflexively in a positive way in the public sphere, with little debate about how much transparency we need and what, exactly, we expect transparency to do to the politics of surveillance. However, a critical discussion of how and under what conditions transparency can temper the harms of surveillance seems necessary in light of the fact that Snowden's public revelations appear to have normalized rather than curtailed state surveillance practices.

Beginning in early June 2013, Snowden's leaks exposed the means and extent by which the United States National Security Agency (NSA) engaged in bulk data collection. Beyond the United States, the leaked documents also implicated the United Kingdom (UK), especially via the British Government Communications Headquarters (GCHQ), and Germany, via the Bundesnachrichtendienst (BND), in mass surveillance practices. The revelations generated heated debates in all three countries and led to calls for reform and regulation of surveillance practices; specifically, reformers focused on ending or curbing bulk data collection and providing oversight mechanisms for surveillance activities. In all three countries, review committees and commissions were established and regulatory legislation followed. Indeed, the democratic process that Snowden had hoped for

DOI: 10.4324/9781003120827-4

seemed to be underway: investigations produced public information about secret programs that in turn led to outrage, debate, and legislative reform with the intent to regulate and prevent abuses. Seen in another light, however, the United States, UK, and German cases present proponents of transparency with a puzzle. Neither the initial revelations nor the subsequent publicity of the extent of government surveillance practices led to rigorous limitations on surveillance in any of the three countries. In fact, the public debates around the surveillance practices, the outcomes of parliamentary investigations, and the subsequent policy changes had the effect of politically legitimizing, partly legalizing, and even extending surveillance practices. What is more, this was not only the likely effect but also the likely intention of some policymakers who saw the revelations as an opportunity to enable rather than to regulate surveillance. In these cases, it would seem, transparency had effects opposite to those anticipated by advocates. This chapter seeks to explain why this was so by thinking about the mechanisms and conditions that enable or limit transparency's regulatory effects. Given the hope placed in transparency, it is crucial to ask whether, when, and to what extent public revelations about surveillance practices yield effective regulatory regimes.

Transparency is always embedded in expectations about what it can *do* or *enable*. I begin by identifying the various arguments that underpin dominant claims about transparency's beneficial effects while critiquing the assumptions that underlie these claims in order to underscore the fragility and contingency of transparency. I argue that naturalistic approaches to transparency miss the ways in which its effects are linked to relations of power and embedded in socio-strategic contexts. Ultimately, transparency is not a coherent norm or practice, and so on its own it is inept at achieving sustainable regulatory outcomes (Pozen 2020). Second, I work out three alternative effects that transparency can have when we allow that transparency is subject to the politics of power: the *condoning effect*, the *ratcheting effect*, and the *circling the wagons effect*. By identifying alternative mechanisms through which transparency works, we can better understand its ambivalent nature. Third, I consider how disclosures about government surveillance practices affected surveillance legislation in three countries—the United States, Germany, and the UK. Snowden's revelations have forced governments around the world to respond to public outrage over mass surveillance, but I argue that these cases illustrate the "transparency trap"—the ways in which the apparent revelation of previously secret surveillance practices can lead to their legitimation, and even extension, rather than limitation. When transparency is focused on the revelation of information, the incentives can become counterproductive to regulatory goals. Transparency on its own is insufficient, and calls for greater transparency can be nominally followed while substantively backfiring. Following recent arguments from the emerging critical transparency literature, I suggest that a more productive approach to transparency in the context of surveillance is to understand it not as the disclosure of information but as

an ongoing sociological and communicative practice whose effects are contingent on the social, strategic, and power contexts in which it operates (see Pozen 2020; Koivitso 2019; Fischer 2019; Alloa 2018; Alloa and Thomä 2018; McCarthy and Fluck 2017).

The logics of transparency: a critical reconsideration

In contrast to surveillance, transparency has a strongly positive normative connotation as a means of preserving democracy, facilitating cooperation, preventing abuse of power, and promoting trust (e.g., see the critical discussion in Bianchi 2013; Peters 2013; Hood 2006). Transparency is often invoked as an inherent good and a self-evident remedy for countering government abuses by enhancing democratic deliberation and enabling government accountability. But to assess these promises and potential pitfalls of transparency, we first have to understand how and under what conditions it can have such effects. By what mechanisms do claims about transparency's beneficial effects work? How robust are these claims? Untangling the various logics—the chain of mechanisms that are presumed to lead to outcomes—upon which the claims of transparency's effectiveness rest can help to understand when, under what circumstances, and to what extent transparency can be regulative of surveillance. From prevailing arguments, we can identify several distinct logics of transparency based on its presumed normative and functional benefits. I outline these here and question the assumptions about information, effectiveness, and trust upon which common arguments about the good of transparency rest.

Transparency as an inherent normative good

In the first place, transparency is often endorsed on the basis of its presumed normative merits (Carson 2010); that is, on the basis of a logic of appropriateness (March and Olsen 2011). In this usage, transparency is a good in itself because it is right and appropriate and it appears to correspond with other values we hold, such as truth-telling. This approach draws on a deep-seated cultural idea about the correlation between secrecy and lying on the one hand, and between openness and honesty on the other hand, with the former coded as bad and the latter as desirable (Carson 2010). Honesty and transparency, however, are not identical. Honesty is based on the prohibition against telling lies, and thus it is a negative rule that instructs us in what not to do. Transparency, in contrast, is a positive imperative that instructs us not only not to hide but also to be candid and to be willing to reveal information. This positive imperative seriously complicates the normative value of transparency in the absence of normative rules that adjudicate when there is harm or benefit in revelation. Moreover, such a normative justification would have to take into account the empirical difficulty of identifying "true" transparency—the

conditions under which we can be assured that we have been transparent. This requires some judgment about what information is important to reveal in the first place and some way of ascertaining whether true transparency has been achieved. In other words, transparency can only take on meaning in an intersubjective context that is itself subject to negotiation and renegotiation. For these reasons alone, we should be skeptical that transparency can carry the burden of being an inherently positive normative value.

Transparency as information: a condition for democratic decision-making

More often, though, transparency is acclaimed on the grounds of its functional benefits and, in particular, for the functional role it plays in supporting democratic values and procedures. Rather than a logic of appropriateness, the virtues of transparency are in this approach based on a logic of consequences (March and Olsen 2011). We can identify at least two distinct consequentialist arguments. The first sees transparency as a condition that facilitates participation and choice via information sharing (transparency-as-information). Transparency here is related to a liberal understanding of democracy as rooted in popular participation, one that emphasizes transparency as necessary for choice. Democracies are expected to be open about decisions, to include the public in deliberation, and to seek the public's consent. In order for the public to effectively participate in political decision-making, it requires publicly available information about government activities, goals, and procedures. The importance of transparency-as-information for democratic decision-making is defended on two distinct grounds: its efficiency-enhancing effects and its legitimacy-enhancing effects.

In the view of classical liberal thinkers such as Locke, Mill, Rousseau, or Bentham, transparency enhances the efficiency or effectiveness or, in Bentham's terms, utility of democracy (see the discussion in Fenster 2006). Transparency is valued as pro-democratic because it allows citizens to make better choices and more informed decisions about which policies to support. Fung argues that "information should be publicly available in proportion to the extent to which that information enables citizens to protect their vital interests" (Fung 2013, 202). Transparency, in this account, means the disclosure of information that provides the public with clarity about the actions of government and provides the conditions to influence government priorities and steer policy outcomes in response to the public's needs and preferences. It serves as a prerequisite for informed consent and, therefore, popular sovereignty (Dahl 1971; Hollyer et al. 2011).

A more critical version of this argument sees transparency-as-information not in terms of its efficiency-enhancing effects but in terms of what we might call its legitimacy-enhancing effects on decision-making. Transparency, in

this view, is important because the disclosure and publicity of information contributes to communication and rational deliberation, which, in turn, are crucial to successful participatory democracy. Information forms the foundation for argumentation and common meaning-making. Habermas's idea of deliberative democracy, for example, rests on the principle of transparency as a prerequisite for rational, critical public debate and communication in the public sphere (Habermas 1991, 208–209; Guttman and Thompson 1996, 100–101). In theory, transparent deliberation can create an environment in which ideas are rationally proposed and probed and questioned, tested and rejected or accepted. In the ideal case, prevailing views can change when confronted with evidence and arguments, truth can be revealed, and a voluntary consensus can be achieved. A similar position is taken by Rawls, who identifies publicity as necessary for a just society because it allows individuals to choose and agree on common principles (Rawls 1971, 16, 454, 1993, 35).

The transparency-as-information approach is problematic, however, insofar as it rests on a relatively naive assumption that the disclosure of information is a straightforward process and that transparency is indeed informative. This link between transparency and democratic decision-making assumes that information can be fully and comprehensively disclosed and that more information will get us closer to the accurate truth (Albu and Flyverbom 2016, 14). The assumption here is that the transmission of information is a mechanical process that does not require interpretation and cannot be manipulated. This stands in contrast to an understanding of information as always situated, that is only meaningful as it is processed, interpreted, and mediated (McCarthy and Fluck 2017). Information is subject to power, to instrumental use, to strategic interaction, and simply to social discourses, conventions, and practices. In this understanding, then, transparency cannot refer simply to the unveiling or making visible of what is already there. Transparency as a practice is already implicated in constructing what it is that becomes visible. In this way, transparency can reinforce dominant narratives of what we think we "see." Fischer (2019), for example, shows how the visibility of trans people has normalized their representation as deceptive, deviant, and threatening—thus legitimating their violent disciplining. Another large body of empirical literature has shown that transparency can lead actors to distort their decisions by engaging in herding and conformism such that the tendency to engage in dissent decreases (Prat 2005), or by engaging in strategic "gaming" and antiherding (Levy 2004, 2007). Empirical literature that studies the effects of transparency on deliberation emphasizes the strong and negative effects that transparency has on producing conformity—not the Habermasian ideal of enlightened consensus but rather the pressure of concealing disagreement and diversity (Fehrler and Hughes 2018). In this sense, transparency produces chilling effects similar to surveillance.

Transparency as monitoring: a condition for democratic accountability

A second consequentialist logic understands transparency as a condition for accountability that operates via a monitoring mechanism (transparency-as-monitoring). Indeed, some have argued that the most significant consequence of transparency is that it allows the public to monitor government activity and hold it accountable (Meijer 2014). The assumption underpinning this approach is that governments (or authoritative powers more generally) have the power and ability to act against the will of the people or harm the collective welfare. Transparency enables monitoring government activity for transgressions that can then be corrected or punished. Transparency, on this account, works both via an *ex ante* disciplining effect and an *ex post* punitive effect. The deterrent effect is that the fear of consequences of exposure should induce self-disciplining and, therefore, more favorable behavior. The punitive component is that exposure should make punishment more likely—either directly through reputational costs (e.g., shaming, shunning, etc.) or by activating procedural measures (e.g., due process).

This view of transparency rests on an adversarial approach that emphasizes not public collaboration (or participation) in ruling but a rebalancing of power between the government and the public (Pozen and Schudson 2018). On these grounds, McCarthy and Fluck criticize advocates of transparency for promoting "the creation of monitory democracy, rather than participatory democracy" (McCarthy and Fluck 2017, 422). In this logic, transparency becomes indistinguishable from surveillance itself in that it works as a mode of control. To the extent that both transparency and surveillance operate on the basis of monitoring in an effort to deter or punish certain behaviors, transparency would have the potential to evoke the same kind of social distortions as surveillance—including chilling effects, self-monitoring, and reduction of liberties. Moreover, making transgressions transparent can reveal them as the "norm," and transgressions that are revealed but left unsanctioned can be, paradoxically, legitimized and made acceptable through transparency.

Transparency as a condition for trust

Taken together, the above arguments in favor of transparency are often pushed one step further to claim that transparency—precisely because it enhances efficiency and accountability—also promotes trust. To the extent that public trust is considered crucial to governance and, in particular, democratic governance (Cook 2001; Hardin 2002a; Cook et al. 2005), transparency is promoted as a policy goal of its own. In these arguments, trust is directly linked to access to information and the possibility of public scrutiny. Transparency provides a costly signal because it exposes an actor to examination and possible punishment in the event of

transgressions, and so our confidence—or trust—should be greater toward those willing to be subject to scrutiny (Brugger et al. 2013, 67; Kydd 2000; Hardin 2002a).

This theorized relationship between transparency and public trust is problematic on two counts. First, it assumes again that transparency is somehow neutral or objective and not subject to interpretation, meaning-making, manipulation, and counterintuitive reactions. Second, this view conceives of trust as the result of the risk management that transparency affords, reducing trust to a notion of compliance based on cost assessments (Rathbun 2012, 3–7; Bugger et al. 2013, 74). But if trust is to have any independent theoretical leverage beyond instrumental calculus, then it needs to be conceptualized as willingness to cooperate under conditions of vulnerability to exploitation, rather than under conditions of verifiability. In this view, trust works through social beliefs that others will cooperate and reciprocate *in the absence of* monitoring and punishment mechanisms (Uslaner 2002). Trust, unlike transparency, is not a mode of control. Transparency, then, cannot restore or establish trust, but rather, it substitutes for it by providing a monitoring mechanism that enables enforcement. Indeed, transparency can be a powerful signal of *distrust* to the extent that it is used as a monitoring mechanism (O'Neill 2002; Hardin 2002b). Even more, greater transparency can reduce trust in partners by exposing deceptions as the norms—e.g., "they're all crooks"—or by fueling fears of punishment. In the foreign policy world, recent work shows that greater transparency in international relations can actually reduce trust in partners by exposing deceptions and "normalizing" them (Carnegie and Carson 2018).

The ready embrace of transparency as a watchword for normative and instrumental ends masks difficult questions. In particular, does transparency always promote accountability and cooperation? Under what conditions does it do so or fail to do so? If transparency, understood as disclosure, is a way of regulating behavior, then how is conduct disciplined or normalized by transparency, under what conditions, and with what consequences?

Three distorting effects of transparency

The broader problem with standard views on the beneficial effects of transparency and the mechanisms by which transparency achieves them is that they are rooted in an understanding of transparency as the objective disclosure of information, without paying much attention to the intersubjective and strategic contexts in which transparency as a *communicative* act occurs. Critical transparency studies, in contrast, see transparency "as complex communicative, organizational, and social processes rife with tensions and negotiations, and largely unsettles the assumed positive effects of information disclosure" (Albu and Flyverbom 2016, 10). Transparency does not "merely" disclose information but shapes and creates relations of power. These relations of

power, in turn, condition the kinds of effects transparency can have on sociopolitical relations.

If we take transparency to be embedded in social relations, then we should expect complex strategic interactions to arise. Indeed, empirical works on transparency from a variety of fields ranging from labor economics to psychology to criminology have noted this. Drawing on insights from critical transparency studies, in this section I discuss three dynamics through which transparency might lead not to the regulation of surveillance, but to its wider use, undermining accountability and reducing the effectiveness of civil society critique to shape policy. These three dynamics, resulting in what I label *the condoning effect*, *the ratcheting effect*, and *the circling the wagons effect*, are based on a notion of transparency not as the simple revelation of information but as a strategic and political process of negotiation over meaning that takes place in the context of asymmetrical power relations. The idea is both to offer a corrective to the positive/progressive bias implicit in dominant understandings of transparency and also—importantly—to better grasp *how* demands for transparency might promote rather than restrain state surveillance practices.

First, what I call the *condoning effect* is triggered when high levels of revealed noncompliance reduce the perceived social opprobrium for violating the norm and lead instead to demands for normalizing or legitimizing the behavior. The revelations that follow from transparency offer an opportunity not only to condemn the behavior, as an accountability approach might argue, but also to discuss and normalize it.[1] In the case of surveillance, exposure of illegal surveillance led both to public outrage *and* to debates about how to legalize it. Thus, under the guise of reform legislation, many illegal surveillance practices exposed by Snowden were given a legal basis and, therefore, legitimized. Arguably, the widespread revelations of surveillance—not just by the NSA but also by private firms such as Facebook—have normalized the idea of collecting and utilizing mass data. Exposure and disclosure imply that the behavior is more widespread than anticipated, thus removing the taboo.

Second, the *ratcheting effect* is activated when disclosure of specific violations of the rule or norm creates incentives for more of the same behavior because of revelations that "others are doing it too." This can happen, for example, when asymmetries are disclosed that appear threatening or that appear to require a response in kind. In this case, the reaction might be not to sanction the violation with greater legal restrictions but to allow something like "self-defense" by engaging in the same violations and thereby removing the asymmetry. In the gun law debate in the United States, for example, cases of gun violence often have the counterintuitive effect of leading not to greater gun restrictions but rather to calls for more widespread use of weapons, such as by arming teachers. In the surveillance debate, this might be illustrated by calls to engage in ultraexposure or ultraexhibitionism as a way to reclaim control over the externalization of information and as an act of resistance

against the profiling, sorting, and categorization that surveillance performs. In the case of counterterrorism this often takes the form of "we need all the tools at our disposal" to fight the perceived threat, and even more so now that our tools have been revealed. In the case of US–German relations, there was a lot of anxiety about the greater technological capacity of the United States. A number of German politicians argued that Germany needed to step up its own surveillance practices in order to meet the threat of the Americans rather than engage in greater regulation that would hamper its ability to compete and leave it exposed to the power asymmetry. The "everyone is doing it" argument was used as rhetorical justification for the empowerment of BND surveillance in the German case. In all three cases considered below, once exposed, the intelligence community used the exposure and transparency to argue for even greater measures.

Third, the *circling the wagons effect* is at work when the anticipated exposure that comes from transparency creates incentives for complicity in opacity. At the level of the government, the monitoring implications of transparency might trigger a fear of evaluation and lead to self-censoring or strategic disclosure, such that the presumed benefits of transparency are not attainable and surveillance programs are protected. This is familiar on the individual level as the chilling effect, when, for example, the recording of deliberations leads participants to alter their utterances or engage in self-censorship in anticipation of possible negative consequences (see Hall, this volume). In the case of state surveillance, transparency requirements might lead to the creation of a double-move of partial revelations combined with greater secrecy, for example, through the increasing usage of top-secret classifications or through resistance to rules of oversight, thereby enabling and empowering the circumvention of transparency (Priest and Arkin 2011; also Laidler, this volume). This backlash effect creates practices that restrict information disclosure, minimize oversight, or entrench ineffective programs in anticipation of the negative effects of transparency and the desire to protect the surveillance programs in question.

All three dynamics highlight processes by which transparency can have a distorting effect on democratic demands for regulating and restricting surveillance. In the next section, I argue that all three are present in the public debates and government responses to Snowden's revelations in the United States, UK, and Germany.

The transparency trap: legislative reform of surveillance in the United States, UK, and Germany

The public disclosures by Snowden were wide ranging and implicated not only the United States but also surveillance in the UK and Germany. Arguably, public outrage and the government response were strongest in these three countries. Governments in all three countries came under intense pressure to

investigate Snowden's claims and to offer policy reforms. All three countries indeed passed legislation at about the same time aimed at regulating surveillance practices. While the details in each case differ, I argue that they follow a similar pattern for the period under investigation, 2003–2019. First, outrage over revelations led to calls for greater transparency, leading to further revelations and calls for regulation. Second, in the process of formulating legislative measures to restrict surveillance abuses, (1) the state ends up *condoning* the condemned surveillance practices by providing them with a legal basis, (2) the state *ratchets* up surveillance practices by legislating even more extensive surveillance powers in order to be "competitive" against threats, and (3) some actors succeed in *circling the wagons*—i.e., promoting protections of surveillance practices and surveillance agencies against too much transparency, oversight, and regulation.

The US case: the USA Freedom Act (2015)

While Snowden's disclosures had global reverberations, they were primarily concerned with the surveillance programs of the US government and, in particular, the NSA. Snowden's leak of massive amounts of information regarding government surveillance practices generated an intense debate about the extent, methods, and secrecy of surveillance. In response to public outrage, President Obama initially defended the importance of surveillance for counterterrorism measures and for ensuring the security of the country while downplaying its costs. In his first statement on the revelations, he quipped, "You can't have 100% security and also then have 100% privacy and zero inconvenience" (Obama 2013). Slowly, and pushed by the nature and extent of the revelations, Obama acknowledged that secret mass data collection programs were problematic due to the lack of a legal basis for many NSA activities. He appointed an expert panel, the President's Review Group on Intelligence and Communications Technologies, to review surveillance practices and laws. In addition, the Privacy and Civil Liberties Oversight Board (PCLOB), in response to Snowden's leaks, engaged in a comprehensive review of warrantless surveillance allowed under the Patriot Act. Both of these investigations confirmed the need for surveillance powers to thwart terrorism but also recommended proposals to introduce some limits on and greater transparency of government surveillance. The PCLOB concluded that the Patriot Act did not provide a legal basis for the NSA to collect bulk metadata. Although Obama had previously signed extensions of the Patriot Act, he responded to the new concerns by signing a new law—the USA Freedom Act—that was meant to restrict bulk data collection and enhance transparency of surveillance practices. The Freedom Act is the central legislative reform response to the Snowden revelations in the United States.

Although the Freedom Act is seen by many, especially outside the United States, as a significant effort to limit surveillance powers, the law in effect

reaffirms and even expands the government's legal surveillance powers. In a clear example of the condoning effect, Snowden's leaked information led the government to seek a stronger legal basis to legitimize the revealed surveillance practices. The expiration of the Patriot Act sunset provisions would have ended the legal basis for continued surveillance programs, but the Freedom Act reprises and extends that legal basis. As Obama (2015) put it:

> After a needless delay and inexcusable lapse in important national security authorities, my Administration will work expeditiously to ensure our national security professionals again have the full set of vital tools they need to continue protecting the country. Just as important, enactment of this legislation will strengthen civil liberty safeguards and provide greater public confidence in these programs, including by prohibiting bulk collection through the use of Section 215, FISA [Foreign Intelligence Surveillance Act] pen registers, and National Security Letters and by providing the American people with additional transparency measures.

The Freedom Act did reform the telephone metadata collection program, forbidding the data from being transferred to and stored on government servers.[2] The data stays with telephone companies and is kept for 180 days, and it can only be transferred to intelligence agencies on the basis of a Foreign Intelligence Surveillance Act (FISA) court warrant. Such warrant requests must be based on specific criteria to avoid bulk collection. In addition, warrant requests are made in a FISA court in the presence of citizen privacy advocates, and the requirements for publication of FISA court rulings were expanded. Nevertheless, it remains trivially easy to obtain a FISA court warrant, and according to the government itself, the Freedom Act greatly expanded the overall volume of call detail records subject to query pursuant to court order.[3] According to the "Statistical Transparency Report," created to comply with the terms of the Freedom Act, 2017 tripled the number of call detail records (543 million) collected compared to the previous year (Office of the Director of National Intelligence 2018). This is still far less than the billions of records swept up before the Freedom Act, but it indicates that mass telephony data collection has hardly stopped in spite of Obama's promise of "prohibiting bulk collection." Moreover, while the Freedom Act addressed some of the concerns connected to the Patriot Act, it did not address the broader statutory basis for security surveillance. Most importantly, the FISA Amendments Act of 2008 (FAA), which authorized the NSA's PRISM surveillance program, remains in place.[4] The FAA was itself a response to whistleblower revelations in 2005/2006 that the NSA under the Bush administration was involved in warrantless wiretapping (Risen and Lichtblau 2005; Cauley 2006). The exposure of surveillance to public scrutiny in 2005 and 2006 led to the passage of the FAA in 2008. While the FAA was nominally meant to restrict surveillance and protect civil liberties by strengthening the warrant process, in effect it provided a

legal basis for expanded surveillance powers and reduced restrictions on the targeting of persons. The FAA has been repeatedly reauthorized by Congress with bipartisan support, most recently in January 2018 for six years. Overall, the public discussion about previously secret surveillance practices, enabled by whistleblowers, did not lead to the disavowal of those practices, but rather to an acknowledgment of their existence and a bolstering of their legal basis, providing them official legitimacy.

Another consequence of revealing secret surveillance practices has been the ratcheting effect. The intelligence community has continued to argue that transparency over secret surveillance programs has left the country exposed to security threats, thus justifying greater surveillance measures. US intelligence agencies have carried out numerous classified assessments of the damage caused by Snowden's disclosures. The counterintelligence center continues to claim that damage has been observed or verified, including putting US personnel or facilities at risk, damaging intelligence collection efforts, exposing surveillance tools, and destabilizing US intelligence capabilities (Riechmann 2018). The disclosure of information through whistleblowers has provided ammunition for some to argue for even greater, rather than more restrictive, surveillance powers. Senator Mitch McConnell criticized the passage of the Freedom Act, stating that "It surely undermines American security by taking one more tool from our war fighters, in my view, at exactly the wrong time" (quoted in Strobel and Zengerle 2015). When the November 2015 Paris attacks occurred a few months after the bill's passage, Director of the CIA John Brennan called the attacks a "wake-up call" for the United States to continue controversial surveillance practices, including those that had been mildly limited under the Freedom Act. Brennan asserted that efforts to curtail surveillance practices "make our ability to collectively, internationally, to find these terrorists much more challenging" (quoted in The Editorial Board 2015). Even a modest limit on surveillance practices with dubious effectiveness is seen within the intelligence community as an impediment to counterterrorism.

Within the intelligence community, Snowden's revelations triggered a move to "circle the wagons"—that is, to reduce the anticipated damage that might come about through transparency by protecting existing programs and maintaining secrecy where possible, leading in turn to further distortions of policymaking (Lester 2015). Before Snowden's disclosures, there was already concern within the intelligence community that the massive amount of data collected was inefficient and ineffective. Ironically, the call detail record program that was reined in but not discontinued by the Freedom Act was probably prolonged by the legislation. According to some intelligence officials, "If Snowden hadn't revealed it, NSA probably would have dumped it on their own." It did not, because "There was a great desire to circle the wagons …" (Nakashima 2019). Indeed, the NSA continued to defend the usefulness of the program to the public. But in 2019 the NSA admitted that the

program was ineffective and advised the government to discontinue it (Strobel and Volz 2019). Nonetheless, on August 14, 2019, the Trump administration asked Congress to permanently reauthorize all provisions of the Freedom Act, including the controversial call detail record program.[5] Outgoing Director of National Intelligence, Dan Coats, acknowledged that the program had been suspended on the grounds of its ineffectiveness but argued that it should nevertheless be renewed to give the government every possible tool to confront its adversaries. In a letter to Congress, he argued that "as technology changes, our adversaries' tradecraft and communications habits will continue to evolve and adapt. In light of this dynamic environment, the Administration supports reauthorization of this provision" (Savage 2019; Guariglia 2019).[6] The logic here seems to be defensive and conservative in the fear that something might be taken away—even if that program is demonstrably not useful.

The UK case: the Investigatory Powers Act (2016)

The Snowden revelations implicated the GCHQ in mass surveillance practices and began a debate about the legal basis of bulk data collection, use, and retention policies in the UK. Snowden's information on secret government practices and the connections between the NSA and GCHQ framed a public debate and a policy environment in which the reconsideration of data collection legislation became necessary (Hintz and Brown 2017, 788, 792). In this sense, Snowden's disclosures led to a public debate that likely would otherwise not have happened, and it led to the creation of review committees that raised concerns about the legitimacy and legal grounding of surveillance practices (Anderson 2015). Several different laws regulated various aspects of UK surveillance practices, including the Telecommunications Act (1984), the Data Protection Act (1998), and the Regulation of Investigatory Powers Act (2000). The reviews concluded that the absence of a cornerstone piece of legislation produced regulatory gaps and overlaps, as well as regulatory opacity. Moreover, it was unclear whether some of the newly disclosed practices of UK intelligence agencies had any legal basis at all under existing legislation. In this context, the government decided to introduce new legislation to provide a statutory basis for ongoing surveillance practices. After laws proposed in 2013 and 2014 were defeated,[7] the Investigatory Powers Act (IPA) was introduced and then enacted into law in November of 2016.

As in the US case, the UK government's legislative action was meant to provide a legal basis that would defend and legitimize its contentious surveillance powers. The Act aims to stipulate the electronic surveillance powers of the UK intelligence agencies as well as to impose some checks on those powers. The validation of wide-ranging surveillance powers was justified on the basis of the threat they are supposed to secure citizens against. When the draft IPA bill was released, a government source was quoted in *The Independent* (Griffin 2015) as saying:

> We know these powers are needed as technology changes and terrorists and criminals use ever more sophisticated ways to communicate. But we need to give people the reassurance that, not only are they needed, but that they are only ever used in a necessary, proportionate and accountable way. That is what this bill is all about.

The law has been praised for being "the most transparent bit of legislation that Britain's ever had" (quoted in Hintz and Brown 2017, 795), on the grounds that it provides a clear legislative framework for surveillance activities. Critics, in contrast, have argued that the opportunity for fundamental change to surveillance practices and tighter regulation was lost and that the main purpose of the law is to legitimize what was previously secret practice, now that it has come to light (see Hintz and Brown 2017, 795 and similar statements by their interviewees). In the words of Hintz and Brown (2017, 797), "Policy reform in the UK has not led to a fundamental revision of surveillance practices, nor to a broader public debate that would help to democratically legitimize these practices." Rather, the new legal framework reflects and reinforces the power of the state. As *The Guardian* reported, "A bill giving the UK intelligence agencies and police the most sweeping surveillance powers in the western world has passed into law with barely a whimper, meeting only token resistance from inside parliament and barely any from outside" (MacAskill 2016).

The IPA, which has come to be called the "Snoopers' Charter," provided a statutory basis for practices relating to the bulk interception, collection, use, and storage of communications data, including the metadata of emails, texts, and cell phone calls. The IPA obliges internet service providers to store the internet connection records of their customers for 12 months. Moreover, designated officers in intelligence, law enforcement, and tax or customs agencies can grant their analysts access to this data on a wide range of grounds, including "public health," "financial stability," and "national security" (Investigatory Powers Act 2016, Part 3, 63(7)). The law further provides a legal basis for agencies to remotely access digital communications devices and legally requires third parties to assist in doing so when necessary; in other words, corporations can be forced to circumvent their security features to allow access to communications (UK Home Office 2017). So-called "equipment interference" is allowed in the course of preventing or investigating a criminal offense, furthering the national security interest, or furthering the national economic interest when related to national security. As a concession to privacy concerns, the IPA gives judges the power to veto surveillance requests, but intelligence agencies can request "thematic" rather than individual warrants, limiting this judicial oversight. Moreover, while the relevant minister and a judicial commissioner need to agree in domestic cases, "bulk equipment interference warrants" can be issued in the case of "overseas-related communication." A bulk interference warrant authorizes "any conduct which it is necessary to undertake in order to do what is expressly authorized

or required by the warrant" (Investigatory Powers Act 2016, Part 6, Chapter 3, 177(5)). In light of this permissiveness, Snowden called it legalization of "the most extreme surveillance in the history of Western democracy" that even "goes farther than many autocracies" (MacAskill 2016).

Not only did the IPA condone existing practices by providing a statutory basis, but the IPA also extended the state's surveillance powers (Hintz and Brown 2017, 789; see also Loftus 2019). As the ratcheting effect expects, the opportunity to draw up surveillance legislation was seen by intelligence and law enforcement agencies as a chance to further enhance their powers. Importantly, many of these powers were sought by law enforcement agencies not directly related to counterterrorism (Gallagher 2015). In fact, the IPA grants these powers not only to British intelligence agencies; hacking and secret warrants can be used by law enforcement agencies including the police force and tax and customs agencies. The IPA reflects the oft-articulated argument that surveillance practices need to remain flexible given a rapidly evolving technological environment. In the assessment of David Anderson, the Independent Reviewer of Terrorism Legislation, "If the new law is to have any hope of accommodating the evolution of technology over the next 10 or 15 years, it needs to avoid the trap of an excessively prescriptive and technically-defined approach" (Anderson 2016). According to Hintz and Brown, the Investigatory Powers Bill "constituted a significant shift in British surveillance policy by opening up many of the traditionally secret surveillance measures to public scrutiny and oversight. However, the substance of surveillance powers largely remained and partly expanded" (Hintz and Brown 2017, 789).

Once passed, the IPA was challenged in court by civil liberty organizations. Liberty, a civil rights organization, brought a lawsuit against the government for noncompliance with the law and abuse of rights, stating: "This is a clear-cut example of how the supposed safeguarding and oversight system is failing to protect us from the excessive and unwarranted surveillance and data retention powers created under the 'snooper's charter'" (Bowcott 2019a).[8] The head of the official oversight body, Investigatory Powers Commissioner Lord Justice Fulford, confirmed that MI5 had been noncompliant, including illegally acquiring and storing bulk data and obtaining surveillance warrants on the basis of false information (Bowcott 2019b). In response to the suit, Home Secretary Sajid Javid acknowledged the existence and continuation of serious problems but argued that these were internal matters and, further, that the flagging of them by the watchdog was a vindication of existing safeguards. He explicitly argued against further transparency and applied for closed proceedings that would exclude the public and the media, saying, "I have concluded that such material cannot be disclosed in open [court] because of the damage such disclosure would cause to the interest of national security" (Bowcott 2019a). In July 2019, the UK courts rejected Liberty's argument that bulk data collection under the IPA violates rights and agreed

with the government that the IPA includes sufficient "safeguards against the possible abuse of power" (Perraudin 2019). Counsel representing the government argued that "[t]he powers under challenge are of critical importance to, and are effective in securing, the protection of the public from a range of serious and sophisticated threats arising in the context of terrorism, hostile state activity and serious/organized crime" (Perraudin 2019). Rather than engage in debate and reform in the face of disclosures about ineffectiveness and abuse, the government circled the wagons and defended not only its broad powers but also argued against further disclosure.

The German case: the BND Reform Bill (2016)

Among Edward Snowden's many revelations regarding the United States's surveillance program in 2013 was information that the NSA carried out illegal surveillance not only of Americans but also of citizens of many other countries, including Germany. The leaks notoriously indicated that the NSA was monitoring Chancellor Angela Merkel's private cell phone. These revelations unleashed a heated debate in Germany about the extent of surveillance and also the state of the transatlantic relationship. The public was furious about the implications of the Snowden revelations for privacy. Pundits called the surveillance of Merkel's phone "a game changer in Europe" (Knigge 2013). Merkel famously remarked that there should be no spying "among friends," telling reporters, "We need trust among allies and partners … an alliance can only be built on trust. That's why I repeat again: spying among friends, that cannot be" (Spiegel International 2013a). And, indeed, public opinion polls showed that German citizens' trust in the United States plummeted after the revelations (Spiegel International 2013b). Beyond Merkel's cell phone, the public—in Germany just as in the United States—was outraged that they were subject to unchecked surveillance.

In response to the outcry, in March 2014 the Bundestag launched a parliamentary committee including representatives from governing and opposition parties to investigate the spying accusations.[9] One of the driving questions was whether the United States had betrayed Germany's trust. But, in spite of the public's outrage and the government's initially strong negative reaction, it soon became apparent that the investigatory committee was unlikely to take a hard line. By 2015, officials were dismissing the specific claim that Merkel's cell phone was tapped, even though—at Merkel's request—it was never forensically examined.[10] The Chancellor herself testified before the committee that it was never proven that US intelligence agencies had listened in on her conversations, and she emphasized that President Obama had assured her that her phone was not tapped (Chase 2017). In May of 2017, when the committee wrapped up its three-year-long investigation, its final report concluded that there were "no reliable grounds" for the accusation that the NSA and other intelligence agencies "illegally, systematically

and massively monitor German telecommunications and internet traffic."[11] Moreover, it claimed that the documents provided by Snowden contained "no solid evidence about espionage activities in or against Germany." Although it is clear that the NSA has the capacity to engage in surveillance of Germany, the conclusion was that it never specifically targeted Germany. Indeed, the report reached many "surprisingly positive" conclusions, including that: "The committee is of the opinion that despite all the difference concerning NSA spying in the past there is relatively large agreement about the rigor and establishment of intelligence service oversight by the parliaments in Germany and the US" (Deutsche Welle 2017a).

Despite political attempts to dampen public concern about surveillance, the investigation unearthed and made public critical information about the nature and extent of surveillance that had hitherto been publicly unknown. The investigation revealed that the German intelligence agency, the BND, actually cooperated with NSA surveillance programs, supporting the NSA in its surveillance of allies and providing data to aid US drone warfare in other parts of the world. German media also reported that the NSA had provided German intelligence services with spy software in exchange for data sharing. Pointing to Germany as an example, Snowden argued that "[t]he countries whose citizenries were most opposed to American mass surveillance were those whose governments had most cooperated with it" (Snowden 2019). Moreover, documents first reported on by *Der Spiegel* and then also confirmed by a parliamentary report showed that from 1998 until 2013 the German intelligence services were also operating their own surveillance programs targeting state officials and private citizens. The BND was surveilling hundreds of foreign embassies, including EU and NATO member state diplomats, as well as heads of state, ministers, and ministry staff (Deutsche Welle 2016). Among many other countries, this included surveillance of US government officials (and their emails) from the White House, State Department, Department of the Treasury, military offices, and elsewhere, as well as the surveillance of US businesses (Deutsche Welle 2017b). Moreover, according to the report, the BND was also engaged in surveillance of officials at international organizations, such as the International Monetary Fund, as well as nongovernmental organizations and industries connected to—among other areas—arms trade, aviation, and space. It was because of Snowden's revelations that Germans came to discover the extent of the BND's surveillance.

The 2016 leaked report by Data Protection Commissioner Andrea Voßhoff became a key impetus for policy reform debates. In addition to detailing BND surveillance activity, it argued that those activities should not continue without a legal basis. According to the report published by netzpolitik.org, the "BND has collected personal data without a legal basis and has processed it systematically. The BND's claim that this information is essential cannot substitute a missing legal basis. Limitations of fundamental rights always

need to be based on law" (Meister 2016a). The government came under public pressure to provide better oversight and accountability mechanisms even before the parliamentary inquiry into the Snowden affair ended. Thus, in 2016 the Bundestag debated and swiftly passed legislation aimed at comprehensive reform of the BND-law (BND-Gesetz or BNDG). The reform proposals were passed despite extensive critique by civil society organizations (Meister 2016b).[12] As with the United States and UK cases outlined above, the legislative response had the effect of legalizing heretofore illegal surveillance activity and even expanding and protecting the work of the BND.

The stated purpose of the new BND reform legislation was to strengthen government monitoring of intelligence activities by, for example, subjecting them to an independent panel of judges and a permanent commissioner from the Interior Ministry, making the surveillance of international communications subject to authorization by the Chancellor's office, and making annual BND oversight hearings public rather than private. The legislation also prohibits economic and industrial espionage and offers protections for whistleblowers. At the same time, however, the legislation for the first time explicitly allowed the BND to cooperate with foreign intelligence services, and it explicitly permitted the BND to engage in surveillance of EU institutions and other EU member states when the purpose is to gather "information of significance" for Germany's foreign and security policy. The law allowed the strategic surveillance, including collection, storage, and evaluation, of the telecommunications data of foreigners in foreign countries even in the absence of specific suspicion or cause and allowed for the sharing of this data with foreign intelligence agencies. In other words, the legislation meant to reform and rein in the BND now provides a legal basis that condones the very surveillance activities that had been the source of civil society outrage over the abuse of state power. Critics of the law have said that it rewards the BND, with Amnesty International calling it "nothing but a free pass to intrude into people's private spheres" (quoted in Chase 2016).

In addition to the condoning effect, the reform bill also expanded the BND's power. In light of the Snowden revelations, concern grew that Germany was technologically behind the United States and, as a result, at a strategic disadvantage. Proponents of the legislation argued that it brings the BND into the twenty-first century. The former Chairman of the NSA investigatory committee, Clemens Binninger, asked rhetorically, "How else is the BND supposed to protect us against terrorism other than listening in on conversations between people outside of Germany?" (quoted in Chase 2016). While previously the BND was restricted to listening in on 20% of the traffic that ran through specific internet cables, the new law allows the BND to store and analyze all traffic running through any cable (BND Reform Bill 2016, §6 Absatz 1).[13] The communications of foreigners can be stored and analyzed in order to "ensure the Federal German Republic's capability to

act" (ibid.). Moreover, metadata, as long as it cannot be identified as coming from German citizens, can be stored for six months and transferred to foreign "partners" (BND Reform Bill 2016, §15).

Another concern raised by policymakers in this period was that the revelations about BND surveillance shouldn't lead to the kind of "over-reaction" that would limit the BND and compromise security. Indeed, although the stated goal was to "rein in" the BND, this was complemented by a circling-of-the-wagons mentality that tried to protect the powers of the BND. Rather than framing the law as a restraint on the BND, supporters argued that the law should promote the BND. Accordingly, the head of the Inquiry Committee and Christian Democratic Union (CDU) parliamentary member Patrick Sensburg assured the parliament that "the BND will not be put in chains" (Deutscher Bundestag 2016, 18280C). The Federal Minister for Special Affairs, Peter Altmeier, underscored the point, adding "we don't want to limit the work of the BND. We want to base it on a clear and *publicly transparent* foundation" (Deutscher Bundestag 2016, 18274D).[14] Although the law added an "independent" institution to carry out oversight of the BND, none of the oversight bodies was allowed a complete picture of the BND's activities and they are dependent on BND reporting. Gerhard Schindler, president of the BND from 2012 to 2016, critiqued the oversight mechanisms for being insufficient, arguing that the BND's control over what information gets reviewed defies the logic of independent oversight (Steinke and Pinkert 2016).

The BNDG reform has since been subject to legal contestation, particularly from civil society organizations and journalists claiming that the law violates the German Basic Law with respect to the collection of personal data and freedom of the press. On May 19, 2020, in response to a suit brought by *Reporters sans frontières*, the German Constitutional Court ruled that the law regarding the telecommunications surveillance of foreign nationals abroad does violate fundamental rights and ordered the law to be amended in conformity with constitutional rights.[15] The judgment was significant because it affirmed for the first time that German authorities are bound to respect fundamental rights not only at home but also when acting abroad vis-à-vis foreigners. At the same time, it declared telecommunications surveillance of foreigners abroad to be fundamentally permissible on the grounds of the overriding public interest. In response to the judgment, the Bundestag passed a new BNDG reform law on April 19, 2021.[16] The central goals of the reform are to provide a stronger legal basis for the collection of telecommunications of foreigners abroad and to introduce new control mechanisms. A newly created Independent Control Council is to be introduced to monitor the legality of BND investigations. In the view of the government, the overall aim of both of these measures is to legitimize the collection of foreign information abroad and to make the surveillance powers of the BND more precise.[17]

Conclusions

The goal of this chapter has not been to argue against transparency, but rather against a naive notion of transparency as a remedy to surveillance abuses and a boon to democracy. Because transparency works as a social practice, we need to be sensitive to the ways in which it interacts with power to redistribute risks and vulnerabilities. While the hope may be that transparency can promote honesty, enable accountability, and limit transgressions, I argue that it can have the effect of condoning, promoting, and protecting state surveillance practices. In each of the cases considered here—the United States, UK, and Germany—the government response to public outrage over revelations about the extent of surveillance has been to investigate, reveal, and then legitimize those practices. Public responsiveness to surveillance concerns ultimately allowed governments to defend and expand their surveillance powers.

Transparency, understood as the practice of disclosure, is, on its own, insufficient to do the work of regulating the surveillance state. Transparency should not be attributed independent agency that somehow naturally delivers a rebalancing of power. Disclosure does not have automatic consequences but is subject to power, negotiation, and cooptation. To preserve its democratic power, transparency needs to be understood as an ongoing negotiation over the meaning and value of competing social goods. This ongoing negotiation does not end once transgressions are revealed, nor when pressure is mounted to elicit a government response, but it requires constant vigilance and active contestation.

Notes

1 In my particular case, I am assuming that surveillance is an activity that the public wants checked; but it would be perfectly consistent with my argument to claim that, for example, the condoning effect can lead to normatively desirable outcomes. This might be the case, for example, when the condoning effect leads to the breakdown of a taboo or norm that was restrictive of rights (e.g., undermining norms against homosexuality).

2 www.intelligence.gov/index.php/ic-on-the-record-database/results/787-fact-sheet-implementation-of-the-usa-freedom-act-of-2015. See also Snowden (2019).

3 www.intelligence.gov/index.php/ic-on-the-record-database/results/787-fact-sheet-implementation-of-the-usa-freedom-act-of-2015.

4 This is also true of other legal instruments that sanction government surveillance, such as the 1981 Executive Order 12333, which authorized expansive data collection and provided the basis for subsequent surveillance-related Executive Orders (see, e.g., Tye 2014).

5 Provisions of the Freedom Act were set to expire in December 2019 pending reauthorization.

6 Coates' argument is particularly unconvincing, since one reason for the ineffectiveness of the program is its outdatedness, given the shift to internet-enabled encrypted connections.

7 The Draft Communications Bill was defeated in 2013, and the 2014 Data Regulation and Investigatory Powers Act (DRIPA) was passed but legally challenged and then suspended.
8 Because the European Court of Justice ruled that the provision for bulk data collection in the 2014 DRIPA was unlawful, many observers thought a similar case could succeed against the IPA.
9 This was the "Erster parlamentarischer Untersuchungsausschuss des 18. Bundestages," or colloquially, the "NSA-Untersuchungsausschuss."
10 She claimed she did not want to jeopardize the privacy of her communications.
11 The report, however, was not endorsed by all parties. The opposition wrote its own report in dissent that was never released.
12 This is the *Gesetz zur Ausland-Ausland-Fernmeldeaufklärung des Bundesnachrichtendienstes vom 23. Dezember 2016.* Herein referred to as the "BND Reform Bill."
13 For the previous restrictions, see Meister (2015).
14 The original German of the italicized text is "öffentlich nachvollziehbare."
15 The judgment can be found here: www.bundesverfassungsgericht.de/e/rs20200519_1bvr283517.html.
16 Available here: www.gesetze-im-internet.de/bndg/BJNR029790990.html#BJNR029790990BJNG000403377.
17 See the Bundestag statement here: www.bundestag.de/dokumente/textarchiv/2021/kw04-de-bnd-gesetz-817444.

References

Albu, Oana, and Mikkel Flyverbom. 2016. "Organizational Transparency: Conceptualizations, Conditions, and Consequences." *Business & Society* 58(2): 268–97.

Alloa, Emmanuel. 2018. "Transparency: A Magic Concept of Modernity." In *Transparency, Society and Subjectivity*, edited by Emmanuel Alloa and Dieter Thomä: 21–56. London: Palgrave Macmillan.

Alloa, Emmanuel, and Dieter Thomä, eds. 2018. *Transparency, Society and Subjectivity: Critical Perspectives*. London: Palgrave Macmillan.

Anderson, David. 2015. "A Question of Trust: Report of the Investigatory Powers Review." June 2015, https://terrorismlegislationreviewer.independent.gov.uk/wp-content/uploads/2015/06/IPR-Report-Web-Accessible1.pdf.

Anderson, David. 2016. "Report of the Bulk Powers Review." August 2016, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/546923/56730_Cm_9326_PRINT.PDF.

Bianchi, Andrea. 2013. "On Power and Illusion: The Concept of Transparency in International Law." In *Transparency in International Law*, edited by Andrea Bianchi and Anne Peters: 1–20. Cambridge: Cambridge University Press.

BND Reform Bill. 2016. "Gesetz zur Ausland-Ausland-Fernmeldeaufklärung des Bundesnachrichtendienstes vom 23." December 2016, www.bgbl.de/xaver/bgbl/start.xav?start=%2F%2F*%5B%40attr_id%3D%27bgbl116s3346.pdf%27%5D#__bgbl__%2F%2F*%5B%40attr_id%3D%27bgbl116s3346.pdf%27%5D__1580989707655.

Bowcott, Owen. 2019a. "Sajid Javid Wants High Court Hearing into MI5 Failures to Be Secret." *The Guardian*. May 20, 2019, www.theguardian.com/uk-news/2019/may/20/sajid-javid-high-court-hearing-mi5-failures-secret.

Bowcott, Owen. 2019b. "MI5 Accused of 'Extraordinary and Persistent Illegality.'" *The Guardian*. June 11, 2019, www.theguardian.com/uk-news/2019/jun/11/mi5-in-court-accused-of-extraordinary-and-persistent-illegality.

Brugger, Philipp, Andreas Hasenclever, and Lukas Kasten. 2013. "Vertrauen lohnt sich." *Zeitschrift für Internationale Beziehungen* 20(2): 65–104.

Carnegie, Allison, and Austin Carson. 2018. "The Spotlight's Harsh Glare: Rethinking Publicity and International Order." *International Organization* 72(3): 627–57.

Carson, Thomas. 2010. *Lying and Deception*. Oxford: Oxford University Press.

Cauley, Leslie. 2006. "NSA Has Massive Database of Americans' Phone Calls." *USA Today*. May 11, 2006, http://usatoday30.usatoday.com/news/washington/2006-05-10-nsa_x.htm.

Chase, Jefferson. 2016. "Germany Reforms Its Main Intelligence Service." *Deutsche Welle*. October 21, 2016, www.dw.com/en/germany-reforms-its-main-intelligence-service/a-36109764.

Chase, Jefferson. 2017. "Merkel Testifies on NSA Spying Affair." *Deutsche Welle*. February 16, 2017, www.dw.com/en/merkel-testifies-on-nsa-spying-affair/a-37576690.

Cook, Karen. 2001. *Trust in Society*. New York: Russell Sage Foundation.

Cook, Karen, Russell Hardin, and Margaret Levi. 2005. *Cooperation Without Trust?* New York: Russell Sage Foundation.

Dahl, Robert. 1971. *Polyarchy: Participation and Opposition*. New Haven: Yale University Press.

Deutscher Bundestag. 2016. "Plenarprotokoll 18/184," https://dipbt.bundestag.de/doc/btp/18/18184.pdf.

Deutsche Welle. 2016. "Parliamentary Report Finds Spying by BND on EU and NATO Governments until 2013." *Deutsche Welle.* July 11, 2016, www.dw.com/en/parliamentary-report-finds-spying-by-bnd-on-eu-and-nato-governments-until-2013/a-19393213.

Deutsche Welle. 2017a. "NSA Spying Scandal Committee Presents Controversial Final Report." *Deutsche Welle*. June 28, 2017, www.dw.com/en/nsa-spying-scandal-committee-presents-controversial-final-report/a-39453668.

Deutsche Welle. 2017b. "German Intelligence 'Spied on White House.'" *Deutsche Welle*. June 22, 2017, www.dw.com/en/german-intelligence-spied-on-white-house/a-39365418.

The Editorial Board. 2015. "Mass Surveillance Isn't the Answer to Fighting Terrorism." *The New York Times*. November 17, 2015, www.nytimes.com/2015/11/18/opinion/mass-surveillance-isnt-the-answer-to-fighting-terrorism.html?_r=0.

Fehrler, Sebastian, and Niall Hughes. 2018. "How Transparency Kills Information Aggregation: Theory and Experiment." *American Economic Journal: Microeconomics* 10(1): 181–209.

Fenster, Mark. 2006. "The Opacity of Transparency." *Iowa Law Review* 91: 885–949, http://scholarship.law.ufl.edu/facultypub/46.

Fischer, Mia. 2019. *Terrorizing Gender: Transgender Visibility and the Surveillance Practices of the U.S. Security State*. Lincoln: University of Nebraska Press.

Fung, Archon. 2013. "Infotopia: Unleashing the Democratic Power of Transparency." *Politics & Society* 41(2): 183–212.

Gallagher, Ryan. 2015. "Profiled: From Radio to Porn, British Spies Track Web Users' Online Identities." *The Intercept*. September 25, 2015, https://theintercept.com/2015/09/25/gchq-radio-porn-spies-track-web-users-online-identities/.

Greenwald, Glenn. 2013. "Edward Snowden: NSA Whistleblower Answers Reader Questions." *The Guardian*. June 17, 2013, www.theguardian.com/world/2013/jun/17/edward-snowden-nsa-files-whistleblower.

Griffin, Andrew. 2015. "UK Government Plan to Ban WhatsApp Dropped, as Theresa May Abandons Many of Proposed New Powers for Spies." *The Independent*. November 1, 2015, www.independent.co.uk/life-style/gadgets-and-tech/news/uk-government-plan-to-ban-whatsapp-dropped-as-theresa-may-abandons-many-of-proposed-new-powers-for-a6716756.html.

Guariglia, Matthew. 2019. "Don't Renew Section 215 Indefinitely." *Electronic Frontier Foundation*. August 20, 2019, www.eff.org/de/deeplinks/2019/08/eff-says-no-trump-administrations-push-renew-section-215-indefinitely.

Guttman, Amy, and Dennis Thompson. 1996. *Democracy and Disagreement*. Cambridge: Harvard University Press.

Habermas, Jürgen. 1991. *The Structural Transformation of the Public Sphere*. Cambridge: MIT Press.

Hardin, Russell. 2002a. *Trust and Trustworthiness*. New York: Russell Sage.

Hardin, Russell. 2002b. "Liberal Distrust." *European Review* 10(1): 73–89.

Hintz, Arne, and Ian Brown. 2017. "Enabling Digital Citizenship? The Reshaping of Surveillance Policy After Snowden," *International Journal of Communication* 11: 782–801.

Hollyer, James, Peter B. Rosendorff, and James Vreeland. 2011. "Democracy and Transparency." *The Journal of Politics* 73(4): 1191–205.

Hood, Christopher. 2006. "Transparency in Historical Perspective." In *Transparency: The Key to Better Governance?*, edited by Christopher Hood and David Heald, 3–23. Oxford: Oxford University Press.

Investigatory Powers Act. 2016. www.legislation.gov.uk/ukpga/2016/25/contents/enacted.

Knigge, Michael. 2013. "NSA Surveillance Eroded Transatlantic Trust." *Deutsche Welle*. December 27, 2013, www.dw.com/en/nsa-surveillance-eroded-transatlantic-trust/a-17311216.

Koivisto, Ida. 2019. "Towards Critical Transparency Studies." *Res Publica* 25(3): 439–43.

Kydd, Andrew. 2000. *Trust and Mistrust in International Relations*. Princeton: Princeton University Press.

Lester, Genevieve. 2015. *When Should State Secrets Stay Secret?* Cambridge: Cambridge University Press.

Levy, Gilat. 2004. "Anti-Herding and Strategic Consultation." *European Economic Review* 48: 503–25.

Levy, Gilat. 2007. "Decision Making in Committees: Transparency, Reputation, and Voting Rules." *American Economic Review* 97: 150–68.

Loftus, Bethan. 2019. "Normalizing Covert Surveillance: The Subterranean World of Policing." *British Journal of Sociology* 70(5): 2079–91.

MacAskill, Ewen. 2016. "'Extreme Surveillance' Becomes UK Law with Barely a Whisper." *The Guardian*. November 19, 2016, www.theguardian.com/world/2016/nov/19/extreme-surveillance-becomes-uk-law-with-barely-a-whimper.

March, James, and Johan Olsen. 2011. "The Logic of Appropriateness." In *The Oxford Handbook of Political Science*, edited by Robert E. Goodin: 1–22. Oxford: Oxford University Press.

McCarthy, Daniel, and Matthew Fluck. 2017. "The Concept of Transparency in International Relations: Towards a Critical Approach." *European Journal of International Relations* 23(2): 416–40.

Meijer, Albert. 2014. "Transparency." In *The Oxford Handbook of Public Accountability*, edited by Mark Bovins, Robert E. Goodin, and Thomas Schillemans, 1–20. Oxford: Oxford University Press.

Meister, Andre. 2015. "Interne E-Mail: BND und Deutsche Telekom haben auch Österreich, Tschechien und Luxemburg abgehört (Update)." *Netzpolitik.org*. May 15, 2015, https://netzpolitik.org/2015/interne-e-mail-bnd-und-deutsche-telekom-haben-auch-oesterreich-tschechien-und-luxemburg-abgehoert/.

Meister, Andre. 2016a. "Secret Report: German Federal Intelligence Service BND Violates Laws and Constitution by the Dozen." *Netzpolitik.org*. September 2, 2016, https://netzpolitik.org/2016/secret-report-german-federal-intelligence-service-bnd-violates-laws-by-the-dozen/.

Meister, Andre. 2016b. "Das neue BND-Gesetz: Alles, was der BND macht, wird einfach legalisiert. Und sogar noch ausgeweitet." *Netzpolitik.org*. June 30, 2016, https://netzpolitik.org/2016/das-neue-bnd-gesetz-alles-was-der-bnd-macht-wird-einfach-legalisiert-und-sogar-noch-ausgeweitet/.

Nakashima, Ellen. 2019. "Repeated Mistakes in Phone Record Collection Led NSA to Shutter Controversial Program." *The Washington Post*. June 25, 2019, www.washingtonpost.com/world/national-security/repeated-mistakes-in-phone-record-collection-led-nsa-to-shutter-controversial-program/2019/06/25/f256ba6c-93ca-11e9-b570-6416efdc0803_story.html.

Obama, Barack. 2013. "Transcript: Obama's Remarks on NSA Controversy." *Wall Street Journal*. June 7, 2013, https://blogs.wsj.com/washwire/2013/06/07/transcript-what-obama-said-on-nsa-controversy/.

Obama, Barack. 2015. "Statement by the President on the USA FREEDOM Act." *The White House*. June 2, 2015, https://obamawhitehouse.archives.gov/the-press-office/2015/06/02/statement-president-usa-freedom-act.

Office of the Director of National Intelligence. April 2018. "Statistical Transparency Report Regarding Use of National Security Authorities Calendar Year 2017." www.dni.gov/files/documents/icotr/2018-ASTR----CY2017----FINAL-for-Release-5.4.18.pdf.

O'Neill, Onora. 2002. *A Question of Trust: The BBC Reith Lectures 2002*. Cambridge: Cambridge University Press.

Perraudin, Frances. 2019. "Liberty Loses High Court Challenge to Snooper's Charter." *The Guardian*. July 29, 2019, www.theguardian.com/law/2019/jul/29/liberty-loses-high-court-challenge-to-snoopers-charter.

Peters, Anne. 2013. "Towards Transparency as a Global Norm." In *Transparency in International Law*, edited by Andrea Bianchi and Anne Peters: 534–607. Cambridge: Cambridge University Press.

Pozen, David. 2020. "Seeing Transparency More Clearly." *Public Administration Review* 80(2): 326–31.

Pozen, David, and Michael Schudson. 2018. "Introduction." In *Troubling Transparency: The History and Future of Freedom of Information*, edited by David Pozen and Michael Schudson: 1–10. New York: Columbia University Press.

Prat, Andrea. 2005. "The Wrong Kind of Transparency." *American Economic Review* 95: 862–77.

Priest, Dana, and William Arkin. 2011. *Top Secret America: The Rise of the New American Security State*. New York: Little, Brown, and Company.

Rathbun, Brian. 2012. *Trust in International Cooperation*. Cambridge: Cambridge University Press.

Rawls, John. 1971. *A Theory of Justice*. Cambridge: Harvard University Press.

Rawls, John. 1993. *Political Liberalism*. New York: Columbia University Press.

Riechmann, Deb. 2018. "Cost of Snowden Leak Still Mounting 5 Years Later." *Associated Press*. June 4, 2018, https://apnews.com/797f390ee28b4bfbb0e1b13cfedf0593/Costs-of-Snowden-leak-still-mounting-5-years-later.

Risen, James, and Eric Lichtblau. 2005. "Bush Lets US Spy on Callers Without Courts." *The New York Times*. December 16, 2005, www.nytimes.com/2005/12/16/politics/16program.html?pagewanted=all.

Savage, Charlie. 2019. "Trump Administration Asks Congress to Reauthorize N.S.A.'s Deactivated Call Records Program." *The New York Times*. August 15, 2019, www.nytimes.com/2019/08/15/us/politics/trump-nsa-call-records-program.html.

Schneier, Bruce. 2013. "The Only Way to Restore Trust in the NSA." *The Atlantic*. September 4, 2013, www.schneier.com/essays/archives/2013/09/the_only_way_to_rest.html.

Schneier, Bruce. 2015. *Data and Goliath*. New York: Goliath.

Snowden, Edward. 2019. *Permanent Record*. New York: Macmillan Publishers.

Spiegel International. 2013a. "Merkel Comments on Spying Allegations." *Spiegel International*. October 24, 2013, www.spiegel.de/international/germany/merkel-comments-on-allegations-the-us-spied-on-her-cell-phone-a-929870.html.

Spiegel International. 2013b. "German Trust in United States Plummets." *Spiegel International*. November 8, 2013, www.spiegel.de/international/germany/nsa-spying-fallout-majority-of-germans-mistrust-united-states-a-932492.html.

Steinke, Ronen, and Reiko Pinkert. 2016. "Früherer BND-Chef kritisiert Kontrollsystem des deutschen Geheimdiensts." *Süddeutsche Zeitung*. September 22, 2016, www.sueddeutsche.de/politik/bundesnachrichtendienst-angriff-auf-die-lauscher-1.3174459.

Strobel, Warren, and Patricia Zengerle. 2015. "Obama's Signature on the Freedom Act Reverses Security Policy That's Been in Place since 9/11." *Business Insider*. June 2015, www.businessinsider.com/obamas-signature-on-the-freedom-act-reverses-security-policy-thats-been-in-place-since-911-2015-6.

Strobel, Warren, and Dustin Volz. 2019. "NSA Recommends Dropping Phone-Surveillance Program." *The Wall Street Journal*. April 24, 2019, www.wsj.com/articles/nsa-recommends-dropping-phone-surveillance-program-11556138247.

Tye, John Napier. 2014. "Meet Executive Order 12333: The Reagan Rule That Lets the NSA Spy on Americans." *The Washington Post*. July 18, 2014, www.washingtonpost.com/opinions/meet-executive-order-12333-the-reagan-rule-that-lets-the-nsa-spy-on-americans/2014/07/18/93d2ac22-0b93-11e4-b8e5-d0de80767fc2_story.html.

UK Home Office. 2017. *Investigatory Powers Act 2016 Consultation: Codes of Practice*, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/593725/IP_Act_codes_consultation_Feb2017_FINAL_WEB.pdf.

Uslaner, Eric M. 2002. *The Moral Foundations of Trust*. Cambridge: Cambridge University Press.

Chapter 3

A neo-republican critique of transparency

The chilling effects of publicizing power

Matthew Hall

Introduction

Democratic legitimacy of some kind has been produced by the transparency regulations brought in to oversee state surveillance in the wake of Edward Snowden's revelations about the secret and often unlawful practices of the NSA in the United States and GCHQ in the UK. Granting citizens knowledge over the scope of the rules governing surveillance, providing opportunities to identify abuses of power, and highlighting unfair or unjust uses of surveillance all go some way toward repairing what is considered to be one of the key harms produced by Edward Snowden's denunciation: a breach of the public's trust.

Viewing the harm of surveillance practices and transparency regulations instead through a perspective of *freedom as nondomination* – the neo-republican conception of freedom – however, illuminates something missing from the debate, which is this: making state surveillance practices more transparent may in fact compound surveillance's harmful effects on freedom. This is because publicizing surveillance power through transparency regulations amplifies surveillance's "chilling effects" on individuals already susceptible to being targeted by surveillance.

From the liberal perspective, publicizing surveillance's existence and its parameters makes it less harmful and more legitimate. This justification, however, fails to account for the arbitrary capacities inherent to surveillance and the effects this produces in those subject to it. My argument, instead, is that for it to be legitimate we would need to be able to contest *why* surveillance is conducted – explicitly, contesting the reasons behind the justifications for using surveillance over certain populations – not merely be informed about *how* surveillance is being conducted. Such an ability would also reduce the harmful effects produced by surveillance in certain populations, effects which are exacerbated by transparency as it is commonly understood.

The chapter will unfold as follows. I will firstly sketch what appears to be the primary justification for embedding practices of transparency into law – repairing public trust – focusing on the UK example by discussing the

DOI: 10.4324/9781003120827-5

Investigatory Powers Act (IPA) passed in 2016 by the British government. I will argue in the next section that the real problem concerning surveillance and transparency is the harm being done to our freedom as nondomination. This is the core of my argument, showing from a neo-republican perspective – a perspective within political theory which maintains that liberty is being free from domination – how surveillance and the transparency practices overseeing it impact our liberty as nondomination. I will diagnose existing proposals as instances of what I will call "hierarchical transparency," which a republican framework reveals to be inadequate. This will provide an analytical framework for demonstrating that the characteristic problem with the version of transparency on offer is not an issue of information or openness, but rather one of the power represented by surveillance practices. I will then distinguish between the "demos" and the "demoi" to show that "the public" from whom transparency practices are seeking approval is not the same constituency as the one being harmed by surveillance. Finally, I will offer a route out of these problems by offering my own conceptual innovation to the debate on transparency, the concept of "horizontal transparency" – an analytical framing and political proposal at the same time.

Snowden's "denunciation," transparency proposals, and public trust

While security services by their nature need to act secretly, the discovery that they were operating not only secretly but also in a way that appeared to be unrestrained, excessive, and unregulated, as the public learned from Edward Snowden's revelations (Bauman et al. 2014), brought the legitimacy of these types of surveillance practices into question. Characterizing the problem as a breach of trust between citizen and government led to a recognition that, to rebuild trust, maintain public confidence in institutions, and guarantee continued consent for security agencies, some kind of increased transparency was needed. Despite welcome democratic by-products of transparency proposals – such as norms of openness and procedures to limit the uses of surveillance, which can act as a benchmark and mechanism for holding abuses of power to account – foregrounding public trust as the justifying principle for surveillance regulations contributes to the hierarchical structure of transparency, which reproduces dominating effects on certain groups, as I will show.

In the aftermath of the Snowden revelations John Naughton, Emeritus Professor of The Public Understanding of Technology at the Open University and prominent journalist of technology and surveillance in the UK, was invited to contribute to the inquiry led by the UK's Intelligence and Security Committee of Parliament and stated:

> What it comes down to in the end is essentially a proposition "trust us," and in the past two or three years we have seen a number of startling

> examples of where serious British public institutions have demonstrated vividly that they are not worthy of trust.
>
> (Intelligence and Security Committee of Parliament 2015, 108)

The then Shadow Home Secretary, Yvette Cooper MP, argued that the work of the Agencies

> depends on the framework of consent, and that depends on there being a level of knowledge and understanding as well. I think if we try to keep everything behind closed doors, the danger is that we will undermine the trust that we need for the Agencies to be able to do their work.
>
> (ibid., 107)

The report into the inquiry concluded that "the Government acknowledged the requirement for greater transparency and openness … placed great value in public confidence, recognising that without the public's support they cannot fulfil their functions" (ibid., 107).

While increased clarity with which to restore public confidence was deemed important, the fact that this is inherently partial was concurrently recognized, with the report stating that

> [i]t could also be argued that it may be beneficial for adversaries to be "kept guessing" about the range and scale of the Agencies' capabilities: terrorists' behaviour may be constrained if they believe that the Agencies have more access than they do.
>
> (ibid., 108)

This demonstrates a recognition that unclear yet present surveillance has the power to cause effects in subjects whether they are under surveillance or whether they are not. When those subjects are deemed to be "criminal," this is classed as deterrence; "chilling" begins when lawful behavior is affected (Stoycheff et al. 2019). However, the line between what is deemed to be "criminal" by the security services, and what is not, and therefore who as a result is considered to be "deterred" and who is "chilled" cannot be so clearly drawn.

The assumption underpinning transparency practices and regulations is that citizens now know what the security agencies are doing (to a certain extent), know that surveillance and data collection are regulated, and know that legally underpinned guidance with penalties is attached to the use of citizens' data. Citizens can therefore trust the surveillance practices more fully, because we can trust that surveillance is being conducted in a way that is clearly defined for reasons we, the public, find acceptable.

What the republican perspective brings to light, however, is that greater trust does not necessarily equal greater democratic legitimacy. Social trust is something like a recognition of vulnerability that is accepted on the basis of

assumed good faith on the part of the other party. Placing such good faith in a relationship implies we believe that the other party will be "trustworthy" toward us (Hardin 2006). For authorities, trust has been described as "the invisible institution" that grants legitimacy to other institutions and government actions. Rebuilding trust is, in a sense, a way to rebuild the legitimacy of institutions that may have lost it (Rosanvallon 2008). Trust also has a relationship to risk. Trust anticipates and has expectations of the future. Risk is wary of it and seeks to reduce probabilities that the future will not be like we do not want it to be. Transparency, in an important sense, is the act of making the practices and operations of power visible and reducing an aspect of *unknowability*, thus inviting those subject to state power to trust it on the basis that the consequences of trusting it are now more knowable. In this way a relationship between transparency and risk is apparent, and reducing a perceived risk that institutions will behave badly increases public trust in, and hence the democratic legitimacy of, those institutions.

Yet, *distrust*, rather than trust, is in fact a vital component of maintaining *liberty* in democracies. Surveillance itself as a concept was not always understood as something that authorities and organizations did to citizens and individuals, but rather, surveillance, invigilation, and denunciation are historical methods for citizens to "oversee democracy." Benjamin Constant, a republican thinker, spoke in 1819 of conducting "surveillance in hatred" when asserting that "[e]very [good] constitution is an act of distrust" (Rosanvallon 2008, 7), grounding the principle of liberty in the reality that power needs invigilating because office holders cannot be trusted with that power, putting our liberty is at risk.

Desirable political arrangements from a neo-republican perspective are not to ensure that goodwill and good faith flourish in order to buttress social trust in institutions. Rather, the motivation is to ensure that citizens and their liberty are *not* dependent on the goodwill and good faith of political actors and institutions. Being distrustful of the potential consequences of relying on another's power to treat you in the way you wish to be treated is healthy for democratic freedom. The key point for republicans is to *secure* against the possibility of interference by other actors, not trust that they will behave in good faith toward you and your interests. The desire is to have some kind of control and input so that your life is not subject to the whims of officials, authorities, or rules which you have no say over and no possibility to contest.

Of course, a complete lack of trust is dangerous for democracy as it erodes the preconditions for negotiating a shared life. The antivaccination movement, for example, tries to persuade parents to refuse inoculations for their children, premised on skepticism of authority figures such as doctors and medical professionals and denying the credibility of science. This type of distrust is unpolitical in the sense that it offers no shared grounds for cooperatively resolving such a conflict of competing beliefs. Republican distrust, on the other hand, can be characterized as a healthy guardedness against

political power and authority, not a distrust that seeks to eradicate all faith in an authority.

Rather than responding to the breach of trust by state surveillance agencies revealed by Edward Snowden by trying to rebuild faith and confidence that security agencies are now doing what it is we want them to – to mend the distrust – we can instead use this breach of trust to ask deeper questions about surveillance's effects on those subject to it. For example, we can ask questions about surveillance's purposes, to generate a healthy distrust of state surveillance activities with more depth and breadth. My contention is that, when interpreting the harm of both surveillance and transparency regulations through the concept of freedom as nondomination, *embedding distrust* toward power in a politically constructive way like this seems a more realistic approach.

In order to make this argument, it is first necessary to explain the concept of freedom as nondomination and how we can use it to understand some of the harms of mass surveillance which the mainstream debate occludes.

Surveillance and freedom as nondomination

Freedom as nondomination differs conceptually from negative liberty in a number of important ways. The conception of negative liberty tells us we are free to the extent that we are not interfered with by humanly imposed external obstacles to our choices, classically demonstrated through laws or physical coercion. For republicans, on the other hand, it matters not only whether we are interfered with in this way but also whether we *could* be interfered with in some way, and whether the ability to shape or prevent that interference is beyond our control.

The classic example used in the literature to demonstrate this is the figure of the Roman slave who is relatively free on a day-to-day basis if they happen to have a benign master. In this context the slave may be able to freely socialize, visit the market, have free time throughout the day to be in town, and so on. However, the extent of their unfettered free choices comes at the grace and favor of their master. At any time, the ability to freely act can be removed if the master's mood changes, or if the master simply decides to restrict the slave's freedom in some way. This is a status of domination, no matter the amount of day-to-day negative liberty this slave enjoys. Not only is this a status of unfreedom, but it also engenders *freedom-reducing* behavioral and psychological impacts. Not knowing what behaviors may bring censure from the arbitrary power held over you, embodied in the master, or what the limits to your free behavior are, and having no control over those limits or when they could be imposed, induces effects such as self-censorship, toadying to authority, deference, second-guessing, anxiety, and fear (Skinner 1998). These effects then further limit the capacity to act freely within the space of the free choices that the dominated agent, represented in the figure of the slave, apparently enjoys.

This accurately characterizes part of the problem with mass state surveillance. The key factor for republicans is not whether surveillance constitutes a violation of privacy, nor whether it directly coerces your choices or is used by someone to directly interfere in your life in some way, although this is important. It is the very *possibility* that "arbitrary" interference in your life could occur, due to the gathering of information about you, that is the offense to liberty. In this scenario, all surveillance can be liberty-reducing in certain ways if we cannot know for sure what surveillance is conducted and why, have no meaningful control over the rules governing its practice now or in the future, have no meaningful control over what may be done with our data at some future point, and have no resources to contest surveillance practices.

Importantly, these types of "arbitrary" capacities to use our data or interfere in our choices may produce the freedom-reducing impacts documented in republican literature. These types of effects are demonstrated today in the "chilling effects" caused by surveillance (Stoycheff et al. 2019). Those who suspect they are subject to surveillance may engage in avoidance strategies designed to offset potential or perceived consequences.

In the context of post-Snowden security surveillance, the limits of free inquiry on the internet, for example, are unknown, but it *is* known that you are watched and monitored in some way. If it is unclear what types of communication are definitely allowed or disallowed, or what would be of interest or not of interest to authorities, but *it is known* that searching for these (currently unknowable or unclear) things online may produce a response from authorities of some kind, then this can be interpreted as a situation of domination parallel to that of the controlled Roman slave, and a range of chilling effects may be likely. Chilling effects are well documented, but republican conceptions of freedom as nondomination bring a hitherto missing dimension to explain *why* it is that our free activities are "chilled."

More broadly, if you know that there is the capacity to use the data you generate through your day-to-day internet activity and that that data can be used in ways that are opaque or unclear, it seems plausible that this may also cause some of the impacts observed by republicans when individuals are exposed to power of this type. The machine learning and algorithmically driven Big Data processes that are not directly interfering in your choices now but are building a potential capacity to interfere in your choices at some future point by accumulating knowledge about you represent another version of this type of potential harm. That surveillance and data are so often used for reasons other than those originally justified means that reassurances about data use remain unconvincing in the face of justified skepticism about the future reliability of those reassurances because of the lack of meaningful control over both why and how surveillance is deployed and data is collected. This type of power, for republicans, is considered to be arbitrary power.

Arbitrariness and chilling effects

I will now lay out precisely what arbitrariness means in this context, and why we have reason to be concerned that increases in transparency alone will be insufficient to curtail the arbitrary power that state surveillance represents. Arbitrary means something quite specific in political theory, beyond simply signifying random or unpredictable. Power can be procedurally arbitrary, meaning that the limits and aims of that power are not effectively stipulated, restrained, and fixed and are not made common knowledge to all parties potentially affected by that power (Lovett 2010). Substantive arbitrariness is a power that does not suitably track or, more specifically, is not "forced to track" the welfare and world-view of agents affected (Pettit 1997, Lovett 2010).

Procedural arbitrariness can be offset if sufficient democratic oversight is applied to the scope of the rules governing surveillance, and this is made common knowledge to all. The important aspect of state surveillance considered here, however, is that it produces *effects* distinct from the procedural basis of its justification. These "chilling effects" are produced regardless of whether democratic oversight is sufficiently applied. This demonstrates that a substantively arbitrary aspect to surveillance remains – that which potentially acts against the interests of the subject under surveillance – even if the rules governing it are common knowledge and clearly stipulated. Keeping in mind these distinctions between procedural and substantive arbitrariness is relevant for understanding the distinct approaches to transparency I will unpick below and the solutions I believe can be offered to offset the domination produced by them.

Firstly, a type of transparency that addresses the legal basis and scope of rules to which surveillance practices must adhere mirrors the version of securing "procedural non-domination" espoused by the republican theorist Frank Lovett in his influential book, *A General Theory of Domination and Justice* (2010). He claims that completely eradicating "procedural arbitrariness" – making the rules that govern power absolutely clear, stringently regulated, and common knowledge to all subject to that power – eliminates or radically reduces domination, diminishing uncertainty and other freedom-reducing impacts (Lovett 2010). In such a scenario, he claims, individuals with full and detailed knowledge of the rules of power could then "plan around" those rules and navigate an authority with power over them, because they now know what precisely is proscribed, and what is not. This, it is claimed, increases freedom of the individual by granting them the capacity to avoid knowable consequences (ibid.). This type of procedural nonarbitrariness requires the rules restraining that power to be effective, external, and common knowledge.

Criticisms of this approach have noted a problem, however. This type of procedural transparency could mean that a fully rationalized and well-publicized system of *oppressive surveillance* could, in principle, be acceptable

and nonoffending to freedom. An example used to make this point is the "pass laws" that existed in apartheid-era South Africa. There was a well-defined and strict monitoring system that dictated where black citizens could or could not go at certain times of day. Procedural nonarbitrariness, or procedural transparency, would mean that individuals in this scenario are *not* dominated. Knowing precisely what is allowed, by whom and at what times, eliminates uncertainty and unknowability. However, publicizing the rules of power clearly, making them common knowledge to all, does not in and of itself reduce the harm of that power, simply because its operation becomes transparent and clearly defined. Lovett swallows these criticisms, asserting instead that not everything that is bad about power means that it is dominating. The situation in apartheid-era South Africa could be described as unjust and oppressive, but that does not mean it is dominating in the republican framework he is offering, he claims. For my case, while a clear distinction can be drawn between the oppressive enforcement of rules in apartheid-era South Africa and state surveillance of citizens in liberal democracies, the same procedural issue is relevant.

In the example of internet activity, if it is clear and transparent that very specific and perhaps illegal internet activity would be monitored by security agencies, such as activities for aiding and abetting terrorism, and security agencies were strictly limited to that task alone, then this would seem to produce more areas of activity in which we could operate free from uncertainty, reducing domination and its freedom-limiting effects.

Since the time of the Snowden revelations, and the resulting legal oversight and transparency, the chilling effects have in fact expanded, however. Jon Penney has studied search traffic to what he terms "privacy sensitive" Wikipedia articles, and he found that they experienced statistically significant declines. These declines were not only apparent in the immediate aftermath of the Snowden revelations in 2013, but also demonstrated a downward trend over the long term, up to and including the same year that the IPA was passed into law, 2016 (Penney 2016). Longer-term trends will be interesting to study, but the processes since the Snowden revelations – public awareness, consultation on security activities, and, finally, legally embedded transparency practices – have evidentially generated further chilling-type effects.

Paradoxically, then, Snowden's denunciation has in fact reduced the liberty of citizens in an important way. Prior to Snowden's revelations and the increased transparency they created, citizens at large were exposed to arbitrary power but without their knowledge. This means that "free" action, such as searching at will for privacy-sensitive articles online, was less hindered than it is now. Such activity was conducted without the clear knowledge that state agencies were gathering and collecting information on what one was searching for – knowledge that now exists. To use the omnipotence metaphor, to a certain extent the public was in the panopticon prior to Snowden's denunciation but was not aware that the guard tower watching over them was a guard tower

at all. Those subject to state surveillance without their knowledge prior to the Snowden revelations would not have felt as compelled to limit their own freedom of choice, as they had less knowledge of the capacity of the state to watch over them.

This is a status recognizable to republicans, and even with the apparently increased freedom to act and make choices that comes with the ignorance of a power watching you, you cannot be considered free under the conception of freedom as nondomination. This situation is what Philip Pettit calls "alien control" (Pettit 2008). Alien control is the condition in which you are exposed to a power with an arbitrary capacity to interfere in your life, but you are unaware of that capacity. As such, you operate as if you are not being watched or controlled. Limits to your free action, based on the preferences that a power has over what you choose to do, mean that you are unfree, however. In many ways alien control is more conducive to negative liberty, as described, insofar as your liberty is not limited by your knowledge of any power with an arbitrary capacity to interfere in your life. Chilling and self-censorship are absent. However, unknown to you, there are still limits to your choices, the boundaries of which you may one day bump up against, producing consequences from the surveilling power of which, until that point, you were unaware. With security surveillance in the shadows, unconstrained and unregulated, citizens at large were previously dominated in this way because of these unknown yet present consequences attached to certain behaviors and choices, yet they more "freely" made their choices about how to behave under the surveillance of which they were unaware.

Bringing state surveillance practices into the light, then, through surveillance practices that are now more publicized, can produce *more* chilling effects. Now enlightened to the knowledge that you are exposed to a power with an arbitrary capacity to interfere in your life in some way, avoidance strategies, self-censorship, and second-guessing pertain.

Hierarchical transparency

The problem with this type of transparency offered in Western liberal democracies is that it is *hierarchical transparency*. By this I mean, firstly, that the imbalance of power represented by surveillance is made clear to those subject to it through practices and processes of transparency, producing the chilling effects discussed above, and secondly, what is made knowable to the public, or which rules are given clarity and why surveillance is used, and over whom, is still decided by the surveilling power, not those subject to it.

The amplification of chilling effects produced by transparency practices can be explained if we consider these practices to be only "partial transparency." It may be that it is still not quite clear enough to the public, activists, and journalists what definitely is and what definitely is not allowed. What is "criminal," what is "extremism," what is "radicalism," who are "enemies,"

and what is considered a "threat to the state" by security agencies all remain ambiguous. Is it *really* true that a journalist's sources will not be tracked down in some way if they release sensitive information? Is the line between what is considered "sensitive" and what is a "threat to state security" really clear? Are political organizations, curious citizens, journalists, and certain minority groups susceptible to state surveillance *really* clear about what may be of interest to state agencies that may produce unwelcome attention for those groups? It seems that *publicizing* the scope of the rules by which the public are being monitored on a mass scale, for reasons now apparently clear but importantly open to interpretation, provides only enough knowledge to generate uncertainty among those who feel they may be subject to surveillance. Becoming aware of a power held over you, but without a full knowledge and understanding of its operation and the consequences for certain types of your own behavior, is to realize you live in a status of domination. Procedural transparency of this type cannot completely eliminate the uncertainty associated with surveillance practices that produce chilling effects.

Of course, total transparency cannot eliminate uncertainty either. If *everything* state security agencies did could, in principle, be made public, it might well encourage the opposite of what is sought by calls for transparency. For state surveillance agencies to remain effective, they would be compelled to engage in something like a massaging of the truth, deliberate ambiguity of surveillance aims, or bland descriptions of operations. These types of evasions or half-truths are the symptoms of a hierarchical transparency that must protect the operative capacities of whatever authority is being transparent (O'Neill 2002, 64).

Philip Pettit develops the conception of freedom as nondomination further in a way that is helpful for understanding hierarchical transparency. Pettit describes the difference between negative liberty on the one hand, and freedom as nondomination on the other, as the difference between freedom and free rein (Pettit 2014). When a horse is given free rein, the rider allows it to go where it wills. It may turn left, right, slow down, and speed up, apparently free as the reins hang loose. However, those reins are still held by a rider, and the reason the horse has free rein is not due to the horse's preference, but the preference of the rider. While running freely may *feel* like freedom, someone is still in the saddle. True freedom is not free rein, in which you have a wide range of choices to enact; true freedom is *unbridled freedom*, with no one in the saddle granting you license to have free rein (Pettit 2014).

To be free in this unbridled way we must be able to choose the options that we prefer, despite the preference of others over us. This has three component parts. Firstly, we can choose freely if we have the capacity to choose an option and choose it without the interference of others. Secondly, we must have the room and resources to choose what it is we *prefer to choose*, not just the choices available. For example, a prisoner cannot liberate herself by choosing not to want to walk in the park and therefore "choosing" to stay in

her cell. Altering your preferences to fit the options offered by others is no freedom. Finally, you must be able to be free to choose despite the preferences of others. For example, ingratiating yourself with a prison guard in order to be allowed license to walk in the park – even though this is *your* preference this time – is still no freedom because it depends on the will of another (Pettit 2014, 28–54).

This conception of freedom as nondomination, as may be clear by now, is constitutively linked to how nondomination is secured. In other words, in order to be free to choose a range of preferred options you must have the room and resources to *secure* that range of options for yourself. This requires the power to do so, despite the attitude of the more powerful toward you. In republican terms this is secured through "anti-powers": public laws, norms, and the capacities of citizens to participate in governing, and to contest, impede, and block arbitrary uses of political power in order to enforce those democratically determined laws and norms. This driving principle does not identify clear, unambiguous cases of freedom but rather offers a roadmap to liberate individuals from harmful forms of dependence on others, based on the security of norms, laws, and antipowers with which to defend their liberty.

In this context, then, hierarchical transparency, a process which sets the scope of the rules and the purposes behind those rules and then publicizes them, making them common knowledge to all subject to that power, *demonstrates* the limits of our freedom. Transparency regulations allow us to "liberate" ourselves by *choosing new options* on the basis of the newly available information. However, choosing new options because our preferred options may prove too risky (because we are not sure about what is surveilled and for what reason, or what may be done with our data) is no freedom at all, as we have just seen above. Unless we have the political resources to exercise choices beyond the preferences of the surveilling authorities, set out in the transparency regulations determining the scope of the rules, we remain dominated. Hierarchical transparency regulations simply set out more clearly the boundaries to the free choices we have; they set out the extent to which our free rein runs.

Defending the "demos," dominating the "demoi"

In response to my argument above, it might be objected that existing democratic procedures can counteract the dominating tendencies of publicized surveillance. If the *demos* is considered to fully participate in the rulemaking of the state, then the power represented by state surveillance counts as *authorized interference* and is therefore nondominating. If we can consider the UK as democratic to a certain extent, then this could be considered sufficient to prevent us from being dominated. The rules are governed by a recognizably democratic mechanism in this version, and it could be claimed that we have

sufficient rights to defend ourselves from undue intrusion by state surveillance authorities.

Surveillance scholars have long noted a particular problem with surveillance, however, one that is relevant for claims such as this: namely, the differential treatment under surveillance between individuals and groups, a tendency most famously espoused as "social sorting" (Lyon 2003). This problem reasserts itself in the question of who the demos is – to whom justifications about surveillance are given. Surveillance is engaged in sorting *within* the demos; it does not monitor and defend a homogenous demos in order to keep it free and safe from the private domination of *others*.

In doing so, state surveillance is in fact monitoring the *demoi.* The term "demoi" is used in other republican theories to discuss the delineation that can be drawn *within* political entities between different *peoples*. For example, the European Union is discussed in republican terms as a *demoi-cracy,* which is to say, different peoples engaged with one political authority in a way that grants that authority political legitimacy (Bellamy 2019). Applying this thinking to surveillance reveals the inherently differential nature of the effects produced by surveillance.

A relationship of power involving surveillance of a different type can demonstrate the problem that surveillance represents for the demoi. Consider the case of police body cameras, or "bodycams." The filming of encounters between police and citizens, it is claimed, increases trust in officers by making those encounters transparent and concomitantly produces up to 93% reductions in complaints about the police from the public (Ariel et al. 2016). The implication in transparency claims of this type is that either the dishonesty on behalf of some of "the public" is addressed – they now no longer make complaints they know are spurious – or that the police now behave in a manner more befitting their role, now that they know they are being monitored. However, what may look like a way of making the police more accountable doubles as a means to use surveillance over groups already subjected to more intensive policing and surveillance practices – those groups and classes in society likely to encounter the police.

This brings into question whether the declared purpose behind police bodycams – improving the accountability of the police – is the true motivation and outcome of this type of surveillance encounter. Transparency in this instance is not only for the population who are subject to more surveillance but is also used to build trust with a public not involved in the encounter but whose confidence is required to secure the trust that maintains the legitimacy of the police.

The questions here from a republican perspective would be: do the transparent practices now overseeing encounters between the public and police through police body cameras in fact represent domination of the individual being filmed? And is the reduced volume of complaints and contestation of police practices premised not on the rebuilding of trust and honesty, which

seems to underpin those claims, but rather a result of surveillance *producing* conforming behaviors among those subject to surveillance in those interactions, through domination, fear, self-censorship, and anxiety?[1]

Surveilling more of the *demoi* in this way does produce transparency, but not necessarily for "the public" (or demoi) upon which the police directs its surveillance cameras. Instead, encounters between the police and surveilled subjects are made transparent to another "public" not susceptible to the potential conformity produced by being under surveillance: the *demos* that is not involved in the encounter, but on whose trust the police rely.

Up until now I have offered a critique of the transparency of surveillance practices, showing how it compounds the core harm of surveillance, which I interpret as domination. In what follows I will return to questions of trust and liberty in order to develop my horizontal transparency proposals, which, while necessarily incomplete, are driven by a principle of constructive *mistrust* of the purposes of surveillance and the harmful effects it has on those it monitors.

Horizontal transparency

Horizontal transparency is a way of fleshing out what meaningful control might look like, which we could build toward in the present. My notion of horizontal transparency is premised on the reality of state surveillance and transparency argued for thus far, namely the fact that even democratically authorized surveillance with regimes of transparency and oversight dominate individuals in ways that are prima facie unjustifiable – as demonstrated by the chilling effects they produce. It is not sufficient to transparently expose the scope of rules governing surveillance practices; the justification of the purposes for which surveillance is used must be transparent as well, in order for them to be challenged.

To address this reality, constitutionally embedded *mechanisms of mistrust* can secure our liberty under surveillance (Rosanvallon 2008). In practice, this could mean an array of citizen invigilation mechanisms and organizational forms that act as "editorial" rights (Bellamy 2013) and "anti-powers" to impede power *that has already been democratically authorized.*

There are two aspects of state surveillance that can be impeded with invigilation mechanisms: the harmful effects of surveillance, even when democratically authorized – the "chilling effects" – and the purposes for which surveillance is conducted. Such an alternative framework of demands requires not just more regulatory proposals but normative resources with which those subject to the most intensive state surveillance practices can challenge the basis on which they are under surveillance and the chilling effects produced.

The key to horizontal transparency is a recognition that substantive inequalities produce differentiated harms under surveillance. This is demonstrated by the sociological and economical fact of the demoi. While equality as a

desirable end state is beyond the discussion held here, there are strategies we can discern from societies that were both chronically antiegalitarian yet profoundly pro-liberty, such as the Florentine republics in which republican political philosophy was born. If we accept that surveillance's character is to identify and distinguish between unequal sections of society (to sort them) we can draw on strategies that pull back the veil of formal equality to reveal the class structure of society to combat the sorting inherent in surveillance's logic.

Thanks to Snowden, an opportunity to challenge the imperatives by which mass state surveillance is driven presents itself. This goes significantly further than simply regulating and publicizing already existing surveillance practices. Snowden's denunciation could be considered a first step in an activity of democratic mistrust that could engineer a basis for holding security agencies and government institutions to account for the justifications they offer for putting certain groups and individuals under surveillance, not only their legal basis for doing so. Horizontal transparency not only *looks through* to the purpose of surveillance but also seeks to *see the effects* surveillance produces in the populations it monitors, even when democratically authorized.

The difference between democratic oversight that legitimizes surveillance practices (which may be harmful) and republican nondomination is the difference between "authorial" and "editorial" rulemaking (Bellamy 2013). This distinguishes my approach from participatory, deliberative, and liberal approaches. The capacity to impede and block political power that has been democratically authorized but turns out to be dominating (like state surveillance) is a prerequisite for freedom in the view I am articulating here: freedom as antipower, in Pettit's term (Pettit 1996). This constitutes a bottom-up, "monitorial" (Schudson 1999) and "contestatory" (Pettit 1999) approach, in order to challenge the legitimate limits of what can and should be watched, even if democratically authorized. Horizontal transparency, unlike hierarchical transparency, constitutes "editorial" rights over the political power that is expressed by surveillance, following its authorization, rather than "authorial" rights concerning its legal basis, no matter the harm it presents for certain groups and members. In manifestly and profoundly unequal societies, there needs to be a normative basis for contesting things that have passed through existing "democratic" procedures (even leaving aside the question of how "democratic" these are, given how many are excluded from the rulemaking procedures). This is the point of the "editorial" control requirement.

Transparency implies "looking through" or "seeing through." Making this line of sight nonhierarchical is to enable people to see through to *the purposes* behind the surveillance, and to *see clearly* the consequences and harmful effects that are produced. Doing this holds not only the rules and legal basis of surveillance to account – as is currently the case – but furthermore holds the purposes and effects of state security surveillance to account. This more widespread and comprehensive vision of surveillance – inward to its purposes, and outward to the chilling effects it produces – is the key to horizontal

transparency. Mass state surveillance would need to be not only transparent in its proclaimed aims but also transparent in the *effects* it produces in certain populations and activities, and in why those effects are produced.

What these types of proposals require, to widen lines of vision of political power and the antipowers to then contest political power, is not the separation of powers at an institutional level, as is common to liberal democracies, but the separation of *political power* at the ground level. Such an approach focused on ground-level political power accepts that enforcing formal equality in an environment of substantive inequalities does not reduce the harm generated by unequally applied surveillance. To both recognize the dominating impact of democratically authorized surveillance, while simultaneously being able to act against it, necessitates a series of antipowers; antipowers such as independently constituted invigilation task forces (Hoye and Monaghan 2018), community panels with political oversight of police practices, tribunals, and the right to block, impede, and challenge surveillance.

In the context of security surveillance specifically, avenues for citizen contestation into the actual categories, classifications, and descriptions of surveillance – of "radicals," "threats," and "extremists" – that surveillance's "sorting" is premised on, can provide horizontal transparency. The recent "Spycop" scandal in the UK, where mass police infiltration was revealed to be taking place into a huge array of peaceful, noncriminal political organizations and civil society groups (Woodman 2018), seems to demonstrate that the state security agencies and police's interpretation of what constitutes a "threat," what is "radical," "extreme," or "criminal," needs to be opened up to public debate, not left to the police and security services to define, classify, and then use to monitor those they deem fit that category.

Of course, democratic and liberal approaches could also reflect on the harm caused by surveillance practices and adjust accordingly. To promote republican freedom, however, it is necessary to equalize power imbalances among citizens in order to defend against dominating power. This requires the production of political arrangements to contest those surveillance practices and the antipowers necessary to defend oneself against surveillance.

Conclusion: freedom, self-government, and the eyeball test

The primary purpose of this chapter has been to argue that transparency practices may in fact produce new harms to the freedom of certain groups and individuals under surveillance, demonstrated by chilling effects and articulated through freedom as nondomination. I have also begun to make suggestions as to how this could be countered, with a new line of vision and contestation: horizontal transparency.

This is underpinned by a republican account of power and freedom, and one final crucial point to consider with horizontal transparency needs

reemphasizing. Being able to participate in the way described above, and enact antipowers successfully, is premised on having more or less equal power to do so, whereas those most susceptible to harm by surveillance are often precisely those with less societal and political power. Some type of political equality is a precondition for freedom from a republican perspective. While a full account of political equality is beyond the scope of this chapter, I will end by sketching what I take to be a key republican insight into what substantive, as opposed to merely formal, equality requires.

Social sorting points to the fact of a chronically unequal society being one reason why surveillance is necessary from the state's point of view. The "eyeball test," however, describes the basis of self-government as premised on equalizing power as far as is possible so that citizens can look one another and the government "in the eye" without deference, fear, or favor (Pettit 2012). Enacting horizontal transparency without first doing something about the power imbalances that produce much surveillance over certain individuals, groups, and communities in society in the first place would be insufficient.

To do so would require taking seriously the ability of those in the demoi subject to liberty-reducing surveillance and domination to defend themselves. And this requires the political capacities to normatively contest their condition. For example, opening up public contestation only to ask the question "who is it that ought to be watched by police body cameras and why?" may not provide the desired result. Would it be the case that "we," the public (the demos), would decide we are in fact happy with the people the police are currently monitoring, compounding the problem? In a society of unequal resources, classes, and groups, the logic of the state to categorize and monitor these groups – to sort them (Lyon 2003) – produces surveillance, even if it is to treat those groups in a formally equal way. Opening up participatory avenues to contest state surveillance needs to ensure that those who come forward to participate do not embed the problem being addressed; imbalances of power ricochet through institutional proposals designed to overcome imbalances of power.

To reduce domination by surveillance, actual economic and political power *external to* surveillance practices needs to be equalized to lessen the divisions between citizens that drive much surveillance and to grant those citizens who are subject to surveillance the political capacities necessary to challenge the justifications for the surveillance to which they are subjected. Such societal and historical realities are obviously beyond the reach of this conclusion, but they should not be beyond the considerations of how state surveillance and transparency are deployed, and the domination and chilling effects they produce.

What my argument does show, however, is that transparency practices as they are currently constituted – as hierarchical flows of information – exacerbate the chilling effects experienced by certain groups exposed to surveillance. To secure liberty under surveillance, meaningful participation in the

production of society's information, which produces the justifications for surveillance, is necessary. I have tried to show how the concept of horizontal transparency could contribute to this project.

Note

1 Rachel Hall promotes a similar idea in her excellent work on the "transparent traveler" (2015), in which those subject to procedures such as airport security are forced into certain types of docile and submissive behaviors as they are compelled to be transparent *for* security officials. The same type of coerced submissiveness could be said to be at play here. However, whereas in the case of the transparent traveler it is the subject being forced to perform an "aesthetics of transparency" *for* authority, here the issue is the effects produced in the subject by an authority itself performing transparency.

References

Ariel, Barak, Alex Sutherland, and Darren Henstock. 2016. "Contagious Accountability. A Global Multisite Randomized Controlled Trial on the Effect of Police Body-Worn Cameras on Citizens' Complaints Against the Police." *Criminal and Justice Behaviour* 44(2): 293–316.

Bauman, Zygmunt, Didier Bigo, Paul Esteves, Elspeth Guid, Vivienne Jabri, David Lyon, and Rob B. J. Walker. 2014. "After Snowden: Rethinking the Impact of Surveillance." *International Political Sociology* 8(2): 121–44.

Bellamy, Richard. 2013. "Rights, Republicanism and Democracy." In *Republican Democracy: Liberty, Law and Politics*, edited by Andreas Niederberger and Philipp Schink, 253–75. Edinburgh: Edinburgh University Press.

Bellamy, Richard. 2019. *A Republican Europe of States*. Cambridge: Cambridge University Press.

Hall, Rachel. 2015. *The Transparent Traveler: The Performance and Culture of Airport Security*. Durham, NC: Duke University Press.

Hardin, Russell. 2006. *Trust*. Cambridge: Polity Press.

Hoye, J. Matthew, and Jeffrey Monaghan. 2018. "Surveillance, Freedom and the Republic." *European Journal of Political Theory* 17(3): 343–63.

Intelligence and Security Committee of Parliament. 2015. *Privacy and Security: A Modern and Transparent Legal Framework*. 12 March 2015, HC 1075, House of Commons. London. United Kingdom.

Lovett, Frank. 2010. *A General Theory of Domination and Justice*. Oxford: Oxford University Press.

Lyon, David. 2003. *Surveillance as Social Sorting: Privacy, Risk, and Digital Discrimination*. Abingdon: Routledge.

O'Neill, Onora. 2002. *A Question of Trust*. Cambridge: Cambridge University Press.

Penney, Jonathon W. 2016. "Chilling Effects: Online Surveillance and Wikipedia Use." *Berkeley Technology Law Journal* 31(1): 117–82.

Pettit, Philip. 1996. "Freedom as Anti-Power." *Ethics* 106(3): 576–604.

Pettit, Philip. 1997. *Republicanism: A Theory of Freedom and Government*. Oxford: Clarendon Press.

Pettit, Philip. 1999. "Republican Freedom and Contestatory Democratization." In *Democracy's Value*, edited by Ian Shapiro and Casiano Hacker-Cordon, 163–90. Cambridge: Cambridge University Press.

Pettit, Philip. 2008. "Republican Liberty: Three Axioms, Four Theorems." In *Republicanism and Political Theory*, edited by Cecile Laborde and John Maynor, 102–30. Oxford: Blackwells.

Pettit, Philip. 2012. *On the People's Terms: A Republican Theory and Model of Democracy*. Cambridge: Cambridge University Press.

Pettit, Philip. 2014. *Just Freedom: A Moral Compass for a Complex World*. New York: Norton.

Rosanvallon, Pierre. 2008. *Counter Democracy: Politics in an Age of Distrust*. Cambridge: Cambridge University Press.

Schudson, Michael. 1999. *The Good Citizen: A History of American Civic Life*. New York: Harvard University Press.

Skinner, Quentin. 1998. *Liberty before Liberalism*. Cambridge: Cambridge University Press.

Stoycheff, Elizabeth, Juan Liu, Kai Xu, and Kunto Wibowo. 2019. "Privacy and the Panopticon: Online Mass Surveillance's Deterrence and Chilling Effects." *New Media & Society* 21(3): 602–19.

Woodman, Connor. 2018. "Spycops in Context: Counter-Subversion, Deep Dissent and the Logic of Political Policing." Centre for Crime and Justice Studies, www.crimeandjustice.org.uk/sites/crimeandjustice.org.uk/files/Spycops%20in%20context%20–%20counter-subversion%2C%20deep%20dissent%20and%20the%20logic%20of%20political%20policing.pdf.

Chapter 4

The dynamics of imposed transparency and its role in deep social conflicts

Shaul A. Duke

Introduction

The term "transparency" lives a double life. On the one hand, it has the clean-cut image of a universal standard of proper operation in a free society, an image that seems to be accepted by most; on the other hand, however, it has the rougher image of a power move that tries to expose its target to scrutiny and undermine some of its actions. In this chapter I differentiate between the two and analyze the dynamics of the much less studied "imposed transparency" strand. In particular, I analyze how transparency is imposed as a strategy in a preexisting social conflict characterized by a low level of trust between the relevant parties from the start. In such conflict situations, when the parties do not trust each other, transparency is almost always forced by one party on the other (via surveillance) and almost never willingly adopted by either party. I am interested in: the reasons why individuals/organizations turn to imposed transparency as a political strategy, the ways imposed transparency is carried out, the degree to which these targets tend to accept imposed transparency or resist/evade it, the dynamics that mutual attempts to impose transparency create, the role that power asymmetries have in such attempts, and the effectiveness of forcing transparency in order to achieve specific goals.

In this examination, I will first analyze some of the existing writing on transparency and chart some of its weaknesses as a social change tool. Next, I will turn to differentiate between voluntary universal transparency and imposed targeted transparency, and identify three defining features on which they diverge. I will then proceed to scrutinize the dynamics of imposed transparency as it pertains to two cases (designated A and B) within the Occupied Palestinian Territories (henceforth OPT): (A) the case of the large checkpoints ("terminals") operating within the West Bank to restrict Palestinians' movement and (B) the case of Israeli NGOs operating to safeguard Palestinians' human rights. Both cases will help clarify how and why imposed transparency is deployed, the reactions that such attempts provoke, and the end result with regard to political struggles, asymmetry, colonialism, democracy, operation with impunity, and human rights standards.

DOI: 10.4324/9781003120827-6

The transparency concept

The term transparency has become widespread both among scholars and laypeople around the world (Bertot et al. 2010; Bessire 2005). It is the solution suggested to a variety of social problems that usually revolve around lack of trust (e.g. Auger 2014; Jackson 2015; Kanagaretnam et al. 2010; Rawlins 2008; Schnackenberg and Tomlinson 2016). Transparency's popularity seems to echo a human fascination with "seeing through" opaque things, yet traversing from this alluring/aesthetic notion of transparency to its actual application in complex human reality is not an easy process, and indeed transparency as a solution to social problems has been found to be very problematic in a variety of fields (Bac 2001; Bannister and Connolly 2001; Bauhr and Grimes 2014; Bessire 2005; Brucato 2015; Drucker and Gumpert 2007; Grimmelikhuijsen 2010; Grimmelikhuijsen et al. 2013; Kolstad and Wiig 2009; O'Neill 2002; Schnorf et al. 2014).

Most of the scholastic attention to the concept of transparency is focused on its relation to trust and the building/sustaining of trust. What many studies on the relations between transparency and trust suggest is that, in a variety of settings, transparency does not increase trust and sometimes actually reduces it (Allen 2008; Grimmelikhuijsen 2010; Grimmelikhuijsen et al. 2013; Margetts 2011). Yet this research thread still assumes that trust is a desired social good of its own. But as pointed out by O'Neill, this is not necessarily the case; while we should trust some individuals/organizations on some issues, we should be highly skeptical toward others (O'Neill 2002). Moreover, when referring to nontrust positive effects of transparency (e.g. fighting corruption), there are scholars who point out that if the public does not have the willingness and the means to force social change, transparency in itself is ineffective (Kolstad and Wiig 2009; Lindstedt and Naurin 2010; Marsh 2011).

Feminist surveillance literature, for its part, places a strong emphasis on the differential ways in which making things transparent affects different people (Abu-Laban 2014; Dubrofsky and Magnet 2015; Hall 2017). Transparency technologies/practices that might be considered positive or neutral may be detrimental to certain groups, such as the way full-body scanners can be disturbing for transgender or disabled people, as well as for individuals from certain religions. Nevertheless, transparency still carries a positive connotation in our society and is still widely used.

Two types of transparency

Transparency can be categorized as either imposed or adopted. Imposing transparency on a person/organization usually entails some sort of surveillance (Brucato 2015); it requires monitoring the target to achieve disclosure that is not voluntary—monitoring to which the target has not agreed (e.g. public space CCTV). In these cases, transparency is dictated by others, and consent is neither sought nor received. Indeed, some scholars call this type of

imposed transparency "weaponized visibility" (e.g. Trottier et al. 2020; Young 2020). In our current social reality, some of these one-directional demands for transparency can be resisted, but many cannot.

The second category of transparency is that which people/organizations adopt willingly. Once a disclosure process is initiated, its adopters may be subject to new types of monitoring that can easily be perceived as surveillance. Workers who sign a consent form allowing their own electronic communications to be monitored are one such example of opening the door to their own surveillance. Not in every instance will such surveillance actually take place, but the potential is clearly there. We should note that consensual adoption of transparency does not necessarily mean it is adopted willingly. Demands to adopt transparency often involve a great degree of pressure, offering individuals or organizations deals they cannot realistically refuse. Indeed, the question of willingness to adopt transparency is tricky when transparency can expose one to scrutiny, criticism, and attack (Rawlins 2008). Once our words and/or actions become public record they can easily be misunderstood, misrepresented, or decontextualized (Bannister and Connolly 2011).

One way to mitigate some of the risks of disclosure is if the individual/organization that was made to be transparent controls the disclosed information. For instance, with regard to substance abuse monitoring, a worker may be asked to periodically sign a declaration as opposed to being subjected to urine testing. While in the former instance the individual controls the disclosure process, which allows her/him room to maneuver (e.g. by omitting information), in the latter it does not. This control in turn may reduce the risks resulting from exposure that transparency entails and may also create a mode of good faith between the disclosing and the disclosed parties. What is especially important in understanding the legitimacy of transparency is to know toward whom the transparency procedure is applied; that is, if it is applied universally or if it is targeted. When transparency is applied evenly to all, it is much more palatable. Being asked to start swiping your employee card when entering/exiting work may seem arbitrary if it only applies to some workers. Thus, universal application is another necessary element for voluntary transparency.

Conceptually, we are left with two archetypes of transparency: voluntary transparency and imposed transparency (see Table 4.1). While they both

Table 4.1 Two archetypes of transparency

	Voluntary	*Imposed*
Consent	Sought	Not sought
Disclosure	Self-disclosure	Outside monitoring
Application	Universal	Targeted

expose an individual/group/organization to scrutiny and criticism, one is adopted willingly on the basis of some sort of social agreement and trust, while the other is imposed in a unidirectional fashion, does not rely on its targets for disclosure, and may be applied selectively according to the interest of the imposing party. The fact that both are considered "transparency" seems to benefit those practicing imposed transparency, since it attaches the positive connotations of the voluntary transparency term to what they actually do, which is almost identical to surveillance. Last, it should be noted that these are two archetypes of transparency and that actual cases of transparency may shift from one category to another or be hybrid cases.

The dynamics of imposed transparency

Imposed transparency tends to appear in situations in which there is an existing conflict and low levels of trust between the parties. Given that transparency can expose one to criticism/attacks, in conflict situations voluntarism is low and self-disclosure is regarded as highly unreliable. In such settings, forcing transparency on the other side may be a powerful strategy to achieve a desired outcome that is at odds with the other party's wishes. In cases like these, transparency is used in a utilitarian and targeted way. For instance, in certain settings transparency may be forced on a political rival or a business competitor in order to weaken them and undermine their goals (Sperling 2011). As will be shown in the empirical section, this process of enlisting transparency for a strategic goal may be undertaken by a group/organization that may be committed to transparency (as a social value) but also may not.

Moreover, imposed transparency may be initiated not only by strong groups or organizations but also by weak ones (Koskela 2012; Mann 2013; Wilson 2012; Wilson and Serisier 2010). This may seem counterintuitive since unidirectional power moves are usually associated with powerful social forces, yet marginalized groups and the advocacy organizations that represent them may also enlist certain resources (such as the courts) in order to force transparency on the powerful. For example, a weak community may impose transparency on a wealthy chemical plant in order to disclose the suspected dumping of known pollutants.

It is precisely because imposed transparency may be the weapon of the weak as well as the strong that we can talk of the phenomenon of "cycles of imposed transparency"—that is, a dynamic in which two sides increasingly use transparency in order to combat each other. Imposed transparency, as it so closely relates to surveillance, adheres to surveillance's overall pattern of move and countermove (Wilson 2012; Wilson and Serisier 2010), of being contingent upon the actions of other players. In a dynamic where several players are influencing each other, an account must be given of how each move influences the subsequent one in a sequential fashion. Accepting the forced transparency is not the only possible reaction, and the targeted party

may resist or evade transparency. Thus, while a nontrivial part of the surveillance studies literature follows Foucault's (1991) panopticon reasoning and would expect these targeted parties to accept and internalize the imposed transparency, another part of the surveillance literature suggests resistance is the norm (e.g. Gilliom and Monahan 2012; Marx 2003). We thus might encounter a dynamic in which the panoptic gaze is not accepted but defied.

I will examine imposed transparency by focusing on the dynamics that emerge from the historical sequence that revolves around the restriction of Palestinian movement in the OPT and the defense of their human rights. My study is based on a qualitative analysis of both primary and secondary data, website content, reports and documents, and ten semi-structured interviews and correspondences with NGO activists/personnel working in the field of Palestinian human rights, some of whom have firsthand experience with new hi-tech terminals operating in the West Bank.

Imposed transparency in the OPT

Imposed transparency is at the heart of what has been occurring in the OPT since the beginning of the 2000s, and to a lesser degree since these territories were occupied in 1967. In line with what scholars who link surveillance with colonialism have found in other places/times (e.g. Monaghan 2013; Zureik 2011), contemporary OPT is also a locus for intense implementation of surveillance technologies on indigenous people. Israeli government agencies implement a deep-reaching surveillance of Palestinian movement and actions that is pervasive and affects virtually every Palestinian (Handel 2011; Handel and Dayan 2017; Lentin 2017; Zureik 2001, 2011, 2016). They frame transparency as being carried out in the name of security considerations. The high price that ordinary Palestinians have to pay in order to provide assurance that they do not pose a threat is framed as the collateral damage of past Palestinian terrorist acts, and thus as legitimate. Although this justification of the pervasive practice of surveillance is somewhat contested, the overwhelming majority of Jews in Israel agree with it and endorse it (Avni 2006; Kuntsman and Stein 2015).

This process of forced transparency, coupled with other processes that pertain to maintaining the military occupation of the West Bank and Gaza, entails the violation of Palestinians' human rights on a large scale. These consistent violations, in turn, have provoked the emergence of several dozen advocacy groups and NGOs, some Palestinian, some Israeli, and some international, focused on stopping the violations. These advocacy groups conduct "empowering surveillance" against Israeli government agencies (Duke 2019) and impose transparency on them in turn. Since they impose transparency for policies that are seen as legitimate by most of the Jewish population, these NGOs themselves come under attack, and the Israeli NGOs in particular are subject to imposed transparency from the state.

It is clear that trust between the parties is absent from the outset, and that it is not likely that these steps of forced transparency will produce trust. Instead, transparency is imposed in case A to produce security and control of movement, which are necessary to deepen and perpetuate the occupation, and in case B to protect Palestinian human rights and help end the occupation. This case study will be analyzed by examining the dynamics of the two sets of transparency cycles as a series of moves and countermoves.

Case study A: the dynamics around checkpoints in the West Bank

First move: deploying the checkpoints

In the early 2000s, and specifically after the second Intifada erupted in September 2000, Israel began establishing a new regime of checkpoints crisscrossing a large part of the West Bank (Handel 2011). These checkpoints were erected not only to monitor and control the entry of Palestinians into pre-1967-border Israel, but also in order to monitor/control the movement of Palestinians between Palestinian villages, towns, and cities within the West Bank. Both the army and the border police were put in charge of deploying and running these checkpoints, which placed young enlisted soldiers in charge of carrying out the actual monitoring of the Palestinian population. In accordance with the racist purpose of facilitating the occupation, Jews—both settlers in the OPT and nonsettlers—were exempt from inspection at these checkpoints and thus from any control of movement.

The checkpoints themselves have evolved significantly over the years. They began as no more than roadblocks ("a block, a few sand bags, with a soldier behind them," as described by Barag 2017) and grew into large-scale constructed open-air checkpoints, whose physical design serves the surveillance demands of Israeli security agencies and the desire to run the checkpoint in an orderly fashion. The checkpoints also reinforce the perception that all Palestinians pose a security threat (including to the checkpoint personnel) and create a number of human rights issues that derive from the problems that arise when masses of people are made to wait for a long time in order to pass. Beyond the checkpoints themselves, a variety of steps have been taken to prevent Palestinians from bypassing the checkpoints (Braverman 2012), such as the construction of the West Bank barrier and the establishment of a strict permit system.

Once the checkpoints had transformed into Israel's main surveillance and movement restriction tool in the OPT, they required the investment of a significant degree of resources for their operation. Beyond the capital drain of constructing and maintaining permanent checkpoints that "service" the entire West Bank Palestinian population, there was a need for trained personnel and for competent management that would operate these checkpoints

efficiently. The fact that these facilities enable unwanted control over a large ethnic/national group has made them a potential target for attack, which further increases their resource drain on state agencies. The well-documented chronic unwillingness of the Israeli government to allocate the required resources (State Comptroller of Israel 2011) has exacerbated the stress on the checkpoints, increased the crossing time, and produced further human rights violations.

From the perspective of ordinary Palestinians, avoiding the checkpoints is not motivated primarily by a desire to avoid the imposed transparency. It is more about preventing the significant time loss and discomfort that these checkpoints entail, and their tendency to arbitrarily prevent free movement. Waiting in long lines, sometimes for more than an hour or two, with other people who also want to make it through promptly, produces major discomfort, and sometimes even triggers pushing, fainting, and incidents of violence. Movement is denied for any number of reasons, most of them unknown to the person passing through until s/he is actually refused passage.[1] Beyond the "lawful reasons" (if we can call them that) for denying movement, the fact that the soldiers/border police tasked with running these checkpoints have little relevant training, are overworked, and work under harsh conditions, means that many denials are made for unlawful reasons or due to ignorance of the rules (Hallward 2008; Mansbach 2009). This adds still more arbitrariness to a process that is arbitrary to begin with.

Despite the fact that these checkpoints immediately became loci of massive human rights violations, and despite Israel's and Palestine's small size (which makes the checkpoints more accessible for observation), what went on in them remained largely unknown to both the Israeli public and the international community (Barag 2019). This opaqueness granted the Israeli security forces virtually free rein to operate the checkpoints as they pleased.

Second move: monitoring checkpoints by human rights NGOs

The reaction of human rights NGOs to the creation of this checkpoint regime was to impose transparency on the government agencies managing and operating it. These surveillance efforts in the name of Palestinian human rights were part of well-established practices of empowering surveillance whereby NGOs monitor Israeli agencies operating in the OPT (Duke 2019). These practices date back to the end of the 1980s and were spearheaded by Jewish–Israeli NGOs, which, due to their inclusion in the dominant community, were (and still are) in a special position to gain the cooperation of Israeli agencies.

With the new checkpoint regime in place, some existing NGOs turned their attention to these checkpoints, while in 2001 one new organization was created specifically with the purpose of monitoring them, appropriately named Machsom (checkpoint in Hebrew) Watch. This organization's activists (all volunteers) carry out monitoring at the checkpoints. This allows both

the unmediated observation of what goes on in the checkpoints in real time, and affords the opportunity to intervene in the actions of soldiers/officers operating the checkpoints in order to prevent human rights violations as they unfold (Hallward 2008; Kotef and Amir 2007; Mansbach 2007). Their constant presence at the varied West Bank checkpoints and their intense contact with officers in the Israeli army enabled Machsom Watch activists to pressure the army into making changes in both the checkpoints' procedures and their physical design (Barag 2017; Helman 2015; Hirschfield 2007; Kotef and Amir 2007; Mansbach 2007).

At its peak, Machsom Watch numbered hundreds of activists across Israel, distributed among several different geographical regions, with most of them engaged in checkpoint observation in the West Bank on a weekly basis (Bar 2017; Barag 2017; Braverman 2012; Hallward 2008; Mansbach 2007). This created a situation in which large checkpoints would be monitored at least once a day, while smaller checkpoints would be examined at least once a week. In this way they were able to put in place a mechanism of constant monitoring and intervention, and established themselves as the third major party to the interaction between Palestinians and Israeli security forces at these checkpoints.

Machsom Watch's primary focus on checkpoints and their unmediated contact in "the field" allowed them to gain a great deal of perspective, information, and know-how regarding these checkpoints, their effects on the Palestinians, the military rules that are supposed to govern them, and the de facto arbitrariness that actually governs them most of the time (Braverman 2012). Although the Watch members mostly lacked any identifying features, their constant presence was hard to miss, and it seems most checkpoint operators recognized them and saw them as something between a burden and a full-fledged enemy (Bar 2017; Kutz-Flamenbaum 2016). Machsom Watch's huge database of checkpoint reports is full of descriptions of confrontational encounters with checkpoint operators. The database is also indicative of the intensive contact such monitoring entails between the activists and the higher-ranking officers, who were routinely asked to intervene in either structural/procedural issues, or in individual cases, when common ground with the checkpoint soldier/officer could not be reached.

It is thus of no surprise that those operating the checkpoints tried to undermine the activists' monitoring in a variety of ways. For instance, they often told the activists to move to another spot, away from where the soldier/officer stood (Bar 2017; Kutz-Flamenbaum 2016). In extreme cases, they tried to declare the checkpoint and its surroundings "a closed military area" which, if accepted, would have required the activists to vacate the area and cease the monitoring. However, Machsom Watch activists fiercely resisted these latter practices by being well informed about what is required by law to declare a closed military zone, and by refusing to give merit to any verbal declaration that did not adhere to such requirements (Mansbach 2007, 2009). Still,

attempts to stop the monitoring of checkpoint operators most probably only increased the frustration of the soldiers/officers, whose transgressions continued to be monitored by a group of civilians and were sometimes reported to their superiors.

Third move: new hi-tech indoor checkpoints

The next move was made by the Israeli government, and specifically by the Israeli agencies managing and running the checkpoints, and it marked a radical change to a portion of the checkpoints—those that were in proximity to either the pre-1967 border or to the borders of Larger Jerusalem. These checkpoints were to become "terminals" resembling airports or "normal" land border crossings. Among other things, this shift would entail making these checkpoints more permanent structures, shifting their operation from being run by soldiers/officers to specialized civilian personnel, and replacing much of the close-proximity personal monitoring functions of the checkpoint with less-conspicuous surveillance technologies.

The new indoor checkpoints were part of a greater scheme that also included the construction of the Separation Wall, which circles the West Bank. This project, devised by the Israeli government around 2002–2003, would create a situation in which all Palestinian movement into pre-1967 Israel can only be done via the new indoor checkpoints (State Comptroller of Israel 2011). While in line with contemporary world trends to reduce uncontrolled movement of "undesirables" to a minimum and to privatize border work (Bigo 2006; Walsh 2010), Israel's approach also diverges from this trend in that this border work has not been made more mobile, more ad hoc, or less formalized like in other places (e.g. Andreas and Snyder 2000; Bigo and Guild 2005), but quite the reverse; it is much more permanent and formal than before (Braverman 2011).

The shift to indoor checkpoints took a long time to realize, was implemented unevenly among the different "terminals," and was riddled with errors. In some ways, this project is still ongoing since the full hi-tech vision of a ship-shape terminal was realized only in two "model" crossings (Qalandiya and Checkpoint 300), while the remaining crossings still have a way to go. What became common to all the terminals was the much greater transparency they enforced on Palestinians passing through them. The gradual introduction of database links, magnetic ID cards, and biometrics (e.g. fingerprint reading) allows for much closer monitoring of each Palestinian passing through (Kotef and Amir 2007). Of course, greater transparency spells out greater and more sophisticated movement restrictions.

With regard to the issue of checkpoint operation transparency, what was most critical in this transformation was the shift indoors (Braverman 2012; Mansbach 2009). This meant that the checkpoint would no longer be open to the NGOs' inspection, direct monitoring, and intervention (Afek 2019;

Konforty 2017; Kotef and Amir 2007). While at the open-air checkpoints activists could stand outside the fences and still monitor and intervene, the walls of the indoor checkpoints prevent such monitoring. In addition, in the new terminals Palestinians passing through the checkpoint would no longer be able to plea with the checkpoint operators, to reason with them, or to alert them of any problem they encountered, because the operators are mostly hidden behind walls, heavy-duty glass windows, and CCTV (Braverman 2012; Kotef and Amir 2007; Mansbach 2009; Rijke and Minca 2019). In this new system, the limited transparency that was previously forced on the operators of the checkpoint is now largely lost.

Was this an intended consequence or maybe a coincidence or an oversight on the part of the decision makers? There are several indications that this was a sought-after consequence, even if not an explicit one. First, these terminals were developed from scratch. They were not just another patch on the existing structures, such as the many upgrades that open-air checkpoints underwent, but an entirely new structure designed purposely several years after the checkpoint regime was put in place. Thus, these structures were deliberately designed to lack any outward-facing windows and avoided any inclusion of a physical or virtual viewing gallery, which would have allowed human rights activists and reporters to view the checkpoint processes. Similarly, the lack of any opportunity for feedback from the Palestinians crossing the checkpoint was a desired consequence. While the operators use the specially installed loudspeakers to communicate with the Palestinians, there is "no technology installed to hear possible responses, which explains why Palestinians have to shout or communicate via signs" (Rijke and Minca 2019).

This intentional lack of transparency and one-sidedness of interaction is further reinforced by the reasons given for this transition to indoor terminals. While there are several motivations for this transformation, what consistently appeared at the top of the list of explicit goals was "reducing friction" (Davidov 2014; State Comptroller of Israel 2011). That is, reducing instances in which the operators come into direct contact with the Palestinian population and, I would add, with the human rights activists who monitor and intervene on their behalf. Indeed, as discussed above, both types of interaction tend to produce conflicts and are perceived as a burden by the checkpoint operators and to some extent by the higher army ranks. Therefore, the new type of checkpoint tries to achieve architecturally what in the past soldiers and field commanders tried to achieve unlawfully—to close off the checkpoints to any form of outside monitoring.

This closing off also suited the interests of those higher up the pecking order. Both the security forces' top ranks and the Israeli political leadership of the last decade and a half seem to be invested in upholding the checkpoint regime, as it is highly consensual among the Jewish population. Naturally, bad press, locally and internationally, runs the risk of putting pressure on the Israeli government and ultimately endangering the legitimacy of the

checkpoint regime (Davidov 2014). Hiding what is taking place in these checkpoints from sight and oversight thus serves to avoid negative reactions (Barag 2019; Handel and Dayan 2017). A good indication that this is in fact the thinking is that the two model terminals—the ones that actually resemble an airport—are the ones most exposed to the international community (Hass 2019).

Did this shift to terminals achieve the goals of reducing the operators' transparency? It seems it mostly did. To this day, in all but the two model indoor checkpoints Machsom Watch activists are not allowed to monitor, not even by passing through them as a Palestinian crosser does, while the two terminals that do allow activists to enter are limited to this single crossing-through procedure. Sporadic supervised visits to the checkpoints were organized following requests from activists/reporters, but it seems each time they occurred, the checkpoint was closed off for crossing (Afek 2019; Maor 2019), which meant the visitors did not witness real-world conditions. Machsom Watch activists did not cease their monitoring activities because of this shift, but have had to rely on the feedback of Palestinians exiting the checkpoints in order to understand what is going on within them. They still inspect each checkpoint's facilities and surroundings (Afek 2019; Bar 2019; Barag 2019), yet the bulk of their monitoring and their intervention disappeared with the move indoors.

Case study B: the dynamics around Palestinian human rights NGOs[2]

First move: monitoring human rights violations

As mentioned above, Israeli NGOs have been monitoring Israeli agencies and settler actions for human rights violations for almost three decades. There are currently at least three dozen of these monitoring bodies that engage in some sort of empowering surveillance (Aggestam and Strömbom 2013; Avni 2006; Duke 2019; Fleischmann 2016; Helman 2015; Miretski and Bachmann 2014). That is, they are imposing transparency on government agencies in the name of universal human rights norms. The monitoring is done by a variety of methods such as direct observation, testimony collection, evidence collection, taking affidavits, gathering pictures and video data, making judicial inquiries, making formal and informal information requests, and more.

The collected data is used to monitor violations of human rights by a variety of government agencies and by right-wing social groups that either operate in the OPT or have a role in perpetuating the occupation. NGO proficiency in collecting data, processing it, and disseminating information arising from it has rendered them the primary source of information regarding the OPT for international forums, journalists, scholars, foreign government agencies, and even Israeli government agencies (Barag 2017; Braverman 2012; Kutz-Flamenbaum 2016; Miretski and Bachmann 2014). Indeed, the reliance of

government agencies on the information these NGOs gather and analyze is a testament to the quality of work that they do.

These organizations are thus committed both to stopping human rights violations in the short run and to ending the decades-long Israeli occupation of the Palestinian territories. Yet, what these NGOs have found over the course of their activity is that merely putting the information on the web, available for all the world to see, is not enough. They have also learned that a large majority of the Israeli public does not want to hear about these violations or the occupation in general (Aggestam and Strömbom 2013; Avni 2006; Desai 2015; Fleischmann 2016; Helman 2015), and that in the international arena Palestinian suffering "competes" for attention with many other types of suffering by different groups. This has pushed the organizations to be much more active in their dissemination of information and to dynamically seek an audience. Thus, beyond responding to queries that seek information, some of these NGOs often approach relevant forums that might see value in such information, produce pressure on the Israeli government, and eventually affect decision-making processes.

Nevertheless, despite all the dedication and creativity that Israeli human rights NGOs invest in their endeavor, their overall success is limited (Aggestam and Strömbom 2013; Fleischmann 2016; Kutz-Flamenbaum 2016; Miretski and Bachmann 2014). The occupation in general seems to be deepening with time, and the goal of either nullifying or eroding it has clearly not been realized. Moreover, the much more modest aspiration to put an end to systematic violations of human rights has had a very limited effect.

Second move: attack from the right-wing

It is precisely the role Israeli NGOs play in disseminating information about human rights violations perpetuated against Palestinians that causes a huge backlash against them within Israeli society (Avni 2006; Handel and Dayan 2017). The Israeli right-wing, which enjoys widespread support among Jews in Israel, has recognized that by imposing transparency upon government agencies, and by communicating the mass violation of human rights to publics and organizations abroad, these NGOs are exposing Israel to pressure to change its policies and end the occupation. The right-wing has recognized that this type of transparency jeopardizes the constant gains it enjoys in terms of solidifying and normalizing the occupation and that it should enlist its political power and its control of the Israeli government in order to terminate this transparency.

The method the Israeli right-wing has chosen involves a combination of direct attacks by individuals, groups, and organizations, and indirect attacks using legislative and administrative power (Handel and Dayan 2017). Israel's right-wing control over state power has been used in several ways in order to weaken these NGOs. For instance, taxation policies were altered in order to

make donations to human rights NGOs less attractive and ultimately diminish their funding (Aggestam and Strömbom 2013; Policy Working Group 2018; Sucharov 2016). Legislative steps have also been taken, allegedly in the name of greater transparency, to force these specific NGOs to disclose the sources of their funding (Gild-Hayo 2018) in order to reveal that a significant portion of donations to Israeli human rights NGOs originates from foreign entities.

Complementing these legislative transparency steps were the steps taken by private right-wing individuals, groups, and organizations aimed at delegitimizing NGOs. Such steps included several media campaigns that focused on the fact that much of their funding comes from abroad, and thus painted them as traitors. Among them was a propaganda video titled "The Moles," produced by Im Tirzu (a far-right Israeli organization), which suggests a link between terrorist attacks against Israelis and four figures from four Israeli human rights NGOs. The video claims that these activists and the organizations they are affiliated with work for foreign interests opposing Israel.[3] Tapping into a well-known distrust of Israeli Jews toward foreign governments/bodies, this video attempts to enrage the public against these organizations and provoke retaliation against them.

Another use of transparency by the Israeli right-wing is evident in the heavily funded project "NGO Monitor." This website holds a detailed database of all the human rights-related NGOs that operate in Israel/Palestine. On its homepage, the organization describes its mission as follows: "we work to ensure that decision makers and civil society operate in accordance with the principles of accountability, transparency, and universal human rights" (NGO Monitor 2019). Although not unprecedented (e.g. Kutz-Flamenbaum 2016; Perugini and Gordon 2015), this is in fact one of the most blatant attempts to use Israeli human rights NGOs' rhetoric and methods against them.

Third move: minimal transparency

The effects of the sophisticated right-wing moves against the Israeli human rights NGOs have been nontrivial but still limited. The ultimate goal of disabling these organizations or intimidating them into docility has not been attained. Indeed, the top management of these organizations explicitly says that these campaigns have not changed their work procedure in any significant way (Gvaryahu 2019; Montell 2019).

That said, it is evident that these attacks have posed a challenge to these organizations and hijacked some of their time, attention, and energy. Repeated threats of physical assault against activists, sometimes with indications that these activists were being followed/surveilled, and a handful of actual assaults that took place, have rattled NGO activists (Gvaryahu 2019). Activists from the more well-known human rights NGOs, for instance, try to keep their affiliation somewhat secret (Doe 2017; Smith 2017). The NGOs themselves have in some instances needed to coordinate security arrangements (Gvaryahu

2019; Montell 2019). Beyond the threat of vigilantism from militant right-wing activists, there is a threat of verbal attacks, refusal of service, or work-related reprisals that seems to come from the general Jewish public, which shows strong and sometimes active support for the fight against internal and external "enemies" (Dishy 2017; Kuntsman and Stein 2015). Another type of attack that these organizations, especially the most visible, face is cyberattacks, requiring some NGOs to defend themselves accordingly (Yellin 2017).

These NGOs have needed to adapt institutionally, since they are now legally required to disclose certain facts regarding their funding. Yet these legal obligations have not pushed them to more substantial transparency, but rather to adhere to the letter of the law. Among other things, they are now required to publish a quarterly list of foreign donors, to specify on their website and in mail correspondence if they are mostly funded by foreign entities, and when appearing before the Israeli Parliament, to inform the committee chair of the same. An examination of these NGOs' websites shows that they adhere to these provisions, and sometimes do so under a "Transparency" section. However, that same examination (conducted twice in 2018 and 2019) showed that they did not go beyond what is required by law in any significant measure, although hypothetically this opportunity could have been used to disclose further information. In fact, there are good indications that the combined attacks have shifted these organizations slightly away from transparency and toward opaqueness in their dealings with elements outside the organization. This was alluded to by several activists whom I interviewed (e.g. Doe 2017), and also experienced by me directly when trying to secure interviews. I often found myself denied access and asked to provide ample assurances regarding my aims before and during interviews.

It is precisely the sophisticated use of imposed transparency on the part of the right-wing that has provoked this modest but apparent retreat from transparency by such organizations. Among the tactics that were used at least in one conspicuous case—that of the NGO Breaking the Silence—was the organization's infiltration by several right-wing activists in order to gather information that would present the organization in a negative light and expose it to the public (Gvaryahu 2019). Fears of such forms of information-seeking have provoked heightened suspicion toward unknown outsiders and a much more robust vetting process of would-be activists.

When asked to explain what makes both the governmental and non-governmental efforts to impose transparency on Israeli human rights NGOs instances of "bad faith," interviewees point to their one-sided applicability. NGO Monitor only directs its probes to left-wing organizations, is itself not transparent, and heavily decontextualizes the information it gathers (Policy Working Group 2018; Sfard 2017). The legislation that was passed forcing transparency on these NGOs was carefully worded in order to apply mainly to left-wing human rights NGOs, and not across the board. Even when it

did apply, right-wing NGOs were de facto exempt from it (Bendet 2015; Gvaryahu 2019; Montell 2019). Thus, since these attempts of forced transparency are not universal, they are perceived as illegitimate and disingenuous.

Conclusion

After analyzing the two OPT case studies, what becomes obvious is that imposed transparency is amply used to achieve strategic political goals. New forms of disclosure are constantly being invented and imposed on a targeted party in order to achieve "security," restriction of movement, protection of human rights, the end of the occupation, and other goals. None of the described transparency moves were universally applied. The checkpoints only target Palestinians with their imposed transparency. Jewish settlers, although implicated in a variety of crimes against Palestinians, are not inspected. Similarly, Machsom Watch activists target the checkpoints of the West Bank for monitoring. They do not monitor what other security personnel do in the OPT, nor the occasional crimes carried out against soldiers/police officers. None of the parties asked for consent, and no consent has been given by the targets of imposed transparency. Moreover, most of the transparency is achieved by monitoring/surveillance, and there is very little self-disclosure in the process. Hence, the presented cases lie almost squarely within the imposed transparency archetype (see Table 4.1) and are a good representation of its dynamics.

As the empirical analysis shows, imposed transparency is not something that targeted organizations and individuals seem to come to terms with. Resistance/evasion is strong and both individuals (e.g. soldiers) and organizations (e.g. NGOs) are constantly seeking ways to shake off the monitoring that is imposed on them. Translated into the study of surveillance, the above observed dynamics have pessimistic prospects for the viability of Bentham's and Foucault's idea of internalization of the watching eye in situations of constant imposed monitoring. In fact, the end result is the Foucauldian panopticon effect in reverse—instead of self-regulation, these organizations and individuals opt for regression to opaqueness. This insight may serve as a warning sign for those who overestimate the power of surveillance and of imposed transparency—these tools may achieve an immediate desired goal, but in cases when they truly expose the targets to negative effects, they will probably be neither internalized nor accepted.

Cycles of imposed and counter-imposed transparency seem to come with negative side effects. Among them are the personalization of animosity and the erosion of the concept of transparency. Imposed transparency appears to personalize animosity by connecting what targets perceive as a negative outcome with the entity that initiated it. The term transparency, for its part, sheds all of its positive connotations in this process and becomes hollow and

strictly utilitarian. Most importantly, imposed transparency does not serve as a gateway to voluntary transparency, instead breeding even greater opacity.

That said, we have to acknowledge the sharp asymmetry in power between the different parties in these cycles of imposed transparency. As the empirical examination shows, this asymmetry means that both applying imposed transparency and coping with its imposition as a target are much more effective for the powerful side than for the weaker side. Powerful organizations, such as the army, can establish massive operations of imposed transparency and can rely on their heavy state support to avoid being the target of imposed transparency. Weak groups/organizations can apply imposed transparency, but with great investment of effort and at significant personal cost. Their ability to avoid being targeted also requires a disproportionate investment of energy and has limited results. That said, although imposed transparency favors the strong, it is often the only recourse of the weak. In our case, this asymmetry, which is part of the colonial settings in the Middle East, means that the NGOs' imposed transparency only succeeds in stopping the most egregious violations of Palestinian human rights, and that the occupation is neither eliminated nor curbed.

Notes

1 It is of course paradoxical that the process of demanding transparency from Palestinians is itself starkly untransparent.
2 This section refers to all Israeli NGOs dealing with Palestinian human rights, not just those dealing with checkpoints.
3 The video is available here: https://youtu.be/02u_J2C-Lso.

References

Abu-Laban, Yasmeen. 2014. "Gendering Surveillance Studies." *Surveillance & Society* 13(1): 44–56.

Aggestam, Karin, and Lisa Strömbom. 2013. "Disempowerment and Marginalisation of Peace NGOs." *Peacebuilding* 1(1): 109–24.

Allen, David S. 2008. "The Trouble with Transparency." *Journalism Studies* 9(3): 323–40.

Andreas, Peter, and Timothy Snyder, eds. 2000. *The Wall Around the West: State Borders and Immigration Controls in North America and Europe*. Lanham, MD: Rowman and Littlefield.

Auger, Giselle A. 2014. "Trust Me, Trust Me Not." *Journal of Public Relations Research* 26(4): 325–43.

Avni, Ronit. 2006. "Mobilizing Hope: Beyond the Shame-Based Model in the Israeli–Palestinian Conflict." *American Anthropologist* 108(1): 205–14.

Bac, Mehmet. 2001. "Corruption, Connections and Transparency." *Public Choice* 107(1): 87–96.

Bannister, Frank, and Regina Connolly. 2011. "The Trouble with Transparency." *Policy & Internet* 3(1): 1–30.

Bauhr, Monika, and Marcia Grimes. 2014. "Indignation or Resignation: The Implications of Transparency for Societal Accountability." *Governance* 27(2): 291–320.

Bendet, Shabtai. 2015. "Under the Auspice of the Registrar of Associations: Right-Wing NGOs Are Evading Disclosing Funding Sources." *Walla*, December (in Hebrew).

Bertot, John C., Paul T. Jaeger, and Justin M. Grimes. 2010. "Using ICTs to Create a Culture of Transparency." *Government Information Quarterly* 27(3): 264–71.

Bessire, Dominique. 2005. "Transparency: A Two-Way Mirror?" *International Journal of Social Economics* 32(5): 424–38.

Bigo, Didier. 2006. "Globalized-in-Security: The Field and the Ban-Opticon." *Traces: A Multilingual Journal of Cultural Theory* 4: 109–57.

Bigo, Didier, and Elspeth Guild, eds. 2005. *Controlling Frontiers: Free Movement into and Within Europe.* Hampshire: Ashgate.

Braverman, Irus. 2011. "Civilized Borders: A Study of Israel's New Crossing Administration." *Antipode* 43(2): 264–95.

Braverman, Irus. 2012. "Checkpoint Watch: Reflections on Israel's Border Administration in the West Bank." *Social & Legal Studies* 21: 297–320.

Brucato, Ben. 2015. "The New Transparency: Police Violence in the Context of Ubiquitous Surveillance." *Media and Communication* 3(3): 39–55.

Davidov, Eldad. 2014. "Not Occupiers, Service Providers." *Hamakom Hachi Ham Bagehenom*, December (in Hebrew).

Desai, Chandni. 2015. "Shooting Back in the Occupied Territories: An Anti-colonial Participatory Politics." *Curriculum Inquiry* 45(1):109–28.

Dishy, Aaron. 2017. "Selfies, Sexts, and Squadrons: The Digital Culture of the Israeli Defense Forces." *iJournal* 2(2). https://theijournal.ca/index.php/ijournal/article/view/28122.

Drucker, Susan J., and Gary Gumpert. 2007. "Through the Looking Glass: Illusions of Transparency and the Cult of Information." *Journal of Management Development* 26(5): 493–8.

Dubrofsky, Rachel E., and Shoshana A. Magnet. 2015. "Feminist Surveillance Studies: Critical Interventions." In *Feminist Surveillance Studies*, edited by Rachel E. Dubrofsky, and Shoshana A. Magnet, 1–17. Durham, NC: Duke University Press.

Duke, Shaul A. 2019. "Database-Driven Empowering Surveillance: Definition and Assessment of Effectiveness." *Surveillance & Society* 17(3/4): 499–516.

Fleischmann, Leonie. 2016. "Beyond Paralysis: The Reframing of Israeli Peace Activism since the Second Intifada." *Peace & Change* 41(3): 354–85.

Foucault, Michel. (1975) 1991. *Discipline and Punish*. New York, NY: Vintage Books.

Gild-Hayo, Debbie. 2018. *Overview of Anti-Democratic Legislation Advanced by the 20th Knesset*. Tel Aviv: The Association for Civil Rights in Israel.

Gilliom, John, and Torin Monahan. 2012. "Everyday Resistance." In *Routledge Handbook of Surveillance Studies*, edited by Kirstie Ball, Kevin Haggerty, and David Lyon, 405–11. London: Routledge.

Grimmelikhuijsen, Stephan G. 2010. "Transparency of Public Decision-Making: Towards Trust in Local Government?" *Policy & Internet* 2(1): 5–35.

Grimmelikhuijsen, Stephan G., Gregory Porumbescu, Boram Hong, and Tobin Im. 2013. "The Effect of Transparency on Trust in Government." *Public Administration Review* 73(4): 575–86.

Hall, Rachel. 2017. "Surveillance and Public Space." In *Oxford Research Encyclopedias: Communication*, 1–17. https://doi.org/10.1093/acrefore/9780190228613.013.145

Hallward, Maia Carter. 2008. "Negotiating Boundaries, Narrating Checkpoints: The Case of Machsom Watch." *Critique: Critical Middle Eastern Studies* 17(1): 21–40.

Handel, Ariel. 2011. "Exclusionary Surveillance and Spatial Uncertainty in the Occupied Palestinian Territories." In *Surveillance and Control in Israel/Palestine*, edited by Elia T. Zureik, David Lyon, and Yasmeen Abu-Laban, 259–75. London: Routledge.

Handel, Ariel, and Hilla Dayan. 2017. "Multilayered Surveillance in Israel/Palestine." *Surveillance & Society* 15(3/4): 471–76.

Hass, Amira. 2019. "Renovated Checkpoints for Palestinians Are Nothing but Crumbs of Mercy." *Haaretz*, December.

Helman, Sara. 2015. "Challenging the Israeli Occupation Through Testimony and Confession." *International Journal of Politics, Culture, and Society* 28(4): 377–94.

Hirschfield, Robert. 2007. "The Checkpoint Women of Israel." *In These Times*, December.

Jackson, Brian A. 2015. *Strengthening Trust between Police and the Public in an Era of Increasing Transparency*. Santa Monica, CA: RAND Corporation.

Kanagaretnam, Kiridaran, Stuart Mestelman, Khalid S. M. Nainar, and Mohamed Shehata. 2010. "Trust and Reciprocity with Transparency and Repeated Interactions." *Journal of Business Research* 63(3): 241–7.

Kolstad, Ivar, and Arne Wiig. 2009. "Is Transparency the Key to Reducing Corruption in Resource-Rich Countries?" *World Development* 37(3): 521–32.

Koskela, Hille. 2012. "'You Shouldn't Wear that Body': The Problematic of Surveillance and Gender." In *Routledge Handbook of Surveillance Studies*, edited by Kirstie S. Ball, Kevin D. Haggerty, and David Lyon, 49–56. London: Routledge.

Kotef, Hagar, and Merav Amir. 2007. "(En)Gendering Checkpoints: Checkpoint Watch and the Repercussions of Intervention." *Signs* 32(4): 973–96.

Kuntsman, Adi, and Rebecca L. Stein. 2015. *Digital Militarism: Israel's Occupation in the Social Media Age*. Palo Alto: Stanford University Press.

Kutz-Flamenbaum, Rachel V. 2016. "The Importance of Micro-Level Effects on Social Movement Outcomes." *Sociological Perspectives* 59(2): 441–59.

Lentin, Ronit. 2017. "Race and Surveillance in the Settler Colony." *Palgrave Communications* 3: 17056.

Lindstedt, Catharina, and Daniel Naurin. 2010. "Transparency Is Not Enough: Making Transparency Effective in Reducing Corruption." *International Political Science Review* 31(3): 301–22.

Mann, Steve. 2013. "Veillance and Reciprocal Transparency." *International Symposium on Technology and Society*, Toronto, December.

Mansbach, Daniela. 2007. "Crossing the Borders: The Power of Duality in the Protest of the 'Checkpoint Watch' Movement." *Theory and Criticism* 31: 77–99 (in Hebrew).

Mansbach, Daniela. 2009. "Normalizing Violence: From Military Checkpoints to 'Terminals' in the Occupied Territories." *Journal of Political Power* 2(2): 255–73.

Margetts, Helen. 2011. "The Internet and Transparency." *Political Quarterly* 82(4): 518–21.
Marsh, Kevin. 2011. "The Illusion of Transparency." *Political Quarterly* 82(4): 531–5.
Marx, Gary T. 2003. "A Tack in the Shoe: Neutralizing and Resisting the New Surveillance." *Journal of Social Issues* 59(2): 369–90.
Miretski, Pini P., and Sascha-Dominik V. O. Bachmann. 2014. "The Panopticon of International Law: B'Tselem's Camera Project." *Osgoode Hall Law Journal* 52(1): 235–62.
Monaghan, Jeffrey. 2013. "Settler Governmentality and Racializing Surveillance in Canada's North-West." *Canadian Journal of Sociology* 38(4): 487–508.
NGO Monitor. 2019. "NGO Monitor." www.ngo-monitor.org/.
O'Neill, Onora. 2002. *A Question of Trust: The BBC Reith Lectures 2002*. Cambridge: Cambridge University Press.
Perugini, Nicola, and Neve Gordon. 2015. *The Human Right to Dominate*. Oxford: Oxford University Press.
Policy Working Group. 2018. *NGO Monitor: Shrinking Space*. Jerusalem: Policy Working Group.
Rawlins, Brad R. 2008. "Measuring the Relationship Between Organizational Transparency and Employee Trust." *Public Relations Journal* 2(2): 1–21.
Rijke, Alexandra, and Claudio Minca. 2019. "Inside Checkpoint 300: Checkpoint Regimes as Spatial Political Technologies in the Occupied Palestinian Territories." *Antipode* 51(3): 968–88.
Schnackenberg, Andrew K., and Edward C. Tomlinson. 2016. "Organizational Transparency: A New Perspective on Managing Trust." *Journal of Management* 42(7): 1784–810.
Schnorf, Sebstian, Martin Ortlieb, and Nikhil Sharma. 2014. "Trust, Transparency & Control in Inferred User Interest Models." *Conference on Human Factors in Computing Systems*, Toronto, December, 2249–54.
Sfard, Michael. 2017. "After a Decade of Persecution I Decided to Break the Silence and to Answer Gerald Steinberg." *Siha Mekomit*, December (in Hebrew).
Sperling, Stefan. 2011. "The Politics of Transparency and Surveillance in Post-Reunification Germany." *Surveillance & Society* 8(4): 396–412.
State Comptroller of Israel. 2011. *The 2010 Annual Report 61A*. Jerusalem: State Comptroller of Israel (in Hebrew).
Sucharov, Mira. 2016. "Is B'Tselem Right to Quit Playing 'Middle Man' for the IDF?" *Forward*, December.
Trottier, Daniel, Rashid Gabdulhakov, and Qian Huang. 2020. "Introducing Vigilant Audiences." In *Introducing Vigilant Audiences*, edited by D. Trottier, R. Gabdulhakov, and Q. Huang, 1–23. Cambridge: OpenBook Publishers.
Walsh, James P. 2010. "From Border Control to Border Care: The Political and Ethical Potential of Surveillance." *Surveillance & Society* 8(2): 113–30.
Wilson, Dean J. 2012. "Counter-Surveillance, Protest and Policing." *Plymouth Law and Criminal Justice Review* 4: 33–42.
Wilson Dean J., and Tanya Serisier. 2010. "Video Activism and the Ambiguities of Counter-Surveillance." *Surveillance & Society* 8(2): 166–80.
Young, Sarah. 2020. "More Eyes on Crime?: The Rhetoric of Mediated Mugshots." In *Introducing Vigilant Audiences*, edited by D. Trottier, R. Gabdulhakov, and Q. Huang, 307–30. Cambridge: OpenBook Publishers.

Zureik, Elia T. 2001. "Constructing Palestine Through Surveillance Practices." *British Journal of Middle Eastern Studies* 28(2): 205–27.
Zureik, Elia T. 2011. "Colonialism Surveillance, and Population Control: Israel/Palestine." In *Surveillance and Control in Israel/Palestine*, edited by Elia T. Zureik, David Lyon, and Yasmeen Abu-Laban, 3–46. London: Routledge.
Zureik, Elia T. 2016. *Israel's Colonial Project in Palestine: Brutal Pursuit*. London: Routledge.

Interviews

Afek, Rachel (activist, Machsom Watch), telephone, September 12, 2019.
Bar, Shuli (activist, Machsom Watch), telephone, November 16, 2017 and September 12, 2019.
Barag, Hanna (activist, Machsom Watch and Yesh Din), in person, Jerusalem, November 14, 2017 and by telephone, September 9, 2019.
Doe, John (former B'Tselem employee, pseudonym), in person, Tel-Aviv, November 28, 2017.
Gvaryahu, Avner (director of Breaking the Silence), telephone, September 23, 2019.
Konforty, Aviva (activist, Machsom Watch), telephone, November 22, 2017.
Maor, Idit (activist, Machsom Watch), telephone, September 16, 2019.
Montell, Jessica (director of HaMoked), telephone, September 12, 2019.
Smith, John (former B'Tselem employee, pseudonym), in person, Tel-Aviv, November 15, 2017.
Yellin, Roy (director of Public Outreach at B'Tselem), telephone, December 19, 2017.

Chapter 5

Classifying and dividing labor

The political economy of racializing surveillance

Markus Kienscherf

Introduction

According to Andrea Smith (2015, 23), "Surveillance studies's focus on the modern state similarly hides an analysis of the settler colonialist and white supremacist logics of surveillance that precede the ascendancy of the modern state." Indeed, surveillance studies has not yet fully explored the colonial genealogies of surveillance. In the United States, both the modern administrative state itself and the surveillance practices that have helped and continue to help produce and reproduce it have both a settler colonialist and white supremacist genealogy. In this chapter, I will not only draw out the colonial genealogy of racializing surveillance but also show that contemporary surveillance ultimately serves to secure a neocolonial political economy based on racial divisions within the working class.

Simone Browne (2015, 16) defines racializing surveillance as a "technology of social control where surveillance practices, policies and performances concern the production of norms pertaining to race and exercise a 'power to define what is in or out of place.'" David Lyon suggests that we ought to understand "surveillance as social sorting" in order to tease out the "classifying drive of contemporary surveillance" (Lyon 2003, 13). Surveillance undoubtedly serves the purpose of social sorting, and this holds particularly true for racializing surveillance. Yet, this leaves open the question as to what the purpose of social sorting is. In capitalist social formations a key function of social sorting, although not the only one, is to secure the conditions for capitalist accumulation. In this chapter, I will argue that racializing surveillance is, above all, a colonial technology for (re)producing racial divisions within the US working class while also drawing out the dialectical relations between transparency and opacity in contemporary US racializing surveillance. For, ultimately, contemporary racializing surveillance obscures not only its settler colonial *and* colonial genealogy but also its contemporary neocolonial ontology. Drawing on (neo-)Marxian theory, I will first map how capitalist accumulation was not only historically enabled by settler colonialism *and* colonialism but continues to depend on a neocolonial logic of oppression

DOI: 10.4324/9781003120827-7

that combines "ordinary" exploitation with racialized expropriation and disposability. Second, I will show how capitalist expropriation and disposability in the United States have been and continue to be facilitated by practices of racializing surveillance. Lastly, I will argue that as a key manifestation of racializing surveillance in the contemporary United States, welfare surveillance reproduces neocolonial racial divisions under the conditions of formal legal equality and professed colorblindness.

Race and the exploitation, expropriation, and disposability of labor

In the first volume of *Capital*, Marx begins his critique of political economy with an analysis of the commodity. Marx makes a distinction between the concrete qualitative uses to which commodities can be put—their use value—and their quantitative relation to all other commodities—their exchange value. Nonetheless, despite their material differences and their fundamentally different use values, all commodities are products of labor (Marx 1976). The amount of labor that goes into the production of commodities makes for their commensurability. This is expressed by the concept of value, which Marx (1976, 129) defines as "socially necessary labour time"—the average amount of labor time that goes into the production of a particular commodity at a given place, at a given time. Socially necessary labor time thus determines a commodity's value, which is, in turn, represented by exchange value in relation to other commodities and which is ultimately expressed in terms of a price. Marx goes on to examine the process of commodity exchange and finds that under the conditions of a competitive market for commodities, sustained profits cannot arise from exchange. All market participants try to buy cheaply and sell dearly, and some of them may indeed obtain some profit because, due to the ebb and flow of supply and demand, prices do not always correspond to a commodity's value. But as each seller is also a buyer, profits are fleeting; if one market participant is able to sell particularly dearly today, she may have to buy more expensively tomorrow. In short, because of market competition the price of each commodity will ultimately even out around a commodity's actual value so that profits are ephemeral (Marx 1976).

Yet, capitalists do find one commodity on the market that can create more than its original value. This is the peculiar commodity of labor power. Labor power also has a value, namely the socially necessary labor time for producing the commodities needed to sustain a laborer at a historically and geographically specific standard of living (Marx 1976). The value of labor power is reproduced after a certain time, but if laborers are made to work longer and/or more intensively than required to reproduce the value of their labor power, the capitalist has obtained surplus value. This is the Marxian definition of exploitation: the contractual obligation of laborers to work longer and/or more intensively than necessary to produce the value of the commodities

workers need to sustain themselves at a given standard of living, at a given place, at a given time (Marx 1976). Exploitation is the source of surplus value, which capitalists can consume away and/or reinvest. However, the continuous productive reinvestment of at least some portion of surplus value is what ultimately defines the capitalist. This is what capitalist accumulation is all about: the constant reinvestment of past profits to generate even more profits in the future (Marx 1976).

Marx thus shows that capitalist accumulation ultimately hinges on the commodification of labor power and the concomitant exploitation of the laborer. The commodification of labor power in turn centers on two conditions: (1) generalized commodity exchange based on the large-scale monetization of economic relations; and (2) processes of proletarianization. Yet, whereas the imperative of capital accumulation has become an almost universal social force, processes of proletarianization have unfolded unevenly and continue to be highly particularistic. According to Étienne Balibar (1991b, 161–2), proletarianization entails three separate social processes that cannot be solely derived from the purely economic contradictions inherent in the capitalist mode of production. First, *exploitation*, as outlined above, consists of the extraction of surplus labor (and hence also surplus value) by having laborers work above and beyond the actual value of their labor power. Second, through mechanization, automation, and the rationalization of the labor process laborers come under the ever more direct control and surveillance of the capitalist or her representatives for the duration of their labor time. This is what Marx (1976) called the shift from the formal to the real subsumption of labor under capital. Thus, the commodification of labor power also entails the *domination* of labor by capital at the workplace. Both exploitation and domination are conditioned by locally specific forms of contract law and local variations in how the formal freedom and equality of the public sphere (including the market) is demarcated from the private sphere of production (Marx 1976). Thirdly, laborers also bear the economic risks and associated insecurity of having to sell their labor power. They are exposed to market fluctuations, crises, and a trend toward rendering labor power superfluous through increasing investment in labor-saving machinery. Laborers thus also compete against one another in the labor market. Divisions and hierarchies within the working class both exacerbate *competition* between workers and are also compounded by it, as workers mobilize these divisions and hierarchies not only in making their economic claims but also in expressing their opposition to their own oppression (Balibar 1991a, 214). This spatially and temporally uneven development of proletarianization is, on the one hand, the result of the historical processes that prompted proletarianization in the first place and, on the other, due to the fact that labor power is what Karl Polanyi called a fictitious commodity (Polanyi 1957, 75).

Firstly, proletarianization came about through a set of brutal historical processes that Marx called primitive accumulation. Primitive accumulation

violently divested numerous people from their means of production and/or subsistence—primarily land—and also provided a large influx of precious metals into Europe, which led to increasing monetization, which in turn helped generalize commodity exchange (Marx 1976). Primitive accumulation occurred both in the colonial periphery and the metropolitan core, but with a key difference: whereas in Europe the large-scale dispossession of people mostly drove them into wage labor, the colonized were frequently forced into forms of unpaid labor. The imposition of various coercive colonial labor regimes was, moreover, entangled with the development of racial ideologies. Racial ideologies developed in the context of and as a direct consequence of the colonial conquest of the Americas, where, as the Peruvian sociologist Aníbal Quijano (2000, 533) puts it, "[t]he conquistadors assumed this idea [of race] as the constitutive, founding element of the relations of domination that the conquest imposed." In the United States, the ideology of "race" developed through the codification of differences between free and enslaved people in order to justify and reproduce slavery "in a republic founded on radical doctrines of liberty and natural rights, and, more important a republic in which those doctrines seemed to represent accurately the world in which all but a minority lived" (Fields and Fields 2014, 141). From the foundation of the American republic, racism and class oppression have thus been inextricably intertwined. African Americans became a "race" because of the violent expropriation of their labor power—in short, because of their violently imposed class position as enslaved people (Fields and Fields 2014, 266–7). The ideology of "race" persisted even after the class position from which it originally derived was abolished. The ideology of "race" has undoubtedly undergone profound historical changes, but it still serves to justify various forms of racism—that is to say, forms of differential treatment alleged to result from ultimately fictitious innate differences of the individuals and/or groups who are the victims of discrimination. This is what Fields and Fields (2014, 261 and 97) call "the social alchemy of racecraft [which] transforms racism into race" so that "[d]isguised as race, racism becomes something Afro-Americans are, rather than something racists do." Particular populations are thus "racialized" because they are the targets of racism and not the other way around. Even though racism is no longer directly tied to the class position of enslaved people, in capitalist social formations in general, and in the United States in particular, racism still serves to reproduce labor power below its value and "to exclude populations from the labor market" (Grosfoguel 2003, 210). As Immanuel Wallerstein puts it:

> A capitalist system that is expanding (which is half the time) needs all the labour-power it can find, since this labour is producing the goods through which more capital is produced, realized and accumulated. Ejection out of the system is pointless. But if one wants to maximize the accumulation of capital, it is necessary simultaneously to minimize the costs of

> production (hence the costs of labour-power) and minimize the costs of political disruption (hence minimize – not eliminate, because one cannot eliminate – the protests of the labour force). Racism is the magic formula that reconciles these objectives.
>
> (Wallerstein 1991b, 33)

Indeed, capitalism has never been colorblind, and racism continues to play a significant role in facilitating capitalist accumulation.

Colonial violence, racism, and expropriation were, indeed, pivotal for the eventual expansion of the capitalist mode of production. Colonialism is widely held to have ended with the independence of most former colonies. Yet, a number of scholars argue that coloniality persists despite the abolition of colonial forms of labor control and the independence of former colonies (Grosfoguel 2003; Pinderhughes 2011; Quijano 2000). A hierarchical division of labor along the lines of race and ethnicity "continues to be an integral part of the contemporary global division of labor even after independence and the global expansion of the capitalist wage-labor relation" (Grosfoguel 2003, 146). In fact, "the entanglement of capitalist accumulation processes with a racial/ethnic hierarchy and its derivative classifications of superior/inferior, developed/undeveloped, and civilized/barbarian people" constitutes a global coloniality even in the absence of any formal colonial system of rule (Grosfoguel 2003, 17; see also Quijano 2000). This situation should be termed neocolonial in order to highlight both the ruptures (abolition of colonial labor control, granting of formally equal rights, some forms of self-rule, etc.) and the continuities (racial/ethnic division of labor, persistence of racism) between classical colonialism and contemporary neocoloniality. Primitive accumulation articulated a division between "free" and "unfree" labor upon a division between superior and inferior humans. In fact, unfree laborers in the colonies were not exploited in the strict Marxian sense, but their labor power was violently expropriated. The analytical distinction between exploitation and expropriation is a crucial one, and I will discuss its historical and contemporary significance in greater detail below.

Secondly, the uneven processes of proletarianization are also due to the peculiar nature of the commodity of labor power. The economic value of labor power—the socially necessary labor time that goes into the production of the commodities needed to sustain a laborer—only accounts for the bare life of the laborer. Yet, all sorts of immaterial and unquantifiable factors are required for the production and reproduction of the human bearers of labor power: love, care, education, meaningful social relations in general, etc. Indeed, labor power has come to be exchanged as a commodity, but it is hardly if ever produced as a commodity. This has led Karl Polanyi to treat labor power as a fictitious commodity—alongside land and money (Polanyi 1957, 71–80). The very fiction that labor, land, and money are commodities is what allows for their exchange as commodities, and their exchange

as commodities is, in turn, a basic condition for capitalist accumulation. Polanyi further argues that extending markets to labor, land, and money not only required a separation between economy and society but also reshaped society into a market society. The colonization of social relations by labor markets, in particular, led to major social dislocations. For, "[t]o allow the market mechanism to be the sole director of the fate of human beings and their natural environment indeed, even of the amount and use of purchasing power, would result in the demolition of society" (Polanyi 1957, 76). Society had to respond to these dislocations, giving rise to what Polanyi calls a "double movement":

> Social history in the nineteenth century was thus the result of a double movement: the extension of the market organization in respect to genuine commodities was accompanied by its restriction in respect to fictitious ones.
>
> (Polanyi 1957, 79)

In order to ensure the continuous availability of these fictitious commodities as crucial factors for the capitalist mode of production, to maintain the fiction of their status as commodities, and to secure social stability and hence also the capitalist mode of production itself from the social dislocations caused by processes of fictitious commodification, capitalism requires what Nancy Fraser calls "background conditions of possibility" (Fraser 2014). The aforementioned processes of proletarianization—exploitation, domination, and competition—already indicate that the commodification of labor power is at once an economic and a political phenomenon. Marx himself went beyond exchange into the hidden abode of production to show that the expansion of value does not arise out of exchange but from the exploitation of labor. Moreover, Marx showed how the concentration of private property in the means of production and the commodification of labor power was ultimately brought about by primitive accumulation, that is to say, by state-sanctioned force, theft, and plunder. Throughout *Capital*, Marx also hints at the necessity of state power to prop up an already established capitalist mode of production. However, the main thrust of his argument—except for the section on primitive accumulation—tends to unfold within the parameters of bourgeois political economy: perfectly functioning competitive markets and minimal state interference. Marx's critique of bourgeois political economy is, for the most part, a critique of the capitalist mode of production in the abstract and not of concrete capitalist social formations.

Nancy Fraser, however, argues that capitalism ought to be understood as an institutionalized social order that demarcates and depends on external spheres that not only provide labor power and means of production below value but also ultimately help secure capitalism from its own crisis tendencies as well as from working-class opposition. She suggests that we shift the focus

"from the front-story of exploitation to the back-story of expropriation" (Fraser 2014, 60). From this perspective, the exploitation of laborers and thus the expansion of capital centers on the continuing expropriation of nature, the unremunerated work of women, and the deployment of state power to secure the conditions for capitalist accumulation. Consequently, primitive accumulation does not just constitute "the pre-history of capital, and of the mode of production corresponding to capital" but ought to be seen as an ongoing process (Marx 1976, 875). The violent expropriation of labor and means of production from spheres outside the capitalist mode of production is a structural necessity, especially in response to periodic crises. What is more, primitive accumulation entailed and continues to entail the accumulation of divisions and hierarchies within the working class—divisions and hierarchies that became codified and naturalized in terms of race and gender (Federici 2004, 63–4).

If all commodities, including labor power, are sold and bought at their value, the exploitation of labor is the only source of surplus value. Yet, even though the capitalist mode of production relies on commodity circulation for realizing the value (and surplus value) of its outputs, capitalists still scramble to get their inputs (labor power and means of production) from outside of commodity circulation proper, that is to say, below value or even for free. This has considerable consequences for how we conceive of the working class, because not all members of the working class are wage laborers. What defines the working class is that it creates (surplus) value for capitalists (Wallerstein 1991a, 120).

Workers may get to keep some of the value they create (e.g., in the form of a wage) but never all of it. If a worker gets to keep that portion of the overall value of her product that corresponds to the value of the commodities needed to reproduce herself at a given standard of living at a given place at a given time, she is "merely" being exploited. If she gets less than the value of her labor power, her labor power is being expropriated. What is more, workers worldwide tend to live in households where they pool a variety of different income streams: wage income, subsistence production, petty commodity production, rent, and transfer payments (Wallerstein 2004, 32–4). The degree of proletarianization is thus the proportion of household income derived from wage labor as opposed to other sources of household income. Indeed, the proportion of household income derived from wage income in relation to a household's participation in capitalist surplus production thus ultimately determines the degree of exploitation/expropriation of both the overall household and its individual members. In short, expropriation has not only historically enabled exploitation but also continues to complement it, especially in response to crisis. Expropriation and exploitation are therefore two fundamental logics of oppression inherent in capitalist accumulation. However, we should note that exploitation and expropriation are mere approximations. Empirical reality affords very few examples of "pure" exploitation or "pure"

expropriation, although chattel slavery is a clear case of expropriation in its purest and most brutal sense.

Capitalist accumulation also gives rise to a third mode of oppression: the logic of disposability. Marx argued that continuous changes in the organic composition of capital, that is to say, changes in the relation between constant capital (especially technology and machinery) and variable capital (labor power), tend toward the creation of a surplus population whose labor power is no longer needed (Marx 1976, 782–98). A racialized population who was subject to violent expropriation in the past and whose subsequent exploitation has always contained elements of expropriation through labor market segmentation and discrimination is also more likely to become disproportionately superfluous as a result of technological and organizational changes in production.

Capitalists' scramble for cheap labor power and the concomitant expropriation, exploitation, and disposability of the working class not only allows for the continuing accumulation of capital but also for the accumulation of local, regional, national, and global divisions within the working class. These divisions feed competition between members of the working class, which may in turn further entrench these divisions. In short, divisions within the working class are both a condition for and a consequence of capitalist accumulation while also playing a key role in pacifying working-class struggles. Yet, capitalism cannot secure these divisions by purely economic means. State power in general and state surveillance in particular provide the very infrastructure for maintaining and calibrating divisions within the working class to the degree best suited to continuing capitalist accumulation. State power is thus not only a tool for securing the conditions for continuous expropriation and exploitation but also for managing a disposable, economically superfluous population.

Racializing surveillance in the United States (settler) colonial past and present

The contemporary US capitalist social order has been shaped and continues to be shaped by both the *settler colonial* expropriation of land and the *colonial* expropriation of labor power. According to Lorenzo Veracini, settler colonialism and colonialism are two distinct relations:

> On the one hand, the colonial "encounter" is mirrored by what I have theorized as a settler colonial "non-encounter," a circumstance fundamentally shaped by a recurring need to disavow the presence of indigenous "others." On the other hand, in the case of colonial systems, a determination to exploit sustains a drive to sustain the permanent subordination of the colonized (Veracini 2011, 2).

Although, I am in broad agreement with Veracini's argument that "[c]olonialism *reproduces* itself" and "settler colonialism, by contrast,

extinguishes, itself," I do not think that colonialism can be associated with exploitation (Veracini 2011, 3). Both settler colonialism and colonialism are forms of primitive accumulation expressed by different modalities of expropriation. Settler colonialism expropriates indigenous lands, which frequently entails efforts to make indigenous populations invisible. This is why settler colonialism is marked by a logic of elimination (Wolfe 2006). On the other hand, colonialism's expropriation of labor power requires the presence and, at least partial, visibility of the expropriated workers. Their presence cannot be disavowed, and their continuing expropriation needs to be justified. This is why colonial relations are much more likely to give rise to explicit racial ideologies. I am far from saying that racial ideologies are absent from settler colonial relations, but in the United States, at least, it was the colonial regime of slavery that prompted the development of a racial black–white binary and the associated practices of racializing surveillance. In the case of the United States, the visibility of racialized others brought about by the racializing expropriation of labor power perhaps also obscures the settler colonial expropriation of land that provided the conditions of possibility for the subsequent importation of enslaved people.

Chattel slavery constituted a form of colonial labor control defined by the brutal subordination and oppression of enslaved people for the purpose of coercively expropriating their labor power. Slavery was, moreover, entangled with international systems of banking, insurance, and credit, and it also contributed to the rise of industrialization, first in Britain and later in the American north (see Baptist 2014; Johnson 2013; Oakes 2016). Simone Browne suggests that

> slavery must be engaged if we are to create a surveillance studies that grapple with its constitutive genealogies, where the archive of slavery is taken up in a way that does not replicate the racial schema that spawned it and that it reproduced, but at the same time does not erase its violence. (Browne 2015, 13)

Indeed, as the Southern slave plantation system became ever more closely entwined with global capitalist commodity circulation—through its main cash crop cotton—plantation owners developed increasingly sophisticated strategies of surveillance and control in order to extract ever more labor and hence also value from their slaves. Caitlin Rosenthal (2018) shows that Southern cotton planters combined sophisticated management techniques with violence to improve the productivity of slave labor. In fact, slave owners' techniques for monitoring and measuring productivity foreshadowed Fredrick Winslow Taylor's tools of scientific management. The fact that enslaved people were subject to much more intensive and extensive domination than "free" wage laborers meant that slave owners could and did exercise much more control over the labor process than industrial capitalists. Moreover, slave owners

measured and classified enslaved people not only as a captive input to production but also as a form of alienable commodity capital whose value could either appreciate or depreciate over time (Rosenthal 2018).

Wage labor centers on the commodification of labor power. The bearers of this peculiar commodity remain its owners and can sell it as they see fit, although often under highly unfavorable conditions. Yet, once sold, laborers no longer fully control their labor power and have no legal rights to the products of their labor apart from their wages. The contractual exchange of labor power for a money wage is what ultimately allows for exploitation. Slavery, on the other hand, entailed the (almost) total commodification of people themselves. Slaves had neither legal ownership of their labor power, nor could they exert much (if any) control over it. They did not work over and above the value of their labor power to produce surplus value, because the value of their labor power did no longer belong to them. Their labor power had been violently expropriated through their enslavement and was now completely owned by their master. Thus, the surplus value produced by slaves—that is to say, the value they produced over and above their own exchange value as slaves and the value of the commodities needed to keep them alive—is not a product of exploitation in the Marxian sense but of violent expropriation.

The commodification of humans ultimately depended on the definition and enforcement of property rights as well as on the classifications—to be found in ledgers, bills of sale, etc.—that marked people as commodities. Enslaved people were ripped out of their communities and stripped of all the customs, hierarchies, social distinctions, and identities that characterized their previous way of life in order to become subject to the commodifying classifications around productivity and value imposed by the slave trade and the plantation system. However, precisely because enslaved people were humans and not commodities, efforts to commodify them required such horrific forms of violence. Enslaved people did not voluntarily submit to their commodification. In order to become commodities, they constantly needed to be violently subjected to a process of commodification by means of surveillance and violence. And even then, they retained and struggled to assert their humanity (Rinehart 2016; Rosenthal 2018). As Rosenthal demonstrates, the written records of the surveillance and management practices used in and for the profitable commodification of enslaved people both obscure the violence inherent to slavery and also highlight the necessary brutality of a mode of production that feeds on humans as commodities (Rosenthal 2018, 187–205).

The growing size of the slave population was, moreover, considered a massive social control problem. The threat of slave insurrection and the constant risk of slave flight led to the emergence of increasingly formalized slave patrols. The first slave patrols were formed in the seventeenth century and were informal bands of volunteers tasked with recapturing runaway slaves. In the course of the eighteenth century, slave patrols became more

organized and were also charged with preventing insurrection. The Fugitive Slave Act of 1850 gave state governments wide-ranging authority to recruit individuals—especially poor whites—into slave patrols that now had almost unlimited coercive powers over the slave population. Slave patrols were tasked with the routine surveillance of the slave population in order to regulate and manage their movement according to the politico-economic imperatives of chattel slavery (Bass 2001, 159; Brucato 2014, 38–9). In fact, slave patrols are a significant strand in the genealogy of US police (Bass 2001; Brucato 2014; Hadden 2001).

Brutal efforts to control the movement, and hence also the labor, of the black population continued after the abolition of slavery. Immediately after the end of the Civil War, most Southern states replaced their Slave Codes with the so-called Black Codes, which were aimed at severely restricting the freedom of former slaves and maintaining them in a state of quasi-slavery through extremely low wages, debt peonage, as well as numerous sweeping vagrancy statutes. Mounting criticism from the Northern States led to a brief interlude during which the federal government tried to turn freed people into citizens and "free" wage laborers with the help of the Bureau of Refugees, Freedmen, and Abandoned Lands, better known as the Freedmen's Bureau. The Freedmen's Bureau was set up toward the end of the Civil War in March 1865 to provide immediate relief to freed people as well as to poor whites uprooted by the war, but its mission expanded to a large-scale and often contradictory effort to protect freed people's civil and political rights, to revive agricultural production in the South, and to turn former slaves into free wage laborers (often on the same plantations they used to work on as slaves) (Goldberg 2007). The Freedmen's Bureau can be understood as an early, although ultimately failed, attempt to (unevenly) integrate African Americans into a Northern capitalist order as both citizens and self-dependent but docile wage laborers. Despite its checkered track record, the Freedmen's Bureau started from the assumption that African Americans could be turned into self-dependent citizens and workers. This is perhaps why Du Bois (2007, 179) praised the Bureau as "the most extraordinary and far-reaching institution of social uplift that America has ever attempted," despite the fact that it also frequently served as an instrument for disciplining black labor (Goldberg 2007, 40–2). The simple fact that freed people could now enter labor contracts, even if they were extremely harsh and, more often than not, entered into under highly coercive conditions, was a first step toward less expropriatory and more exploitative labor relations. In 1872, Southern white supremacists ultimately succeeded in swaying Congress to terminate the Freedmen's Bureau. The Black Codes were replaced by the Jim Crow laws in 1877. The Jim Crow laws contained many provisions that were frequently as, if not more, oppressive than the original Black Codes. Besides mandating strict racial segregation and brutally punishing any infraction against whites, Jim Crow laws also ensured African Americans' continuing availability as an expropriable agricultural labor force

through debt peonage and convict leasing. This brutal colonial regime of racist oppression and expropriation was ultimately backed by both legal and extra-legal violence in the form of lynching (Marable 1983).

A neocolonial "entanglement of capitalist accumulation processes with a racial/ethnic hierarchy" persisted after the abolition of slavery and the end of Jim Crow (Grosfoguel 2003). Although African Americans (as well as other racialized groups who are considered citizens) have struggled for and ultimately won formally equal rights, although there now is a sizable black professional class, and although the United States elected its first black president, racial divisions of labor are still firmly in place. Michael Dawson makes this point forcefully:

> Whether as slaves during one epoch; as colonized workers, sharecroppers, workers within segregated/segmented labor markets throughout the twentieth century; or, as disposable workers in this neoliberal era—those marked by race within the United States and elsewhere have been denied a basic feature of capitalism—access to labor markets or, if granted access, the ability to sell their labor on an equal basis.
>
> (Dawson 2016, 150)

Indeed, in socio-economic terms, particularly with regard to their unequal access to labor markets, the racialized poor in the United States still find themselves in a neocolonial situation.

Surveillance plays a key role in securing this neocolonial situation. Practices of surveillance not only grant or deny access to (segmented) labor markets but also facilitate exploitation if access is granted (see Fuchs 2013 for a discussion of capitalist labor force and market surveillance). Even after the abolition of colonial labor control and the extension of formal legal equality, surveillance continues to have a disproportionate impact on the racialized poor. Surely, in a context of formal legal equality, racial difference itself can no longer legitimate the use of intrusive surveillance and authoritarian labor control. However, discourses of criminality and welfare dependence are now mobilized for legitimating the disproportionate surveillance of the racialized poor. In short, racializing surveillance continues to play a key role in reproducing a racial division of labor by either excluding the racialized poor from the labor market through criminal justice sanctions or including them in the lowest rungs of the labor market through welfare-cum-workfare programs.

Neocolonial racialization through welfare surveillance

The rise of the modern administrative state is closely entwined with the development of various techniques for gathering knowledge on "the processes of the population," many of which were honed and developed in settler colonial and colonial settings (Gordon 1991, 20; see also Foucault 1991; Giddens

1987). Hence, the rise and expansion of state-administered welfare also went hand-in-glove with an extension and intensification of surveillance. The moment the state took on the task of supporting those who were deemed unable to support themselves, people in need had to be identified, their level of need had to be assessed, and, above all, their eligibility had to be ascertained. From the inception of modern state welfare, surveillance served the primary purpose of making a distinction between those eligible for public support and those who must fend for themselves. In the United States, this distinction between the deserving and the undeserving poor has always been profoundly racialized. Indeed, welfare has been and continues to be "one of the most racialized of political domains" in the United States (Brown 2013, 395).

The history of modern poor relief is closely tied to questions of social control, on the one hand, and the constitution and maintenance of labor markets, on the other (Polanyi 1957; Dean 1991; Piven Fox and Cloward 1993). In fact, through its emphasis on means-testing and the principle of less eligibility, the 1834 Poor Law Amendment Act in Britain marked the constitution of the first national labor market and was thus key for the expansion of industrial capitalism (Polanyi 1957; Dean 1991). Both the means test and the principle of less eligibility are major drivers of welfare surveillance. The means test hinges on determining who actually needs and deserves poor relief. Today, means-tested welfare refers to programs that are only targeted at particular populations—mainly those whose income is below a certain threshold. There are other forms of welfare, such as insurance-based programs, that potentially benefit a larger portion of the overall population. In the United States, in particular, the very term welfare now denotes primarily means-tested forms of poor relief. We should note that this is wildly inaccurate because the middle classes are still the prime beneficiaries of welfare spending (Ward 2005, 244–7; see also Wacquant 2009). Means testing entails gathering vast amounts of information on those seeking public support in order to determine whether they are eligible. Application forms and interviews with case managers require very detailed information about applicants' family situation, health, job history, and even sometimes sexual history.

The principle of less eligibility, first formulated by Jeremy Bentham, moreover, stipulates that public relief ought to be less attractive than the most onerous and most badly paid work (see Sieh 1989, 162). Less eligibility is the primary source of welfare stigma. Welfare applicants and recipients are subjected to various rituals of humiliation, which often take the form of intrusive surveillance, including home visits, mandatory drug testing, etc. The main justification for intrusive welfare surveillance is, however, the prevention of welfare fraud. Ironically, welfare fraud is a structural necessity, while its prevalence is massively overstated. A number of studies found that levels of fraud are very similar across different government programs (see Gilliom 2001). Welfare recipients are, thus, as likely—or as unlikely—to cheat as, let's say, recipients of farm subsidies. Yet welfare recipients are subject to far more

intrusive levels of surveillance than recipients of farm subsidies. It is thus probably fair to say that surveillance is largely used for making welfare less eligible. At the same time, welfare benefits alone are barely sufficient to allow a household to make ends meet. Most welfare recipients, therefore, rely on some sort of unreported income, which means that they are living in constant fear of being found out and of having their benefits cut or even terminated as a result (Gilliom 2001; Wacquant 2009).

Welfare surveillance has been expanded enormously in response to the growth of the welfare state and the extension of relief to minorities, especially African Americans, in the wake of President Johnson's Great Society programs and the successes of the civil rights and welfare rights movements (Gilliom 2001, 26–7; see also Piven Fox and Cloward 1993; Ward 2005). Welfare surveillance is geared toward determining eligibility, preventing fraud, and deterring people from applying. To illustrate some of the surveillance practices that welfare applicants and recipients are subject to, I will use the example of Temporary Assistance for Needy Families (TANF), which replaced Aid to Families with Dependent Children (AFDC) as part of Clinton's 1996 welfare reform. TANF provides cash benefits and is primarily targeted at poor single mothers. The 1996 welfare reform pretty much abolished welfare as an entitlement. TANF comes with a five-year lifetime limit. Moreover, TANF recipients have to find work within two years of receiving benefits. Thus, TANF is a form of workfare pushing the poor—in this case primarily single mothers—into the lowest rungs of the labor market. At the same time, states and even counties can set even more stringent eligibility criteria and conditionalities than the ones stipulated by the federal government. As a consequence, surveillance practices vary enormously between jurisdictions. TANF consists of a multistage and multiday application process, including interviews, group sessions, and assessments of employability. During this process, applicants have to answer questions regarding needs, psychological well-being, resources, paternity information about children, etc. Moreover, they have to back up their answers with a lot of additional third-party information. All information is electronically stored and compared with federal, state, and commercial databases in order to determine eligibility and identify both fraudulent information and duplicate applications. Some jurisdictions even obtain debit card information to track their recipients' spending habits. Many jurisdictions require fingerprints and photographs. TANF also enforces child support. Thus, if the paternity of children is contested, TANF recipients have to agree to DNA testing. A number of jurisdictions also conduct home visits. And some jurisdictions also mandate drug testing (Gilman 2008). If benefits are awarded, recipients are responsible for keeping their information up to date. Failure to do so may result in sanctions such as cuts to or even cancellation of their benefits.

Welfare surveillance does not affect only people of color, but the massive expansion of welfare surveillance coincided with the extension of poor relief

to people of color. In addition, in public discourse, welfare—often narrowly viewed as encompassing only means-tested programs benefitting the poor—is often closely associated with blackness (Wacquant 2009; Roberts 2014a; see also Roberts 2014b). The replacement of AFDC by TANF is a case in point. As Deborah Ward puts it:

> Race and racial distinctions had become so embedded in our welfare state that changes in recipient demographics—perceived or real, justified or not—led to the dismantling of a long-standing system, and this dismantling both reflected and reaffirmed the racial division between the worthy and the unworthy poor.
>
> (Ward 2005, 31)

The abolishment of poverty relief as an entitlement through Clinton's 1996 Personal Responsibility and Work Opportunity Act (PRWOA) marked the culmination of a racial backlash to the expansion of relief to poor African Americans. But there could only be a racial backlash because poor relief had always been racialized.

Virginia Eubanks suggests that welfare surveillance constitutes a form of poverty profiling: "Like racial profiling, poverty profiling targets individuals for extra scrutiny based not on their behavior but rather on a personal characteristic: living in poverty" (Eubanks 2018, 158). Yet, in my view, welfare surveillance must be viewed rather as racialized class profiling, whereby class-specific behaviors are classified as deviant so that particular populations can be slated for extra scrutiny and punitiveness without violating the principle of legal formal equality. These behaviors are class specific because they are associated with extreme poverty, but because people of color are disproportionately affected by poverty—especially by its most extreme forms—welfare surveillance also disproportionately targets people of color and thus inevitably intersects with racial profiling.

Eubanks also makes the compelling argument that "[r]elief institutions are machines for undermining the collective power of poor and working-class people, and for producing indifference in everyone else" (Eubanks 2018, 178). Relief institutions indeed serve to pacify poor and working-class people while ensuring their continuing availability for exploitation and expropriation. However, the pacification of the working class is also effected through divisions within the working class, and the very distinction between the poor and the working class is both product and producer of these divisions. Distinctions between the poor and the working class, and between the deserving and undeserving poor, moreover, reinforce racial divisions, because "[t]hroughout welfare state development, *deserving* is a code word for 'white'" (Ward 2005, 241).

Welfare surveillance constitutes a political technology for punitively managing and racializing an economically disposable population. Enforcing less

eligibility through intrusive surveillance ultimately reinforces the stigma attached to means-tested welfare. In its efforts to sniff out even the smallest infraction of the onerous rules of means-tested welfare programs and through its rituals of humiliation, welfare surveillance serves to push welfare applicants into the lowest rungs of the labor market, where their labor power is often not only exploited but also expropriated. The work requirements now attached to welfare programs, such as TANF, facilitate capitalist accumulation through the provision of cheap labor, while the meager financial transfer payments serve to (partially) address some of the social dislocations caused by capitalist accumulation. As a consequence, welfare surveillance produces and reproduces racial divisions and hierarchies within the US working class. Welfare surveillance stigmatizes and ultimately racializes welfare recipients while obscuring the colonial genealogy of racializing state surveillance. Welfare surveillance brings about the hypervisibility of welfare applicants and recipients for the administrative state as well as in public discourse (through media representations), while the neocolonial racializing effects of these surveillance practices remain largely invisible. Furthermore, welfare surveillance renders the individual failings of its targets transparent while obscuring structural inequities that create the demand for public relief in the first place. In short, welfare surveillance has emerged as a central neocolonial technology of racialization in the context of formal legal equality and professed colorblindness.

Conclusion

In capitalist social formations a key function of surveillance-as-social-sorting is to secure the conditions for capitalist accumulation. This occurs through the classifications and ultimate division of those people who comprise the class that produces the value necessary for capitalist accumulation: the working class. Making distinctions between those whose labor can be expropriated, those who are "merely" exploited, and those whose labor is viewed as disposable; more finely grained classifications around the productivity of individual and/or collective units of labor within particular industries or places of production; as well as distinctions between the worthy and the unworthy poor have divided and continue to divide the working class.

In a *settler colonial* and *neocolonial* context, such as the United States, these distinctions are also always both racialized and racializing. Rationalities and practices of racializing surveillance, from chattel slavery to contemporary poverty governance, have thus been central to the reproduction of divisions within the US working class. However, rationalities and practices of racializing surveillance have also changed, particularly in response to various forms of resistance by racialized populations. As a result of the struggles of racialized populations, particularly the civil rights movement,

racializing surveillance now operates in the context of formal legal equality and professed colorblindness, and thus has to obscure both its colonial genealogy and its racializing effects. But, in spite of these highly significant changes, surveillance-as-social-sorting continues to divide the working class in order to extract as much value out of labor as possible as well as to prevent, control, and pacify working-class resistance.

References

Balibar, Étienne. 1991a. "Class Racism." In *Race, Nation, Class: Ambiguous Identities*, edited by Etienne Balibar and Immanuel Wallerstein, 204–16. London: Verso.

Balibar, Étienne. 1991b. "From Class Struggle to Classless Struggle." In *Race, Nation, Class: Ambiguous Identities*, edited by Étienne Balibar and Immanuel Wallerstein, 153–84. London: Verso.

Baptist, Edward E. 2014. *The Half Has Never Been Told: Slavery and the Making of American Capitalism*. New York: Basic Books.

Bass, Sandra. 2001. "Policing Space, Policing Race: Social Control Imperatives and Police Discretionary Decisions." *Social Justice* 28: 156–76.

Brown, Hana E. 2013. "Racialized Conflict and Policy Spillover Effects: The Role of Race in the Contemporary U.S. Welfare State." *American Journal of Sociology* 119(2): 394–443.

Browne, Simone. 2015. *Dark Matters: On the Surveillance of Blackness*. Durham: Duke University Press.

Brucato, Ben. 2014. "Fabricating the Color Line in a White Democracy: From Slave Catchers to Petty Sovereigns." *Theoria: A Journal of Social & Political Theory* 61(141): 30–54.

Dawson, Michael C. 2016. "Hidden in Plain Sight: A Note on Legitimation Crises and the Racial Order." *Critical Historical Studies* 3(1): 143–61.

Dean, Mitchell. 1991. *The Constitution of Poverty: Towards a Genealogy of Liberal Governance*. London: Routledge.

Du Bois, W.E.B. 2007. *Black Reconstruction in America: An Essay Toward a History of the Part Which Black Folk Played in the Attempt to Reconstruct Democracy in America, 1860–1880*. Vol. 6 of *The Oxford W. E. B Du Bois*, edited by Henry Louis Gates Jr. Oxford: Oxford University Press.

Eubanks, Virginia. 2018. *Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor*. New York: Picador.

Federici, Silvia. 2004. *Caliban and the Witch: Women, the Body and Primitive Accumulation*. New York: Autonomedia.

Fields, Karen E., and Barbara J. Fields. 2014. *Racecraft: The Soul of Inequality in American Life*. London: Verso.

Foucault, Michel. 1991. "Governmentality." In *The Foucault Effect: Studies in Governmentality*, edited by Graham Burchell, Colin Gordon, and Peter Miller, 87–104. Chicago: The University of Chicago Press.

Fraser, Nancy. 2014. "Behind Marx's Hidden Abode: For an Expanded Conception of Capitalism." *New Left Review* 86(March–April): 55–72.

Fuchs, Christian. 2013. "Political Economy and Surveillance Theory." *Critical Sociology* 39(5): 671–87.

Giddens, Anthony. 1987. *The Nation State and Violence*. Berkeley: University of California Press.
Gilliom, John. 2001. *Overseers of the Poor: Surveillance, Resistance, and the Limits of Privacy*. Chicago: University of Chicago Press.
Gilman, Michele E. 2008. "Welfare, Privacy, and Feminism." *University of Baltimore Law Forum* 39(1): 1–24.
Goldberg, Chad Alan. 2007. *Citizens and Paupers: Relief, Rights, and Race, from the Freedman's Bureau to Workfare*. Chicago: The University of Chicago Press.
Gordon, Colin. 1991. "Governmental Rationality." In *The Foucault Effect: Studies in Governmentality*, edited by Graham Burchell, Colin Gordon, and P. Miller, 1–52. Chicago: University of Chicago Press.
Grosfoguel, R. 2003. *Colonial Subjects: Puerto Ricans in a Global Perspective*. Berkeley: University of California Press.
Hadden, Sally E. 2001. *Slave Patrols: Law and Violence in Virginia and the Carolinas*. Cambridge: Harvard University Press.
Johnson, Walter. 2013. *River of Dark Dreams: Slavery and Empire in the Cotton Kingdom*. Cambridge: Harvard University Press.
Lyon, David. 2003. "Introduction." In *Surveillance as Social Sorting: Privacy, Risk, and Digital Discrimination*, edited by David Lyon, 13–30. London: Routledge.
Marable, Manning. 1983. *How Capitalism Underdeveloped Black America: Problems in Race, Political Economy and Society*. Boston: South End Press.
Marx, Karl. 1976. *Capital: A Critique of Political Economy Vol. I*. London: Penguin Books.
Oakes, James. 2016. "Capitalism and Slavery and the Civil War." *International Labor and Working-Class History* 89: 195–220.
Pinderhughes, Charles. 2011. "Toward a New Theory of Internal Colonialism." *Socialism and Democracy* 25(1): 235–56.
Piven Fox, F., and Richard A. Cloward. 1993. *Regulating the Poor: The Function of Public Welfare*. New York: Vintage.
Polanyi, K. 1957. *The Great Transformation: The Political and Economic Origins of Our Time*. Boston: Beacon Press.
Quijano, Anibal. 2000. "Coloniality of Power, Eurocentrism and Latin America." *Nepantla: Views from the South* 1(3): 533–80.
Rinehart, Nicholas T. 2016. "The Man That Was a Thing: Reconsidering Human Commodification in Slavery." *Journal of Social History* 50(1): 28–50.
Roberts, Dorothy. 2014a. "Complicating the Triangle of Race, Class and State: The Insights of Black Feminists." *Ethnic and Racial Studies* 37(10): 1776–82.
Roberts, Dorothy E. 2014b. "Child Protection as Surveillance of African American Families." *Journal of Social Welfare and Family Law* 36(4): 426–37.
Rosenthal, Caitlin. 2018. *Accounting for Slavery: Masters and Management*. Cambridge, MA: Harvard University Press.
Sieh, Edward W. 1989. "Less Eligibility: The Upper Limits of Penal Policy." *Criminal Justice Review* 3(2), 159–83.
Smith, Andrea. 2015. "Not-Seeing: State Surveillance, Settler Colonialism, and Gender Violence." In *Feminist Surveillance Studies*, edited by Rachel E. Dubrofsky and Shoshana Amielle Magnet, 21–38. Durham, NC: Duke University Press.
Veracini, Lorenzo. 2011. "Introducing *Settler Colonial Studies*." *Settler Colonial Studies* 1(1): 1–12.

Wacquant, Loïc. 2009. *Punishing the Poor: The Neoliberal Government of Social Insecurity*. Durham, NC: Duke University Press.
Wallerstein, Immanuel. 1991a. "Class Conflict in the Capitalist World-Economy." In *Race, Nation, Class: Ambiguous Identities*, edited by Etienne Balibar and Immanuel Wallerstein, 115–24. London: Verso.
Wallerstein, Immanuel. 1991b. "The Ideological Tensions of Capitalism: Universalism Versus Racism and Sexism." In *Race, Nation, Class: Ambiguous Identities*, edited by Etienne Balibar and Immanuel Wallerstein, 29–36. London: Verso.
Wallerstein, Immanuel. 2004. *World-Systems Analysis: An Introduction*. Durham, NC: Duke University Press.
Ward, Deborah E. 2005. *The White Welfare State: The Racialization of U.S. Welfare Policy*. Ann Arbor, MI: University of Michigan Press.
Wolfe, Patrick. 2006. "Settler Colonialism and the Elimination of the Native." *Journal of Genocide Research* 8(4): 387–409.

Part II

Transparency and trust as institutional constraints and critical praxis

Chapter 6

Secrecy versus transparency in the US national security surveillance state

Paweł Laidler

Introduction

In 2013, Edward Snowden, the former National Security Agency (NSA) contractor, copied classified documents that revealed the scope of US government surveillance. The leaked documents referred to secret programs that enabled the collection of metadata on foreign and American citizens, and to the interception of domestic internet communications leading to the creation of an enormous database by government surveillance agencies with access to personal communications, including emails, social network entries, audio and video chats, visited websites, and medical and financial records (Olmsted 2018; Greenwald 2014; Gurnow 2014). Snowden's revelations ignited social and political discussion concerning the scope of government surveillance powers, as well as the impact of the secret NSA programs on the privacy of American citizens and on various potential violations of the constitution by the authorities (Goldfarb 2015; Lyon 2015; Kitrosser 2015). The substance of the leaked documents ignited an academic debate on the functioning of the US foreign and domestic surveillance system and its impact on the state of democracy and the rule of law.

Research has been conducted with regard to both national security and domestic surveillance in the United States, with a focus on the powers of institutions responsible for conducting or controlling surveillance procedures, as well as on the conflict this has caused between freedom and security (Farrell and Newman 2019; Johnson 2018; Keller 2017; Goldfarb 2015; Lester 2015; Angwin 2014) and between secrecy and transparency (Graham 2017; Frost 2017; Kitrosser 2015; Arnold 2014). It is no surprise to learn that the NSA was the most studied institution (Hayden 2018; Edgar 2017), but important analysis has also been done with regard to the surveillance activities of the Central Intelligence Agency (CIA) (Johnson 2018; Prados 2014) and the Federal Bureau of Investigation (FBI) (McCabe 2019). Studies focusing on concrete surveillance institutions have had at least one thing in common: a broader reference to the role of the executive branch of government in building,

DOI: 10.4324/9781003120827-9

preserving, and defending a complex system of secret surveillance aimed at providing national security.

Unlike the case of post-9/11 legislation and executive action, when the main theme of the public debate focused on the clash between freedom and security (Herman 2011; Posner and Vermeule 2006; Davis and Silver 2003), the post-Snowden era has been marked by a more frequent reference to the clash between two other important features of a surveillance state: secrecy and transparency. The debate has raised questions concerning the excessiveness of the US secrecy regime with respect to surveillance policies, appealing to the necessity of imposing broader transparency measures which would restore democracy and enable a proper oversight of the government's actions (Edgar 2017). Transparency has become the most demanded value, treated by many as a remedy for the overwhelming system of excessive secrecy and over-classification (Goldfarb 2015; Kitrosser 2015).

The problem the chapter addresses concerns the struggle between secrecy and transparency rooted in the institutional and systemic mechanisms of the separation of powers and the checks and balances system in the United States. I argue that in the area of national security surveillance, the adherence of the executive toward secrecy outweighs transparency as promoted by Congress and defended by the judicial branch. It seems that—not despite but because of the separation of powers doctrine—there is more secrecy rather than transparency in US national security surveillance, which may lead to an argument about the illusion of transparency within the national security framework. The illusion, understood as a difference between the reality and the perception of the reality, in this context means that although the government has undertaken several legal and political measures to achieve the socially demanded level of transparency, the result has been more a matter of perceived than actual change, due to the engagement of all branches in the defense of secret surveillance. The chapter analyzes the policies of these branches toward the conflict between secrecy and transparency in the area of national security surveillance in the pre- and post-Snowden eras. Due to the fact that congressional legislation, executive action, and judicial interpretation of surveillance measures are intertwined, the empirical analysis is conducted in chronological order, focusing on the most important issues occurring before and after 2013.

For the purpose of the study, surveillance is defined as "the collection of information in order to manage control" (Lyon 2015, 3) with "the intention to protect, understand … or influence groups or individuals" (Kuntze 2018, 45). Considering government surveillance, it seems obvious that in a democratic state there should be a mutual relationship based on control: the authorities control the society, and the society controls the authorities, although the character of the two types of control is quite different and is conducted with varying intensity. By managing control, the surveilling party influences the lives of surveilled subjects, often justifying it by the need to protect them; however, the scope of this protection is determined by means of surveillance

and its more (or less) secretive character. The biggest challenge concerns the level of understanding among the subjects of the surveillance relationship, as it often has an impact on the scope of the accountability of the surveillance programs. This can be seen especially in government surveillance, where the society, aware of the authorities' need to impose certain measures of surveillance, is reluctant to approve the culture of secrecy in which the surveillance state is shrouded (Arnold 2014). In what follows, government surveillance shall refer to national security surveillance, that is, US foreign intelligence surveillance and other surveillance activities conducted by the intelligence community, as well as by the institutions involved in such activities (Friedman and Hansen 2012). Although the 2013 leaks revealed the scope of US surveillance of foreigners, including political leaders, and thus affecting transatlantic relations (Cole et al. 2017), the analysis focuses mainly on those aspects of national security surveillance which were directed toward American citizens, raising the problem of constitutionality and governmental accountability.

In discussions of national security surveillance, transparency should be understood as oversight and control of the activities of institutions involved in conducting government surveillance, rather than the full disclosure of information concerning surveillance programs and their outcomes. In order to pursue the politics of national security effectively, the government must be allowed to act in partial secrecy and to select the means necessary to provide the expected level of safety to its citizens (Cain 2015, 41). But the lack of control from oversight institutions may lead to the abuse of power and to violations of the rights and freedoms of individuals, who demand a certain level of transparency from their government. Such a level could be reached, for example, by legislation limiting the scope of national security surveillance, as well as by institutional solutions providing for a system of effective oversight imposed on different levels and in different relations (Eskens et al. 2015, 8). From the perspective of the separation of powers, control over executive actions should be conducted by both Congress and the judiciary, despite the different character of their functioning. It seems that without the people's knowledge of the scale and character of government surveillance, resulting from the effects of this congressional and judicial oversight, there is neither democratic accountability nor the proper functioning of the constitution as a fundamental guarantee of individuals' rights.

The core question about the relation between secrecy and transparency is not new to surveillance studies and has been examined from various perspectives (Moses and de Koker 2017; Lyon 2014; Ball et al. 2012; Friedman and Hansen 2012; Theoharis 2011; Herman 2011). The methodology of political and legal sciences applied here, based on historical institutionalism and systemic analysis, will focus on the character of the separation of powers doctrine, which evolved along with the growth of the secret surveillance state. The system revealed by Snowden, who uncovered a secret web of programs conducted by the federal executive and uncontrolled by Congress and the

courts, affected the checks and balances system (Goldfarb 2015; Arnold 2014; Greenwald 2014). Some researchers placed the responsibility for the existence of the secret surveillance state on concrete examples in specific presidential administrations (Graham 2017; Glennon 2015; Theoharis 2011); some tried to find the explanation for the temporary violation of the rights and freedoms of individuals in a state of emergency (Edgar 2017); and others have explained that the executive acted in accordance with the Constitution (Calabresi and Yoo 2012). These research findings confirmed conflicting arguments raised by politicians, journalists, and American citizens, who presented different approaches toward the interpretation of the constitutional powers of the government with respect to its surveillance competences. My argument focuses mainly on the scope of the separation of powers doctrine, which is the key to understanding why the transparency of national security surveillance has been an illusion, rather than a reality.

National security surveillance pre-Snowden

The Cold War era

The national security paradigm has always been rooted in the American political system, becoming an indispensable element of the policies of most presidential administrations. It has been systematically used since the late 1940s, usually applied by the executive with regard to foreign policy (Theoharis 2011, 133–5). The separation of powers was not in the spotlight of early Cold War national security legislation, but Congress was aware that the expansion of executive powers should be somehow controlled by other government branches. The National Security Act of 1947 placed theoretical limitations on the functioning of the intelligence community, by requiring the president to keep Congress "fully and currently informed of the intelligence activities of the United States, including any significant anticipated intelligence activity" (*National Security Act* 1947). The law confirmed congressional oversight over intelligence activities, but it was obvious that the scope of control and transparency would depend on a president's will.

Five years later, President Harry Truman issued a top-secret directive establishing the NSA, responsible for monitoring communications out of the United States (Glennon 2015, 12–13). In order to achieve national security goals, the government operated several secret surveillance programs aimed at both foreign and national subjects. Institutionally, all three major agencies, the NSA, the CIA, and the FBI, were involved in the process of protecting national security during the Cold War era, and their activities were held far from public scrutiny due to the imposition of a broad secrecy system (Edgar 2017). Surveillance measures quickly became an effective tool of government agencies' control of the communications and activities of US persons involved in "subversive activities" (Dudziak 2000). At the same time, the NSA

was involved not only in counterintelligence but strictly collaborated with both the CIA and the FBI in sharing information about foreign and domestic threats to national security (Keller 2017).

The truth about several secret surveillance programs was revealed during the investigations conducted by congressional oversight committees established in the mid-1970s: the Pike Committee (House) and the Church Committee (Senate). The investigations focused on the secret and—in many respects—illegal programs conducted by the CIA and NSA, as well as on the FBI's wiretapping of politicians and journalists (Prados 2014). The Church Committee's investigation, followed by a series of reports, not only disclosed the scope of national security surveillance for domestic reasons but also raised concerns about the character of the separation of powers with regard to national security surveillance. The Committee found that "intelligence activities were essentially exempted from the normal system of checks and balances," decreasing the constitutional accountability of the executive, which had an exclusive role in conducting national security policies, including surveillance of US citizens. The report indicated that the executive agencies applied excessive secrecy in their conduct of surveillance programs in order to limit congressional oversight and the knowledge of the people targeted by government due to their political beliefs (*Church Committee Report* 1976).

As a result, Congress established two stable oversight bodies whose role was to control foreign intelligence and counterintelligence activities and expanded the powers of the justice committees of both houses to oversee the actions of domestic surveillance agencies (Glennon 2015; Solove 2011). Furthermore, in 1978 Congress implemented the Foreign Intelligence Surveillance Act (FISA), introducing higher judicial scrutiny over national security surveillance measures and establishing the Foreign Intelligence Surveillance Court (FISC) to grant warrants for the surveillance of those who were suspected of being foreign agents (*Foreign Intelligence Surveillance Act* 1978). The means of appointment of FISC judges, as well as the length of their tenure and the necessity to close the court's proceedings to the public, were aimed at producing a system of judicial check on the activities of institutions imposing surveillance, without violating the sensitive character of the cases discussed. On the other hand, the special court had to operate on the basis of information and documents provided solely by the executive, which made its proceedings and decision-making process dependent on the value and relevance of the shared data (Glennon 2015, 45). Theoretically, transparency was weakened by institutional secrecy.

The analysis of the legislative and institutional effects of the committees' investigations proves that Congress did not want to strip the executive of the power to exercise its constitutional goal of providing security to US citizens. The secrecy rule guiding the FISC procedures, and the discretionary power of the executive to control the content of shared information with the judges, served the purposes of national security. None of the congressional acts or

institutional changes within the government significantly limited the scope of national security surveillance. Furthermore, the Supreme Court confirmed—or at least did not neglect—the leading role of the executive in implementing and operating national security policy, even if it resulted in violations of the civil rights of Americans. The reference to the privilege of state secrets in the dispute over the crash of a military plane (*United States v. Reynolds* 1953), lack of ripeness in a case concerning US Army surveillance of American citizens (*Laird v. Tatum* 1972), or the limitation of First Amendment rights during the Red Scare era of the early 1950s (*Dennis v. United States* 1951) may serve as good examples of the strengthening of the government's powers for national security reasons.

The post-9/11 era

The secrecy of national security surveillance was again at the center of US political debate after the terrorist attack of 9/11, when Congress implemented antiterrorist legislation. The USA Patriot Act became the main source of power for the federal institutions responsible for law enforcement and intelligence activities (Smith and Hung 2010). Among various provisions determining the relations between executive agencies, the Act introduced National Security Letters (NSL), issued without judicial control by the FBI, and roving wiretaps focusing on individual persons rather than the devices which they used (*USA Patriot Act* 2001). Generally, Congress agreed to expand executive powers by delegating vast competences to executive agencies, referring to the times of emergency (Akerman 2006), which allowed the George W. Bush administration to justify its national security policy.

Among several measures undertaken by the administration was a secret program, called Stellar Wind, which became public due to a press leak in 2005 (Fisher 2013, 251–2), as a part of a broader Terrorist Surveillance Program (TSP) implemented in 2002 (Kuntze 2018, 82). Its main purpose was to collect international phone calls and emails of targets suspected of organized terrorism, but in addition to data on foreign nationals the program allowed the NSA to intercept and store metadata from telephone and internet providers, including information about the private communications of US citizens (Edgar 2017, 40). Importantly, Stellar Wind not only lacked the approval of Congress and the judiciary, including the FISC, but it was also based on an internal memorandum created by the Office of Legal Counsel (OLC). The document assumed that presidents—based on unitary executive theory—had almost unlimited power in determining the scope of government surveillance (Posner and Vermeule 2006). The theory claimed that the president, as commander-in-chief, had the power to initiate any surveillance program, because all executive power belonged to the president, especially in times of war and emergency (Goldfarb 2015). Apart from legitimizing Stellar Wind and other initiatives of the TSP, the memo indicated that the lack of

control by other branches of government was justified by the necessity to keep the programs secret (Lester 2015).

In 2007, the government decided to launch a new national security surveillance program, called PRISM, to monitor the data of the users of the most important internet providers. As a result, in order to provide information necessary to limit the terrorist threat the NSA secretly collected, stored, and analyzed billions of items of data on US citizens (Edgar 2017, 5). In contrast to Stellar Wind, PRISM was based on congressional authorization, Section 702 of the Protect America Act (2007), and the FISA Amendments Act (2008). The legislation permitted the government to intercept communications inside the country connected with foreign suspects of terrorism, but it had to be approved by the FISC, which applied minimization rules in order to protect the rights of American citizens. Still, the reasonable belief standard substituted the former probable cause standard, thus making it easier for the government to obtain FISC approval.

According to Section 702 of the 2007 Act, the government also conducted so-called upstream collection, which focused only on domestic communications by intercepting information from major internet cables and switches in the flow of communications between communication service providers (Edelson 2016, 120). The executive also used the amended Section 215 of the Patriot Act to intercept data from domestic bulk collection of international and domestic telephone records. It guaranteed thousands of numbers analyzed with regard to one seed number, providing for the almost infinite collection of data concerning US persons (*USA Patriot Act Additional Reauthorizing Amendments of 2006*).

All these programs introduced some level of control over the surveillance activities of the executive. After 2006 especially, Congress and the courts became more actively involved in the process of overseeing national security surveillance measures imposed by the NSA or FBI. Still, national security surveillance, or rather dataveillance (Lyon 2014; van Dijck 2014), was imposed so broadly that there was no way for the oversight institutions to exercise their powers effectively. The collection of the electronic data of foreign and US citizens by government agencies was often conducted without the approval of FISC, or based on a general acceptance of the operation of certain surveillance programs by the court (Glennon 2015). Despite theoretically broader congressional and judicial control of the surveillance measures, there was a lot of criticism that too much information was kept secret, thus leading to potential overuse of executive powers (Herman 2011; Romero and Temple-Raston 2007).

Barack Obama's win in 2008 gave hope to his supporters of a change in the national security surveillance system, especially with regard to the scope of powers of the executive, and the level of transparency (Olmsted 2018, 220). As a Senator, Obama had criticized the administration's accumulation of powers for the purpose of the war on terror, but he did not condemn any

concrete NSA surveillance program (Edgar 2017, 51–52). As a presidential candidate he referred to the greater transparency of the government's surveillance programs (Graham 2017, 180–181). The fact is that as president, Obama modified, and even expanded, some of the surveillance programs initiated by the Bush administration. He decided to continue programs based on Section 215 of the Patriot Act, approved the continuation of PRISM based on Section 702 of FISA, actively used the NSL, and signed the extension of the FISA Amendments Act (Graham 2017; Glennon 2015). It seems as if the main purpose of Obama's administration was to adapt the law to serve the purposes of the politics of surveillance rather than impose a new system of transparency.

National security surveillance post-Snowden

Soon after the Snowden revelations, President Obama insisted on conducting a broad investigation of NSA surveillance, appointing a Review Group on Intelligence and Communications Technology. It recommended several reforms, from terminating the existing surveillance programs to preserving a limited impact of the NSA on the collection of the data necessary to conduct effective surveillance against potential terrorists (Kitrosser 2015, 338). In early 2014, the White House issued a directive that clearly stated that "the collection of signals intelligence [was] necessary for the United States to advance its national security and foreign policy interests and to protect its citizens and the citizens of its allies and partners from harm" (*Presidential Policy Directive* 2014, 28). As a confirmation of the differences between the rhetoric and activities of the presidential administration, Obama's government denied access to several requests for information about government actions (Keller 2017, 31).

At the same time, Congress initiated a discussion over legislative reform that would legalize the existing surveillance programs. The Privacy and Civil Liberties Oversight Board (PCLOB) produced a report that concluded that the NSA's program of bulk collection of phone data raised several constitutional issues concerning both the scope of executive powers and potential violations of individuals' freedoms. The report determined certain NSA surveillance programs as illegal and ineffective, thus raising several doubts concerning their continuation (*The Report of the PCLOB*). With regard to the bulk collection of phone metadata, the Board suggested that the program should be terminated, determining also that the way to intercept the communications stored by telecommunications companies was to obtain the approval of FISC for every individual case of reasonable surveillance (Graham 2017, 197–8).

Finally, in June 2015, the USA Freedom Act (2015) was enacted, thus ending the government surveillance program of bulk collection of metadata. The Act forced the government to obtain FISC warrants in order to conduct

the collection of data from telecommunications companies for foreign intelligence reasons. For the purpose of preventing previous procedural flaws, judges received expert support from technical and privacy advisers, and their legal interpretations became public. Important change was made with respect to the records collected by telecommunications companies, which stored them instead of the NSA; however, the agency could gain access to these records given FISC approval. The Act also limited the NSA's access to targeted individuals' phone records and the records of the phone numbers associated with them (Graham 2017, 198; Olmsted 2018, 223).

Despite strengthening the checks and balances system with regard to judicial control of government surveillance, and ending the bulk collection of metadata, no serious changes were introduced to the institutional and structural aspects of surveillance programs. Actually, the bulk collection of metadata ended six months after the implementation of the Freedom Act, as the presidential administration asked FISC for a transition period that would allow the analysts to end their work (Edelson 2016, 116). Still, the government did not suggest the creation of any new oversight system, but a strengthening of the existing one with effective control of congressional committees and FISC, and the support of such institutions as PCLOB. Analysis of the legal regulations governing the functioning of the oversight system proves, however, that the scope of control of the surveillance measures depended on the will of the executive, which could easily hide behind national security arguments. And even the publication of annual transparency reports by the NSA did not change the feeling that there was more of a rhetoric of openness rather than real transparency (Alloa and Thoma 2018).

Apart from legislative changes, Snowden's actions also had an impact on decisions made by the judicial branch. Until 2013 the courts usually applied the state secrets privilege in lawsuits filed by US citizens who believed that government surveillance violated their constitutional rights. Both the Bush and Obama administrations defended the challenged programs, referring to the necessity to protect national security surveillance, and the courts repeatedly declared the lack of standing of the challengers. Even in 2013 such verdicts were announced by the Supreme Court, where the claims were defined as based on "speculation and on a predicted chain of events that might never occur" (*Clapper v. Amnesty International* 2013). However, Snowden's revelation of the scope and character of the NSA's surveillance legitimized the lawsuits filed by individuals and civil liberties organizations challenging the constitutionality of national security surveillance. In late 2013, the American Civil Liberties Union (ACLU) challenged the NSA's program of bulk collection of phone metadata in the US District Court for the Southern District of New York. The court ruled for the government, finding no violation of the rights of citizens who lacked a reasonable expectation of privacy while providing information to telecommunications companies. However, the appeal of the ACLU to the US Court of Appeals for

the Second Circuit proved successful, leading to a decision on the illegal status of the bulk telephone metadata program, as a violation of Section 215 of the Patriot Act (*ACLU v. Clapper* 2013).

A similar decision was made by the US District Court for the District of Columbia in December 2013, when judge Richard J. Leon called the NSA program an indiscriminate and arbitrary invasion of the privacy rights protected by the Fourth Amendment (*Klayman v. Obama* 2013). Such an inconsistency as that between *Klayman* and *Clapper* proves the existence of conflicting approaches in the judicial branch toward national security surveillance. Both decisions ignited the discussion in Congress about the future of the bulk collection of phone data, which resulted in the termination of the program by the provisions of the Freedom Act (Edgar 2017, 4). Judicial control over the legality of national security surveillance affected the legislative process, but it would be too far reaching a conclusion to say that the legislative and judicial branches became united against the secret surveillance system imposed by the executive, as the Court of Appeals' decision was the only serious limitation of national security surveillance in the post-Snowden era.

There is no surprise that the next president, Donald Trump, became a strong supporter of national security surveillance. In 2015, during the debate concerning the future of bulk collection of phone metadata, he expressed his support for the program (Council on Foreign Relations 2015). But when he became the subject of a secret FBI investigation about possible connections between his campaign and Russian intelligence, Trump accused the Obama administration of illegal surveillance. Time showed that Trump's negative attitude toward the leaders of intelligence and law enforcement agencies determined his personal decisions as president (Hayden 2018, 139–41). Trump's critical attitude toward the FBI, CIA, and NSA led to a decrease in trust among Republican voters toward the national security agencies, in contrast to some Democratic voters (Nelson 2018, 181). From an institutional perspective, the beginning of Trump's presidency marked a politicization of national security surveillance, the source of which was the personal opinion of the President as an alleged subject of illegal wiretapping.

On the other hand, at the beginning of the second year of Trump's tenure Congress passed the reauthorization of Section 702 of FISA. The legislation was preceded by a few months of public debate concerning the effectiveness of the transparency system under the existing regulations. Despite concerns of the Democrats that the intelligence community would be endangered by the President's influence on surveillance programs, the law was presented as a safeguard for civil liberties and an assurance of greater transparency (Goldsmith and Hennessey 2018). Due to the lack of a serious national security surveillance scandal, the proponents of the new transparency system argued, as in 2007 and 2012, that it worked properly thanks to the broad oversight system imposed by the legislation. One should remember, however, that

the two earlier reauthorizations of the law had raised hopes for a diminishing of the level of secrecy of national security surveillance, which did not actually happen.

A culture of interbranch secrecy?

Secrecy had always played an important role in the American political system from the time of its establishment, becoming a valuable tool during the Revolutionary War, when it assured the effectiveness of the government (Ginsberg 2016, 7), and during the Philadelphia Convention, when the Framers referred to the executive branch as the one possessing "the powers of secrecy, vigor, and dispatch" (Farrand 1966, 70). Thus the executive invoked the principle of secrecy as a guarantee of its proper functioning (Graham 2017). The growing impact of secrecy on the operations of the US government in the twentieth century led to the notion that there is a specific culture of secrecy (Moynihan 1997; Theoharis 1998), manifested not only in the amount of classified information kept far away from the public's reach, but—above all—in the conviction that secrecy ensures effectiveness and accountability (Edgar 2017, 345; Ginsberg 2016, 7).

In the twenty-first century the US government agreed to conduct a similar politics of surveillance, supporting the necessary secrecy of government activities relating to security issues, especially when they were undertaken by the executive branch (Laidler 2019). The culture of secrecy is obviously rooted in activities undertaken by presidential administrations, or is a "product of the executive branch's very nature" (Kitrosser 2015, 2). The executive, unlike the legislative and judicial branches, has more space to act in the shadows because both Congress and the courts operate through publicly recorded legislation and written public opinions. Furthermore, the executive branch also has access to human and technological resources, enabling it to act in broader secrecy than any other part of the government (Kitrosser 2015, 2–3).

There is surely a contradictory approach toward the scope of transparency and secrecy between the executive and legislative branches. While presidents have to keep some of their communications and actions secret, Congress's main role is to control these actions either by implementing legislation or imposing oversight measures (Lester 2015, 5). Both branches are involved in a constitutional tug-of-war in the direction of broader secrecy versus more openness. Even the analysis of constitutional provisions concerning the separation of powers as articulated in Article Two leaves the impression that the executive was meant to be the most secret one. All this has led to the creation of various theories supporting the secretive powers of the executive, such as executive privilege, protecting the confidentiality of presidential communications from Congress (Frost 2017; Garvey 2014); unitary executive theory, stemming from the Vesting Clause assigning the president all executive

powers (Edelson 2016; Calabresi and Yoo 2012); and state secrets privilege, limiting public access to certain national security information (Arnold 2014; Herman 2011).

These theories are obviously in conflict with the traditional understanding of the checks and balances system, as they assume narrow congressional oversight and judicial control of the legality of the national security policies of the executive. In other words, they legitimized certain policies of presidential administrations in the pre- and post-Snowden eras, including the imposition of often unlimited surveillance. The controversy is even greater when one realizes that the government has the discretionary power to decide which information should be kept secret without thoroughly explaining the reasons for its classification as such. However rational it would seem with regard to the intelligence community, which operates within the realm of secrecy ensuring efficacy (Edgar 2017, 76; Sagar 2015, 151), there is no doubt that the executive has overused the paradigm of national security. Furthermore, whenever presidents have announced "times of emergency" it has meant an automatic change in the scope of protection of constitutional rights, such as freedom of speech, freedom of assembly, due process of law, and the right to privacy (Farber 2008; Akerman 2006). Such an approach was usually supported by other branches of government, especially the courts, which followed the rule that in "times of emergency and peril" the scope of the constitutional protection of basic rights and freedoms may be limited (*Korematsu v. United States* 1944). There is no doubt that extended surveillance measures have played a significant role in the government's use of emergency powers and that national security arguments have enabled the authorities to classify most of their operations in that respect.

Of course, stable and ad hoc congressional committees, inspectors general, courts, and special tribunals have played an important role in imposing control on US surveillance legislation and the executive actions of the national security state (Glennon 2015). Analysis of the character and results of that control proves that, except for the times of increased transparency stemming from press publications or leaks of information concerning surveillance programs (Keller 2017), there has been no clear indication from the controlling institutions about the possible unlawfulness of these programs. Transparency has usually resulted from *ex post* rather than *ex ante* congressional oversight (Lester 2015), which proves that the system governing national security surveillance is more likely to promote secrecy than openness. The debates in Congress on the reauthorization or modification of surveillance legislation have ended, in most cases, by reaffirming or even expanding the powers of executive agencies. The only significant changes in preventing the further growth of surveillance powers of the government occurred in times of leaks about secret surveillance programs, such as in the 1970s, and after 2005 and 2013. These were the only moments in which the investigative and oversight

powers of Congress proved effective, but the analysis of the legislative and institutional outcomes of the postcrisis reforms did not diminish the level of secrecy of national security surveillance.

Similarly, the Supreme Court has never ruled against secret surveillance conducted by the government, and neither has it limited the agencies' surveillance powers (Fisher 2017). Furthermore, the Court has never found any major national security legislation unconstitutional, especially if it adjudicated in times of emergency (Laidler 2011; Akerman 2006). Despite public criticism of certain sections of the Patriot Act by civil rights advocates (Romero and Temple-Raston 2007), the Justices did not address the issue of the constitutionality of these provisions, leaving their modification to Congress in a politically driven legislative process. Lower federal courts were more active in imposing judicial review of the surveillance programs, but when it comes down to the constitutionality of these programs the result is vague. The lack of a transparent and unified position of the federal judiciary on the scope of government surveillance programs strengthens the argument that these programs are legal.

Historically, the courts have hesitated to check the constitutionality of the actions undertaken by the executive, especially when the powers of intelligence agencies, or foreign policy in general, were at stake (Fisher 2017). That leads to another observation, that the federal judiciary was constructed to serve mainly as a "national policy-maker" (Dahl 1957), thus supporting not only the direction of government policies but legitimizing concrete government decisions and programs, provided they protected national security. Even if one argues that such an approach was typical for the early stages of the Cold War, the announcement of the "war on terror" by the Bush administration created an emergency state with national security arguments closing the door to any debate on the constitutionality of secret surveillance programs (Akerman 2006). The problem clearly lies in the culture of secrecy, which may be especially observed with respect to the FISC procedures. If a judge is forced to make a decision concerning the government's request to impose surveillance measures without having access to the full information about the program or to the probable cause of the national security danger caused by the surveilled subject, it is impossible to obtain transparency. Secrecy forces the judicial branch to trust the government in determining the legality of its operations, which can be directly observed in the FISC decisions. According to existing reports, between 1979 and 2009 it approved more than 99% of government requests for surveillance from 28,000 applications overall (Herman 2011, 112).

The abovementioned examples prove that the principle of separation of powers has been affected by the secrecy of executive actions relating to national security and that both Congress and the courts have agreed to play the game with the rules set out by presidential administrations.

The illusion of transparency

The post-Snowden checks and balances system consists of the oversight of national security surveillance by the judges of the FISC and by members of Congress participating in the works of House and Senate intelligence oversight committees, as well as the members of PCLOB, seeking to ensure that surveillance programs do not violate the constitutional rights of Americans. From the structural perspective, each branch is represented in the system, checking whether the institutions responsible for conducting national security surveillance are acting in accordance with the constitution. The legislative branch has the power to reauthorize national security legislation or to adopt new regulations potentially limiting excessive surveillance measures. Congress also has control over the annual budget appropriation, which enables the operation of surveillance programs, and is thus able to determine the character of national security surveillance. At the same time, the federal judiciary has the potential to adjudicate in cases concerning the right of individuals by imposing statutory or constitutional interpretations of government surveillance policies and programs. The power of the courts is not limited to solving disputes stemming from excessive surveillance measures imposed by executive agencies but often comes down to a determination of the parties' legal standing. Additionally, the subjects conducting surveillance, such as the NSA, release several reports regarding the scope of their surveillance programs, thereby becoming the most transparent intelligence community in US history. At least in theory, the current oversight system of national security surveillance should satisfy anyone concerned with the lack of transparency.

In practice, however, when one compares the post-Snowden system with the oversight measures established in the 1970s as a consequence of the Church and Pike Committees' reports, there are no serious institutional differences. The House and Senate intelligence oversight committees have been monitoring national security surveillance since the late 1970s. The level of knowledge of committee members of how the national security surveillance system works may seem higher than 50 years ago, but real changes in that system resulted from uncontrolled leaks to the press rather than effective oversight conducted by these committees (Arnold 2014). Similarly, the lack of serious budget cuts to national surveillance programs (Goldfarb 2015) reveals the congressional attitude toward national security surveillance, not to mention the dramatic change in the character and amount of data intercepted by the government due to broad programs of electronic surveillance. The scope of national security surveillance has changed, but the oversight system does not keep up with these changes.

Congress, as the national legislative body, has always used its power to implement certain regulations aimed at conducting effective control over national security issues. None of the legislation was immune from executive action, which resulted in further expansion of surveillance powers, often

leading to limitations on the rights of individuals as the price for increased security. On the other hand, despite very active use of judicial review, the Supreme Court rarely entered into the world of national security politics, leaving it to presidential discretion and interpretation. Finally, the special court approving foreign surveillance requests did not play its role effectively for procedural reasons and because of the excessive secrecy around national security surveillance. Secrecy is, therefore, a natural element of foreign surveillance, but it is also the main obstacle to conducting proper oversight of government surveillance. Excessive secrecy means that the system lacks transparent control over executive actions or that the applied measures of control are ineffective and inefficient. In both perspectives, stable or ad hoc control is imposed marginally, as the information shared by the executive about the scope and character of the surveillance programs is limited by the principle of secrecy.

As David Lyon (1994, 24) observes, "surveillance is an institutionally central and pervasive feature of social life. Paradoxically, it expanded with democracy." The expansion of national security surveillance became one of the key elements in the evolution of the checks and balances system in American democracy. That evolution was possible not only due to the role of the executive but because Congress and the judicial branch were reluctant to limit presidential attempts to establish a secret national security state. Functioning in an almost never-ending state of emergency enabled those governing to legitimize the implementation of secret NSA programs aimed not only at foreign terrorist suspects but also at American citizens who often did not pose any threat to national security. These programs were and still are defended for their effectiveness, which may be legitimized only because the national security policies are generally kept secret. Whether the purpose of such surveillance measures is always achieved seems disputable, but as long as the system protects the government in the process of limiting the constitutional rights of Americans there is no way to change it, considering that in the contemporary United States, at least in the area of national security surveillance, the meaning of the constitution is determined by all three branches of government.

It seems obvious, then, that secrecy and transparency cannot fully coexist at the same time; therefore, the institutions responsible for interpretation of the law should pose a concrete limit to both values. Such a limit may depend on the state of mind of the society: in times of intensified press investigations, whistleblower leaks, active operation of oversight committees, and frequent judicial review, there is pressure for greater transparency. But in times of crisis, wars, or terrorist attacks, secrecy not only prevails but is treated as a value by both the authorities and the society (Fung et al. 2008, 106). Post-9/11 polls indicated that a lot of citizens were ready to give away their freedoms for stronger security and approved of the antiterrorist measures imposed by the government (Davis and Silver 2003; Parenti 2003, 184; Solove 2011, 67).

In contrast, just after Snowden, when civil liberties were threatened by excessive government surveillance, distrust of the authorities expanded, with four out of five citizens negatively evaluating secret surveillance programs (Epstein 2017, 303).

Analysis of pre- and post-Snowden national security surveillance leads to the impression that the demanded transparency has never been and will never be achieved, and the main reason for this is the way the separation of powers and checks and balances systems work. Although there is no reference in constitutional documents to either secrecy or transparency, the analysis of early writings by the Framers proves that they valued the necessity of imposing a system of government transparency (Arnold 2014, 31), but, at the same time, they accepted a certain level of secrecy, especially of the executive (Frost 2017, 146). The evolution of the national security state proved, however, that if the government wanted to conduct successful foreign and security policy, it had to keep information about surveillance programs out of public reach. Furthermore, the government was able to select the means by which it would act internationally and domestically; therefore, it was just a matter of time until most of the surveillance measures would be cloaked in total secrecy. The adoption of several theories to legitimize and justify application of these measures was the last step on the way to establishing a secret surveillance state. Today, even if presidents are critical about the level of secrecy of surveillance programs, they prefer to legalize them, rather than withdraw from them (Olmsted 2018). Moreover, according to recent public opinion polls, such an approach is accepted by the majority of society, which wants to feel safe and secure, listing dealing with the terrorism threat as one of the three top public priorities (Pew Research Center 2019).

The rhetoric of safety or security has often served as the legitimization of surveillance policies, and political leaders in democratic states have strongly supported the vision that full security can only be achieved with surveillance measures (Green and Zurawski 2015). In times of internal or external danger, usually referred to as times of emergency, governments have implemented broad surveillance programs that expanded their authority, thus potentially limiting the rights and freedoms of the people (Greenwald 2014; Farber 2008; Akerman 2006). This does not mean that the authorities put aside the discussion of transparency, which could be observed in their rhetoric, and even in some institutional solutions (Fisher 2017, 280). Still, with regard to the national security state, the successful implementation of surveillance measures outweighed the possibility of providing information about their scope and character. In that perspective, the rhetoric of the executive, as well as the establishment of a more transparent oversight system, created an illusion that excessive secrecy has diminished. This means that all of the transparency policies implemented by US government as a result of the Snowden affair—annual transparency reports, internal civil liberties

monitoring, or the new rhetoric of openness—are just tools with which to convince society that the culture of secrecy has given place to transparency. In reality, however, little has changed: national surveillance is conducted in secret, both with regard to foreign intelligence collaboration and domestic surveillance of potential terrorist suspects. The separation of powers, which is an effective means of control among the branches in several constitutional areas, is not effective with regard to national security. The powers of the executive, rooted in the principle of secrecy, limit congressional and judicial checks and provide no balance; therefore, the illusion of transparency stems mainly from institutional rather than ideological or partisan factors. This all leads to a strengthening of the idea of the national surveillance state, which can be seen as a permanent feature of governance now substituting for the classical national security state (Balkin 2008, 4). If the national surveillance state becomes more powerful, the erosion of the system of checks and balances will continue, further deepening the illusion that Congress and the courts are controlling what the executive does in secret.

References

ACLU v. Clapper, 959 F.Supp.2d 724 (2013); 14–42 2d.Cir (2015).

Akerman, Bruce. 2006. *Before the Next Attack: Preserving Civil Liberties in an Age of Terrorism*. New Haven: Yale University Press.

Alloa, Emmanuel, and Dieter Thoma. 2018. *Transparency, Society, and Subjectivity: Critical Perspectives*. New York: Palgrave Macmillan.

Angwin, Julia. 2014. *Dragnet Nation: A Quest for Privacy, Security, and Freedom in a World of Relentless Surveillance*. New York: Henry Holt and Company.

Arnold, Jason Ross. 2014. *Secrecy in the Sunshine Era: The Promise and Failures of US Open Government Laws.* Lawrence: University Press of Kansas.

Balkin, Jack M. 2008. "The Constitution in the National Surveillance State." *Minnesota Law Review* 93(1): 1–25.

Ball, Kirstie, Kevin D. Haggerty, and David Lyon. 2012. *The Routledge Handbook of Surveillance Studies*. New York: Routledge.

Cain, Bruce E. 2015. *Democracy More or Less: America's Political Reform Quandary*. New York: Cambridge University Press.

Calabresi, Steven G., and John R. Yoo. 2012. *The Unitary Executive: Presidential Power from Washington to Bush*. New Haven: Yale University Press.

Church Committee Report. 1976. *Final Report of the Select Committee to Study Governmental Operations with Respect to Intelligence Activities, United States Senate, Foreign and Military Intelligence*. Washington, DC: GPO.

Clapper v. Amnesty International, 568 U.S. US 398 (2013).

Cole, David, Federico Fabbrini, and Steven Schulhofer. 2017. *Surveillance, Privacy, and Transatlantic Relations*. New York: Hart Publishing.

Council on Foreign Relations. 2015. *Donald Trump on National Security*, www.cfr.org.

Dahl, Robert. 1957. "Decision-Making in a Democracy: The Supreme Court as a National Policy-Maker." *Journal of Public* 6: 279–95.

Davis, Darren W., and Brian D. Silver. 2003. "Civil Liberties v. Security: Public Opinion in the Context of the Terrorist Attacks on America." *American Journal of Political Science* 48(1): 28–46.

Dennis v. United States, 341 U.S. US 494 (1951).

Dudziak, Mary L. 2000. *Cold War Civil Rights: Race and Image of American Democracy*. Princeton: Princeton University Press.

Edelson, Chris. 2016. *Power Without Constraint: The Post-9/11 Presidency and National Security*. Madison: The University of Wisconsin Press.

Edgar, Timothy H. 2017. *Beyond Snowden, Privacy, Mass Surveillance, and the Struggle to Reform the NSA*. Washington, DC: Brookings Institution Press.

Epstein, Edward Jay. 2017. *How America Lost Its Secrets: Edward Snowden, the Man and the Theft*. New York: Alfred A. Knopf.

Eskens, Sarah, Ot van Daalen, and Nico van Eijk. 2015. *Ten Standards for Oversight and Transparency of National Intelligence Services*. Institute for Information Law, www.ivir.nl/publicaties/download/1591.pdf.

Farber, Daniel, ed. 2008. *Security v. Liberty: Conflicts Between Civil Liberties and National Security in American History*. New York: Russell Sage Foundation.

Farrand, Max, ed. 1966. *Records of the Federal Convention of 1787. Vol. I*. New Haven: Yale University Press.

Farrell, Henry, and Abraham Newman. 2019. *Of Privacy and Power: The Transatlantic Struggle over Freedom and Security*. Princeton: Princeton University Press.

FISA Amendments Act, 122 Stat. 2436 (2008).

Fisher, Louis. 2013. *Presidential War Power*. Lawrence: University Press of Kansas.

Fisher, Louis. 2017. *Supreme Court Expansion of Presidential Power: Unconstitutional Leanings*. Lawrence: University Press of Kansas.

Foreign Intelligence Surveillance Act, 92 Stat. 1783 (1978).

Friedman, Lawrence, and Victor M. Hansen. 2012. "Secrecy, Transparency, and National Security." *William Mitchell Law Review* 8(5): 1610–28.

Frost, David B. 2017. *Classified: A History of Secrecy in the United States Government*. Jefferson: McFarland and Company.

Fung, Archon, Mary Graham, and David Weil. 2008. *Full Disclosure: The Perils and Promise of Transparency*. New York: Cambridge University Press.

Garvey, Todd. 2014. *Presidential Claims of Executive Privilege: History, Law, Practice, and Recent Developments*. Congressional Research Service, https://fas.org/sgp/crs/secrecy/R42670.pdf.

Ginsberg, Benjamin. 2016. *Presidential Government*. New Haven: Yale University Press.

Glennon, Michael J. 2015. *National Security and Double Government*. New York: Oxford University Press.

Goldfarb, Ronald J. 2015. *After Snowden: Privacy, Secrecy, and Security in the Information Age*. New York: Thomas Dunne Books.

Goldsmith, Jack, and Susan Hennessey. 2018. "The Merits of Supporting 702 Reauthorization (Despite Worries About Trump and the Rule of Law)." *Lawfare Blog*, January 18, www.lawfareblog.com/merits-supporting-702-reauthorization-despite-worries-about-trump-and-rule-law.

Graham, Mary. 2017. *Presidents' Secrets: The Use and Abuse of Hidden Power*. New Haven: Yale University Press.

Green, Nicola, and Nils Zurawski. 2015. "Surveillance and Ethnography: Researching Surveillance as Everyday Life." *Surveillance & Society* 13(1): 27–43.

Greenwald, Glenn. 2014. *No Place to Hide: Edward Snowden, the NSA, and the U.S. Surveillance State*. New York: Henry Holt.
Gurnow, Michael. 2014. *The Edward Snowden Affair: Exposing the Politics and the Media Behind the NSA Scandal*. Indianapolis: Blue River Press.
Hayden, Michael V. 2018. *The Assault on Intelligence: American National Security in an Age of Lies*. New York: Penguin Press.
Herman, Susan N. 2011. *Taking Liberties: The War on Terror and the Erosion of American Democracy*. New York: Oxford University Press.
Johnson, Loch K. 2018. *Spy Watching: Intelligence Accountability in the United States*. New York: Oxford University Press.
Keller, William W. 2017. *Democracy Betrayed: The Rise of the Surveillance Security State*. Berkeley: Counterpoint.
Kitrosser, Heidi. 2015. *Reclaiming Accountability: Transparency, Executive Power, and the U.S. Constitution*. Chicago: University of Chicago Press.
Klayman v. Obama, 957 F. Supp 2d.1 (2013).
Korematsu v. United States, 323 U.S. US 214 (1944).
Kuntze, Jan-Hendrik. 2018. *The Abolishment of the Right to Privacy? The USA, Mass Surveillance and the Spiral Model*. Baden-Baden: Tectum Verlag.
Laidler, Paweł. 2011. *Sad Najwyzszy Stanow Zjednoczonych Ameryki. Od prawa do polityki*. Krakow: Jagiellonian University Press.
Laidler, Paweł. 2019. "How Republicans and Democrats Strengthen Secret Surveillance in the United States." *Political Preferences* 25: 5–20.
Laird v. Tatum, 408 U.S. US 1 (1972).
Lester, Genevieve. 2015. *When Should State Secrets Stay Secret? Accountability, Democratic Governance, and Intelligence*. New York: Cambridge University Press.
Lyon, David. 1994. *The Electronic Eye. The Rise of Surveillance Society*. Minneapolis: University of Minnesota Press.
Lyon, David. 2014. "Surveillance, Snowden, and Big Data: Capacities, Consequences, Critique." *Big Data & Society* 1(2): 1–13.
Lyon, David. 2015. *Surveillance After Snowden*. Cambridge: Polity.
McCabe, Andrew G. 2019. *The Threat: How the FBI Protects America in the Age of Terror and Trump*. New York: St. Martin's Press.
Moses, Lyria Bennett, and Louis de Koker. 2017. "Open Secrets: Balancing Operational Secrecy and Transparency in the Collection and Use of Data by National Security and Law Enforcement Agencies." *Melbourne University Law Review* 41(2): 1–41.
Moynihan, Daniel P. 1997. "The Culture of Secrecy." *Public Interest* 128: 55–72.
National Security Act, 61 Stat. 496 (1947).
Nelson, Michael. 2018. *Trump: The First Two Years*. Charlottesville: University of Virginia Press.
Olmsted, Kathryn. 2018. "Terror Tuesdays: How Obama Refined Bush's Counterterrorism Policies." In *The Presidency of Barack Obama: A First Historical Assessment*, edited by Julian E. Zelizer. Princeton: Princeton University Press.
Parenti, Christian. 2003. *The Soft Cage: Surveillance in America. From Slavery to the War on Terror*. New York: Basic Books.
Pew Research Center. 2019. *Public's 2019 Priorities: Economy, Health Care, Education and Security All Near Top of List*, www.pewresearch.org/politics/2019/01/24/publics-2019-priorities-economy-health-care-education-and-security-all-near-top-of-list/.

Posner, Eric A. and Adrian Vermeule. 2006. *Terror in the Balance: Security, Liberty, and the Courts*. New York: Oxford University Press.
Prados, Jeff. 2014. *The Family Jewels: The CIA, Secrecy, and Presidential Power*. Austin: University of Texas Press.
Presidential Policy Directive, 28 January 17, (2014).
Protect America Act, 121 Stat. 552 (2007).
Romero, Anthony D., and Dina Temple-Raston. 2007. *In Defense of Our America: The Fight for Civil Liberties in the Age of Terror*. New York: William Morrow.
Sagar, Rahul. 2015. "Against Moral Absolutism: Surveillance and Disclosure After Snowden." *Ethics and International Affairs* 29(2): 145–59.
Smith, Cary Stacy, and Li-Ching Hung. 2010. *The Patriot Act: Issues and Controversies*. Springfield: Charles C. Thomas.
Solove, Daniel J. 2011. *Nothing to Hide: The False Tradeoff Between Privacy and Security*. New Haven: Yale University Press.
Theoharis, Athan G. 2011. *Abuse of Power: How Cold War Surveillance and Secrecy Policy Shaped the Response to 9/11*. Philadelphia: Temple University Press.
Theoharis, Athan G., ed. 1998. *A Culture of Secrecy: The Government Versus the People's Right to Know*. Lawrence: University of Kansas Press.
United States v. Reynolds, 345 U.S. US 1 (1953).
USA Freedom Act, 129 U.S. US 268 (2015).
USA Patriot Act, 115 Stat. 272 (2001).
USA Patriot Act Additional Reauthorizing Amendments, 120 Stat. 278 (2006).
Van Dijck, Jose. 2014. "Datafication, Dataism and Dataveillance: Big Data Between Scientific Paradigm and Ideology." *Surveillance & Society* 12(2): 197–208.

Chapter 7

Secret surveillance in Poland after Snowden

Between secrecy and transparency

Mateusz Kolaszyński

Introduction

Surveillance powers are typical in the work of law-enforcement agencies and intelligence services around the world. In democratic states, they make it possible to fight against such threats as terrorism, cyber-attacks, organized crime, etc. (Gill and Phythian 2018). To this end, state services use secret surveillance—covert techniques and practices of information gathering about people that occur without the monitored subjects' knowledge or approval. These surveillance powers, typically carried out by law-enforcement and intelligence services, are more sensitive politically, as well as closely related to core issues of power and security (Svenonius and Björklund 2018). However, these state activities may also seriously interfere with fundamental rights, in particular privacy and data protection. Nowadays, technological advancements have generated new threats and, at the same time, have provided means of fighting those threats, making such work increasingly complex. Technological progress means that intelligence services have tools for almost unlimited surveillance. It is the obligation of the state to provide adequate safeguards for people and to enact clear laws in this area (FRA 2017a, 2017b).

This problem has often been described as a conflict between security and human rights (Bigo 2012). However, secret surveillance can also be used to protect human rights, e.g., potential victims of crime or terrorist attacks. Thus, this chapter recasts the conflict in surveillance policy as a dilemma between secrecy and transparency (Matei and Bruneau 2011). Secrecy ensures the effectiveness of security services, and thus agencies lobby for solutions that limit transparency. In turn, explicit provisions regarding surveillance, control mechanisms, and independent oversight can be considered aspects of transparency. Such guarantees can also contribute to increased protection of human rights. The goal of this chapter is to discuss the barriers against overcoming the culture of secrecy in the area of surveillance (Kovanic and Coufalova 2019) with particular focus on Poland, where debates about the Snowden revelations have not succeeded in making surveillance practices more transparent (Gruszczak 2017).

DOI: 10.4324/9781003120827-10

The obligation to provide security for citizens is one of the constitutional values in a democracy, and the effectiveness of security provision sometimes requires secrecy. However, the domination of secrecy over other constitutional values is a systemic and institutional problem. Since 1990, there has been no comprehensive move toward transparency. The construction of modern intelligence services has not been completed in Poland. There is a lack of response to contemporary challenges, including the development of information technologies and international cooperation with the services of other countries, as well as regulatory challenges related to Snowden's revelations.

On the contrary, even after Snowden's revelations security services have increasingly extended surveillance powers (Kolaszyński 2019). Since 2016, the role of the Polish Constitutional Tribunal has been limited. Earlier, the rulings of the tribunal had a substantial impact on limiting surveillance. This makes Poland one of the countries that still has a broad surveillance mandate (Svenonius et al. 2014). In general, successive Polish governments have supported reforms that tend to increase surveillance powers. This practice is mostly influenced by the politicization of law enforcement and, first and foremost, intelligence services. Security services can push for beneficial solutions for themselves, such as unlimited access to information. The success of these policies also derives from the weakness of institutional arrangements, including limited possibilities of the opposition, low public awareness, and a lack of real independent oversight. Overall, there is institutional support for broad surveillance powers and a lack of significant safeguards against such policies in Poland.

The article is structured as follows: the first part will present significant legislative changes in the area of surveillance after 2013; the second part will describe institutional and administrative arrangements that should ensure there is a balance between secrecy and transparency, and therefore the successful governance of surveillance; the third part will show the balancing role of the Constitutional Tribunal prior to 2016 and its limited role ever since.

Legal framework after 2013

Since Snowden's warnings about the extent and dangers of secret surveillance, Poland has had no radical rethinking with respect to secret surveillance practices. Since 1983, Polish law has used the term "preliminary investigation" (*czynności operacyjno-rozpoznawcze*) to refer to secret surveillance. This significant change did not mean that before 1983 security services did not keep citizens under surveillance. Indeed, they frequently operated in such a way but did so without any statutory basis. The Act of 1983 thus did not regulate preliminary investigation in a comprehensive way. The practices of the Security Service (*Służba Bezpieczeństwa*—SB) in the Polish People's Republic (*Polska Rzeczpospolita Ludowa*—PRL) made that draft regulation almost irrelevant,

since under the communist system secrecy was the norm in the state's surveillance policies (Persak and Kamiński 2005).

In 1990, a new intelligence and police law led to changes in regulations concerning secret surveillance (preliminary investigations). The statutory regulation was expanded, and there were attempts to improve the rules in the ensuing years. The process of declassifying secret surveillance during the political transformation came down to the following key issues: changing the statutory basis for secret surveillance; new intelligence and police services structure that would formally separate preliminary investigations from politics; increasing governmental control and external oversight of secret surveillance. But the reforms also raised doubts regarding the role of transparency in surveillance and did not strike a balance between security and human rights.

With regard to state surveillance, the culture of secrecy and the lack of citizen awareness still dominate, despite a few solutions aimed at enhancing transparency. Very often, extensive surveillance powers are granted without adequate procedural guarantees for the protection of human rights and without creating independent oversight mechanisms over security services. Increasingly, the capabilities of state institutions stem from adopting imprecise, laconic regulations (FRA 2017a). This problem of lack of balance has received attention from several institutions, even if it remains unresolved. At the national level, these institutions are primarily the Constitutional Tribunal, the Commissioner for Human Rights (RPO), the Supreme Audit Office (NIK), NGOs, and some experts. At the international level, relevant institutions include the European Court of Human Rights (ECHR), the Court of Justice of the European Union (CJEU), the Venice Commission, and the European Union Agency for Fundamental Rights (FRA).

This part of the chapter will present the most important legal changes regarding secret surveillance after 2013. Most of them were introduced in 2016 after the election of the conservative Law and Justice party (PiS) in order to increase the scope of state secret surveillance. Earlier, the ruling liberal coalition of the Civic Platform (PO) and the Polish People's Party (PSL) ignored changes in the area of secret surveillance, even though reforms became a necessity as a result of the Constitutional Tribunal's ruling and alarming signals from other institutions, such as the RPO. Current solutions in Poland will be presented in the context of international standards set by the ECHR, the Venice Commission, and the FRA.

A key piece of legislation were the amendments referred to as the Surveillance Act of 2016,[1] which implemented some recommendations included in the Constitutional Tribunal judgment of July 30, 2014 (No. K 23/11), which demanded rigorous reform to surveillance. However, the Act only partially implements the judgment, and the most essential principles formulated in the judgment, which reflected the process of the revision of secret surveillance legislation, were not included. This issue will be discussed in the latter part of the chapter. The Surveillance Act additionally introduced

other legal solutions that the Constitutional Tribunal's judgment did not require or refer to at all, in particular with reference to the scope of intelligence services' access to telecommunications and internet data, which have been significantly extended. This led to the creation of a mechanism for the *ex post* oversight of access to telecommunications and internet data conducted by the regional court based on a biannual statistical report prepared by law enforcement and intelligence services. However, the judicial oversight is illusory due to the limited powers of the regional court, which will be further discussed in the second part of the chapter.

In 2016, the Sejm (lower house of the Polish Parliament) passed numerous other laws that extended the reach of surveillance powers. A notable event was the passage of the amendment to the Code of Criminal Proceedings, introduced in March 2016,[2] enabling the broader use of surveillance in criminal proceedings (Grabowska-Moroz 2016). The amendment introduced a provision (§168a), which states that evidence cannot be considered inadmissible solely because it was obtained in violation of the rules of criminal procedure or by committing an offense. The only exception is when the evidence has been obtained as a result of murder and/or willfully causing bodily injury or imprisonment in connection with the performance of an official public duty. Moreover, the amendment deleted the so-called "*ex post* consent procedure" conducted by the court. According to the previous law, if operational surveillance—recording the contents of telephone conversations and correspondence conducted via telecommunications networks—provided evidence of a different crime or one committed by a person other than the one under investigation, the decision of the court was required. The Act deleted this procedure and provided that only the consent of a prosecutor is required (§168b).

Another regulation that impacts the oversight system of intelligence services and law enforcement is the new *Law on the Prosecutor's Office*.[3] According to this new law, the office of the Prosecutor General is held by the Minister of Justice so that this function is fulfilled by a politician, a member of the government. This dual role is especially important because prosecutors are also entitled to permit the use of some secret surveillance. Their control covers access to classified files containing information gathered during surveillance. Moreover, the new law allows the Prosecutor General to order the competent authorities to conduct secret surveillance operations if they are related to the ongoing investigation (Rzepliński 2003).

On June 10, 2016, the Sejm also adopted the Anti-terrorism Law.[4] This regulation extends the powers of the Internal Security Agency (ABW) and, at the same time, relaxes oversight requirements, particularly toward foreigners. At least three controversial provisions of this Act are related to secret surveillance and concern the following issues: the confidential register maintained by the ABW, wiretapping (in legal terminology: operational surveillance) of foreigners, and criminal proceedings based only on information from secret surveillance. To prevent "terrorist events," the head of ABW keeps a

register of persons who may be associated with terrorism.[5] However, how this confidential register is maintained does not meet the standards set by the ECHR (Leander v. Sweden, No. 9248/81). The Anti-terrorism Law regulates the exception by way of a fundamental principle in the Polish legal system, according to which any application of operational surveillance by intelligence services and law enforcement requires the consent of an independent authority (a regional court).[6] The third significant change introduced by the Anti-terrorism Law "liberalizes" criminal trial procedures.[7] A person can be charged in criminal proceedings based only on information obtained as a result of secret surveillance. Moreover, information from secret surveillance may be the basis for the prosecutor's request for detention on remand. Thus, pretrial detention and prosecution may occur based on anonymous data, for example, an officer's note from a meeting with an informant not disclosed in the case file (Bodnar et al. 2019).

Recently, three new institutions emerged which were granted considerable powers in terms of surveillance: the National Revenue Administration (KAS), the National Security Services (SOP), as well as the Internal Oversight Inspector (BNW), which is subject to the mandate of the Ministry of Internal Affairs. The KAS was created from the merging of two services that used surveillance. Due to the large number of institutions authorized to undertake surveillance in Poland, this combination is generally favorable. The SOP, like the Government Protection Bureau (BOR), is responsible for providing VIP security services for the Polish government (security of incumbent and former Presidents of Poland, high-ranking state officials, etc.). However, the new service has garnered significantly more far-reaching powers. Controversy was aroused when surveillance powers were granted to the SOP, because the BOR did not have such powers. The surveillance powers of the SOP are extensive and include operational surveillance and the collection of metadata. It is particularly worth noting that the new law copied the solutions of other police acts without any new proposals for better safeguards for human rights (Kolaszyński 2019).

The BNW is a part of the Ministry of Internal Affairs and is supposed to keep under surveillance other security services upon the request of the Minister of Internal Affairs. The purpose of this service is to improve and unify ministerial control of other institutions, such as the police, the Polish Border Guard, and the SOP. One of the tasks of the new agency is to control the surveillance activities of the services mentioned above. Seconded police officers, border guards, and SOP officers work primarily in the BNW. Formally, this institution is a part of the internal organization of the Ministry of Interior (Kolaszyński 2019).

The extensive surveillance powers of the BNW are controversial. Since 1990—when civilian control over security services was established—only security services (the police, the Polish Border Guard, and intelligence services) have had surveillance powers. The Minister of Internal Affairs had

the right to intervene in the work of services only when entitled to do so by applicable acts. This solution was designed to separate civil and political management in the ministry from professional and apolitical law enforcement and intelligence services (Widacki 1999). After 1990, control over surveillance powers gradually became the domain of prosecutors and courts. The surveillance powers of the new services under the full control of the Ministry of Internal Affairs work against the model mentioned above. On the one hand, the minister gets the opportunity to view the surveillance materials of the supervised services. On the other hand, the minister's Internal Oversight Inspector—the BNW—also has extensive surveillance powers. For example, this institution can use operational surveillance or partake in collecting metadata (Kolaszyński 2019).

Surveillance methods form the core of the activity of each service. Problems arising from the monitoring of this activity, that is, controlling the controllers, are visible in many countries (FRA 2017a, 2017b). However, the common standard is oversight exercised by an independent, external body. The appointment of the BNW does not meet this standard. The Ministry of Internal Affairs is politically accountable for the activities of the services controlled by it (the police, the Polish Border Guard, the National Security Bureau). That is why a reliable explanation of violations may conflict with the minister's potential accountability (Kolaszyński 2019).

The legislative changes presented above grant the security services extensive opportunities to use secret surveillance. It is also necessary to indicate areas in which systemic reforms have not been undertaken for many years. Three such areas, where regulations are residual and loose, are essential for surveillance. More clarification of the law on these issues and proper development of regulations would ensure an adequate balance between transparency and secrecy (FRA 2017a, 2017b). The first area is the system of control and oversight over intelligence and police services. More on this subject will be discussed in the second part of the chapter. The law also barely regulates the second area—international cooperation in the Polish security services. Additionally, there is no legal basis for intelligence actions taken abroad. Currently, the law does not control any surveillance methods that are used to collect data outside the country. It also does not require the officers to fulfill any particular responsibilities or comply with bans. Both legislative changes and a lack of initiative in other areas mean that the current legal system may be incompatible with the Polish constitution and international standards in many elements (Lefebvre 2016; Kolaszyński 2019).

Since Snowden, international standards have generally been ignored by the Polish authorities, despite the recommendations of the Polish Ombudsman, NGOs, and experts. A report prepared under the auspices of the ombudsman pointed to many deficiencies in the Polish legal system (Bodnar et al. 2019). Polish law does not conform to international standards relating to the use of wiretaps and operational surveillance (as well as the use of metadata) resulting

from the case law of the ECHR. Moreover, Polish law does not correspond to the standard for the use of metadata by the security services and the protection of information related to professional privilege (e.g., lawyers, journalists) set out in the judgment in the case of Big Brother Watch and Others v. the United Kingdom (European Court of Human Rights 2018, application Nos. 25198/0258170/13, 62322/14, and 24960/15). Polish authorities do not implement standards related to the jurisprudence of the CJEU, especially in the field of standards related to telecommunications data based on the so-called retention directive (Court of Justice of the European Union 2014, Digital Rights Ireland, Nos. C-293/12 and C-594/12; Court of Justice of the European Union 2016, Tele2, Nos. C-203/15 and C-698/15) and procedural protection for persons at risk of expulsion (Court of Justice of the European Union 2013, ZZ v. Secretary of State, No. C-300/11). The problems identified by international organizations are also not the subject of reflection. A number of recommendations from the Venice Commission have not been introduced into Polish law. According to the Opinion of 2016 (Venice Commission 2016), procedural safeguards and material conditions established in the police acts on implementing secret surveillance are still insufficient because they do not prevent excessive use of powers and unjustified interference that conflict with the privacy of individuals.

In Poland, there is a visible departure from European standards regarding secret surveillance (Wetzling and Vieth 2018). The lack of balance between secrecy and transparency is a systemic problem that has been known for years. Intelligence services and law enforcement are increasingly able to use secret surveillance. Additionally, more and more institutions are entitled to undertake such activity. The problem is also that politicians have an increasing impact on the use of surveillance. Moreover, rather than the development of adequate control and oversight mechanisms, there has instead been a deterioration in standards (Bodnar et al. 2019). The second part of this chapter will show how this process is supported by institutional solutions or, oftentimes, a lack of them.

Institutional and systemic challenges

According to Richard J. Aldrich and Daniela Richterova, Snowden's disclosures have not changed the state's interference in personal privacy but have rather exposed the crisis of state secrecy. In their view, "the key issue is not government looking at us, but our increasing ability to look at government, and especially new ways of calling the secret state to account" (Aldrich and Richterova 2018, 1003). A similar opinion can be found in the Guardian article about the situation in Poland that was published shortly after Snowden's revelations: "The Prism affair questions the very essence of the contract between societies and their governments: accountability" (Bodnar and Szymielewicz 2013). It does seem that after 2013, the challenges

of creating an oversight system of state surveillance became the primary issue. The way these mechanisms function is a practical reflection of how the state confronts the dilemma between transparency and secrecy.

The problem of the lack of balance between secrecy and transparency can be seen from the perspective of the separation of powers. Each branch has a different role in secret surveillance. Together, the executive, legislative, and judicial branches can provide guarantees against the use of secret surveillance. In turn, possible shortcomings of this system have allowed laws to be passed without a balance between transparency and secrecy (Wegge 2017).

In Poland, there is a serious problem with the politicization of the services. Until 1990, security services were part of ministries and were fully politicized (Gruszczak 2009; Caparini 2014). Formal regulation in 1990 was designed to separate civil and political management in the ministry from professional and apolitical services. This solution was to guarantee that secret surveillance would not be used for current policy (Widacki 1999). This was necessary because of the use of surveillance against the opposition in the communist system (Persak and Kamiński 2005). However, separating politics from intelligence services turned out to be very difficult in practice.

In 1990, the principle was introduced according to which politicians would no longer have complete control over the surveillance of citizens, and it was no longer to be used as a tool in dealing with legitimate political opposition (Widacki 1999). However, some chosen members of the government were given control over surveillance powers, in particular, the Prosecutor General as the Minister of Justice (1990–2010, and since 2016) and the Minister of Internal Affairs (1990–1996, and since 2018). After winning the 2015 election, the PiS government not only reverted to the previous influence of politicians on the secret surveillance apparatus but significantly expanded this influence. The new Law on the Prosecutor's Office discussed above and the establishment of the BNW allow for more far-reaching secret surveillance than before.

Politicians can be influenced by those who decide on secret surveillance in Poland, that is, the heads of the special services. These heads have enormous power over their services as they primarily decide on the scope of the surveillance activity. At the same time, they are not clearly separated from the current policy because there are no significant restrictions on who should be appointed head of a service. A candidate for the position does not have to be an officer of any service, nor demonstrate specific experience, knowledge, etc. It is also quite common that many functions are performed by politicians or other people not directly involved with intelligence services and more connected with current politics.

In Poland, there is a lack of governmental control over secret surveillance. According to Hans Born and Gabriel Geisler Mesevage (2012, 6–7) "oversight" should be distinguished from "control" because "the latter term implies the power to direct an organization's policies and activities. Thus, control is typically associated with the executive branch of government and specifically

with the senior management of intelligence services." There are practically no permanent, institutionalized forms of control over services responsible for secret surveillance. Since there are so few institutional limitations, different governments enjoy considerable independence in exercising control. As a result, since 1990, law enforcement and intelligence services have been supervised by a number of bodies of various structural and political statuses with unsuitable experience and backgrounds. This means no officials have specialized in control over these institutions.[8] For example, in the government of Jerzy Buzek (1997–2001), the Board for Special Services (KSS) never met at all (Zybertowicz 2007). The creation of effective control mechanisms is hampered by the lack of political responsibility for special services. In Poland, there have been many scandals related to the impact of special services on political and economic life. However, political responsibility for these events is not typical for politicians who control the services. Andrzej Zybertowicz (2007) calls this phenomenon "the institutionalization of non-accountability" and "self-tasking of the services."

In this situation, with a lack of permanent control over security services and a lack of political responsibility, the special services gain a considerable advantage over politicians. First of all, they are the only ones who have expert knowledge about intelligence activities, including secret surveillance (Łoś 1995). In Poland, there are still not enough civilian experts and supervisory institutions. The small number of private experts has historical reasons, since before the political transformation security research was dominated by the communist party structures (Matei and Bruneau 2011). At the same time, the security services have centralized and hierarchical structures that minimize access from the outside. In the face of any reform attempts, state security experts present a reliable and determined group of influencers with a high degree of knowledge and power. Mixing these two spheres—politics and special services—can give rise to support for broad surveillance powers. In this tandem, intelligence services enjoy expert knowledge and access to secrets. The government lacks permanent structures, and knowledge about special services is almost impossible to verify. These circumstances make politics vulnerable to manipulation. This situation is further exacerbated by the system of informal relations between these spheres (Zybertowicz 2007).

Such relationships within the executive branch have an impact on parliamentary oversight. In 1995, the Sejm Committee for Special Services (SKSS) was appointed, made up of members of the parliament.[9] The parliamentary majority has a decisive influence on the work of the committee. Recently, several practices meant to increase the power of the opposition to the work of this body have been abandoned. With the original establishment of the committee, the practice of a six-month rotating chairmanship was introduced. During the fourth term of the Sejm (2001–2005), the additional practice developed by which only the opposition deputies became rotating chairmen

(Kolaszyński 2018). In 2015, however, the parliamentary custom of a rotating chairmanship of the committee was abandoned.

The SKSS formally has a broad mandate regarding oversight of the special services. However, the importance of the committee is not demonstrated by the full range of its work since its powers are limited in practice. The committee's members are formally allowed to demand any information about secret surveillance from the government, the heads of special services, and officers subject to them, but the real power to request this information is limited. In order to disclose any information related to secret surveillance, the head of a given institution has to give their consent. The regulations do specify any particular grounds for either approval or rejection of consent, so the committee might be denied access to information without detailed justification (Sarnecki 2010). Polish parliamentary oversight is very often reduced to trying (and failing) to access the "secrets" of special services. At the same time, the committee has not contributed to initiating a policy debate on government control of secret services. Since 1995, the SKSS has not prepared any public report on the situation of special services and their government control that could initiate a debate on this issue.

The lack of real oversight and parliamentary debate is also evident in the legislative process. Laws on secret surveillance have passed without serious discussion about the balance between secrecy and transparency. Opposition MPs and NGOs are often concerned about the encroachment on human rights associated with excessive secret surveillance. However, their impact on the final form of the law is minimal. The majority of the Sejm supports unequivocally government projects that give broad powers to security services. The ultimate argument for supporters of governmental projects is often populist rhetoric, i.e., if someone disagrees with the broad powers of a particular service, then he or she is a supporter of criminals. This approach was evident during the legislative work on the Central Anti-Corruption Bureau (CBA) Act in 2006. Criticism of the extensive powers of this institution was often rejected with arguments such as "honest people have nothing to fear" or "only a supporter of corruption may have doubts about the broad powers of the CBA." Eventually, despite its unprecedented broad powers in Poland, the CBA Act was passed with the support of a significant part of the opposition.

Populist rhetoric is effective due to public opinion. Knowledge about the activities of intelligence services is not common. In general, citizens do not know what functions the security services other than the police perform, nor is there widespread knowledge of the umbrella mechanisms of control and oversight. This problem is characteristic of many Central and Eastern European countries (Matei and Bruneau 2011). One of the main reasons for this is the government and intelligence services' information policy, which leaves a lot to be desired. There is a culture of secrecy in this area because even the necessary information on the activities of special services is not provided. The need for confidentiality often masks incompetence. This also applies to

proactive information policy, which is, to some extent, carried out by only two services, the ABW and the CBA (Matei and Bruneau 2011).

The secret surveillance issue is not popular with the public. This factor reduces the pressure on the government to seek a balance between broad powers and human rights. According to the Public Opinion Research Center (CBOS), the majority of voters support broad surveillance powers. In the opinion of Poles, there is no need to change surveillance capabilities, and security services should have wide surveillance powers. This is particularly apparent with regard to internet surveillance. According to CBOS, when faced with a choice between, on the one hand, increased possibilities for internet surveillance for the police and other services in order to combat crime and, on the other hand, decreased control of online communication to protect users' privacy, Poles usually choose the first option (46% vs. 30%).[10] Moreover, half of the respondents think that the current powers of police services and intelligence agencies to gather information about internet users are acceptable. It is important to note that this CBOS research was carried out in April 2016 after the reform that introduced the so-called Surveillance Act. In general, surveillance is not an issue that is particularly important for Poles. Shortly after the introduction of the Surveillance Act, 54% of Poles didn't know anything about this law (27% of Poles had heard of it but did not know what the changes were; only 19% of Poles had heard of it and had some idea of the changes introduced) (CBOS 2016, 5). A large group of Poles are not interested in the issue of surveillance whatsoever. It seems that lack of awareness is a crucial factor in assessing the attitude of Poles toward this problem (Svenonius and Björklund 2018).

This indifference can be gradually reduced by the activities of NGOs and media pluralism. More and more NGOs are comprehensively monitoring the issue of surveillance. The largest of them include the Panoptykon Foundation, the Helsinki Foundation for Human Rights, and Amnesty International. They use the Act on access to public information.[11] As a result, the media has often proved a more effective oversight tool than the overall formal control and oversight mechanisms (Matei and Bruneau 2011). Most of the evidence of irregularities associated with security services originated in media reports (Hillebrand 2012).

The balance between secrecy and transparency is also distorted due to the weakness of independent oversight. In 2001–2002 some responsibilities related to secret surveillance—operational surveillance—were transferred from the Prosecutor General to the courts. The Prosecutor General was no longer supposed to authorize this power but merely provided an opinion on the motions submitted to the court by the various services. This method officially guaranteed external, independent oversight over this area of secret surveillance, which impinges upon human rights to the greatest extent. However, there is a lack of actual judiciary oversight in practice. Judiciary oversight is exercised by the criminal divisions of regional courts, mostly dealing with

criminal cases. There are no other specially designed departments or other structures that would be responsible for giving consent to operational surveillance. For this reason, such duties are treated as peripheral and secondary tasks. Moreover, the courts are not able to review all materials regarding a particular case. They can only examine what the services show them. Ultimately, this oversight is illusory. Publicly available statistics confirm this thesis—the courts accept about 99% of the requests from the heads of secret services for the application of operational surveillance (Rojszczak 2021).

In Poland, no independent body has yet been established to examine citizens' complaints about the surveillance activities of security services. There is still no effective external oversight of access to telecommunications, posts, and internet data, as that guaranteed by law since 2016 is mostly illusory. This monitoring is exercised only *ex post* and randomly; the lack of prior and individual oversight is not the only deficiency with regard to current solutions (Bodnar et al. 2019). Both types of judicial oversight—that established in 2001 over operational surveillance and the one established in 2016 over telecommunications, internet, and postal data—share the same limitations. In both cases, permanent organizational structures that would deal with this type of activity were not guaranteed in the acts. Moreover, no additional financial and human resources were provided for this purpose. Ensuring adequate organizational structures to enable permanent oversight is justified by the scale of the security services' activities: in 2017, special and police services acquired over 1.2 million pieces of data. As for operational surveillance, the police alone filed nearly 10,000 wiretapping applications in 2017 (Bodnar et al. 2019; Kolaszyński 2019).

In Poland, there is no specialized, independent institution that would deal only with the oversight of secret surveillance. In many countries, such external bodies have been created. Currently, one or more such institutions dedicated to security services operate in 16 EU countries. Only some aspects of secret surveillance work also used to be monitored by an independent constitutional body—the NIK and the RPO. Their role is essential, but neither is authorized to carry out any regular oversight of the services (Kolaszyński 2018).

The role of the Constitutional Tribunal

According to some researchers, breaking the secrecy culture exceeds the capabilities of any institution in Poland (Zybertowicz 2007). However, it is worth noting the role of the Constitutional Tribunal in regulating surveillance. This institution has played one of the most significant functions in developing the statutory basis for secret surveillance over the last 30 years. The tribunal has often contributed to the introduction of changes in the regulations and, consequently, the move toward more of a focus on the protection of human rights (judgments No. W 12/94, No. K 45/02, and No. W 54/07). The tribunal's case law has significantly reduced surveillance powers and was of fundamental

importance for statutory changes in the matter of surveillance. However, in 2016 the function of the tribunal in this field was actually suspended. The paralysis of the constitutional court is the most severe change in surveillance policy since Snowden and can explain the expansion of surveillance powers in recent years.

Before 2016, the tribunal decided to limit surveillance powers on several occasions. Two representative cases will be presented below. In both cases, these were sentences issued shortly after the establishment of new special services: the Internal Security Agency (ABW) and the Foreign Intelligence Agency (AW) (2002) and the Central Anti-Corruption Bureau (CBA) (2006). The judgment of the Constitutional Tribunal of April 20, 2004 (No. K 45/02) considered the appointment of political heads to security agencies as nonconstitutional. According to the tribunal, assigning the heads the role of secretaries of state was a sign of circumventing the constitutional ban on joining the parliamentary mandate with employment in a government agency, and the post of head of special services had not been prepared for politicians. This also applies to the use by politicians of intelligence services and their surveillance powers. This ruling was welcomed by constitutionalists (Radziewicz 2004), and since then, the heads of the ABW and AW have not been secretaries of state with political functions.

As with the establishment of the ABW and AW, the Constitutional Tribunal examined the constitutionality of the Act on the CBA. In a judgment on June 23, 2009 (No. K 54/07), the Constitutional Tribunal ruled that the definition of corruption in the CBA Act was unconstitutional because the definition was unclear and ambiguous, resulting in CBA's broad scope of competence. This legal definition played a fundamental role in determining the scope of the CBA's tasks. In this context, the court also ruled on surveillance powers. It considered the use of sensitive data and information obtained as a result of performing surveillance activities without instruments for controlling how these data are stored and verified unconstitutional. This problem also concerned the method of deleting unnecessary data due to the statutory tasks of the CBA. Based on this judgment, the CBA Act was thoroughly amended. This amendment introduced to the CBA somewhat independent, internal control of the rights related to the collection and processing of personal data.

The Constitutional Tribunal judgment of July 30, 2014 (No. K 23/11), which was issued after the Snowden revelations, could have had a similar impact. In this case, the tribunal ruled at the request of the Polish Ombudsman comprehensively concerning surveillance powers. In this judgment, the tribunal specified essential principles that must be jointly met by provisions that regulate acquiring information on individuals in secrecy by public authorities in a democratic state ruled by law. The judgment required the introduction of changes in the law, which concerned the introduction of a mechanism of independent oversight over access to telecommunications data by police and special services officers; clarification in the law of the types of crimes detrimental

to the economic foundations of the state, in respect of which the ABW may conduct surveillance control; introduction of a mechanism guaranteeing the protection of attorney–client privilege; and introduction of a procedure for the destruction of redundant telecommunications data. Furthermore, the tribunal's judgment contained many recommendations regarding limitations on the use of operational surveillance.

As noted above, the 2016 Surveillance Act implemented some recommendations included in this judgment. The difference from previous rulings of the Constitutional Tribunal lies in the fact that this judgment was only partially implemented—the Polish legislature did not include the essential principles of secret surveillance. Moreover, the Surveillance Act introduces other legal specifications that the Constitutional Tribunal's judgment did not require or refer to at all (Bodnar et al. 2019). In February 2016, the Polish Ombudsman referred the most important provisions of the Surveillance Act to the Constitutional Tribunal. In his words, the reform not only fails to execute the judgment of the Constitutional Tribunal of 2014, but also "seriously violates the constitutional rights and freedoms and the standards set out in international law."[12] According to the ombudsman, in the Polish legal system there is still a shortage of legal safeguards that would ensure that surveillance measures do not violate fundamental rights. However, in March 2018, the ombudsman withdrew his application from the Constitutional Tribunal. He stated there was no chance of an independent and substantive judgment of the Constitutional Tribunal. This decision is related to the dispute surrounding the Constitutional Tribunal in Poland. The withdrawal of the application is significant if we take into account the role of the Constitutional Tribunal in limiting the powers of surveillance. Until now, it has been one of the key institutions that make up the oversight system of police and intelligence services. In the same year, the ombudsman withdrew the motions for all legal changes discussed in part one of the work: the Code of Criminal Procedure (April 2018–Article 168a and May 2018–Article 168b); the Anti-terrorism Act (April 2018); and the Act on the Prosecutor's Office (October 2018). The reason for all these decisions was changes in the composition of the previously appointed Constitutional Tribunal and the fact that unauthorized persons were appointed on political grounds.

Conclusion

A culture of secrecy still dominates Polish surveillance policy. This is connected with the still-dominant logic and interests of the security services, as secret surveillance is primarily used to combat crime and other threats to national security in an effective way. Such an approach is supported by the government, which has limited the influence of alternative expert knowledge. Ultimately, this leads to the adoption of laws that provide extensive surveillance powers without sufficient institutional or administrative mechanisms to govern surveillance practices and prevent abuse.

The pressure toward a more transparent approach to surveillance is still weak due to many factors. The political opposition still has a limited influence on the shape of surveillance law. Public opinion has little interest in this issue, which weakens potential pressure on the government. Also, independent oversight, which only exists formally, does not play any substantial role; it does not allow reliable conclusions based on verifiable facts, and it falls short of professional control mechanisms with appropriate substantive facilities and proper procedures. In addition to all this, the activities of the Constitutional Tribunal—which has in the past played an important role in limiting surveillance and protecting rights—have recently been paralyzed, resulting in a continued imbalance between transparency and secrecy in surveillance.

Notes

1 The Act of 15 January 2016 Amending the Police Act and certain other acts (the so-called Surveillance Act).
2 Act of 11 March 2016 amending Code of Criminal Procedure and other acts, Journal of Laws, item 437.
3 Act of 28 January 2016 Law on Prosecutor Office, Journal of Laws of 2017, item 1767 as amended.
4 Act of 10 June 2016 on antiterrorist action, Journal of Laws of 2018, item 452 as amended.
5 Act of 6 June 2016 on antiterrorist action, Journal of Laws of 2018, item 452 as amended.
6 Article 9 of Act of 10 June 2016 on antiterrorist action, Journal of Laws of 2018, item 452 as amended.
7 Article 26 of Act of 10 June 2016 on antiterrorist action, Journal of Laws of 2018, item 452 as amended.
8 In 2014, the NIK ran an oversight of control regarding special services (ABW, AW, CBA, and others). Due to classified data protection, the results were never disclosed. They only issued one public statement, which claims that rules in force limit the Prime Minister's power to control special services effectively.
9 Article 95, second paragraph of the Constitution of the Republic of Poland of April 2, 1997 (Journal of Laws, no. 78, item 483 as amended) states that the Sejm is responsible for government oversight.
10 Fieldwork for national sample: April 2016, N = 1104. The random address sample is representative of the adult population of Poland. For more information see CBOS 2016.
11 The Act of September 6, 2001 on Access to Public Information, Journal of Laws of 2019, item 1429.
12 The Commissioner for Human Rights application, No K 9/16, p. 6.

References

Aldrich, Richard J., and Daniela Richterova. 2018. "Ambient Accountability: Intelligence Services in Europe and the Decline of State Secrecy." *West European Politics*, 41(4): 1003–24.

Bigo, Didier. 2012. "Security, Surveillance and Democracy." In *Routledge Handbook of Surveillance Studies*, edited by Kirstie Ball, Kevin D. Haggerty, and David Lyon, 277–84. New York: Routledge.

Bodnar, Adam, and Katarzyna Szymielewicz. 2013. "Poland's Citizens Need to Know the Impact of Prism on Their Lives." *The Guardian*, 16 October, www.theguardian.com/commentisfree/2013/oct/16/poles-prism-poland-surveillance-threat.

Bodnar, Adam, Tomasz Borkowski, Jacek Cichocki, Wojciech Klicki, Piotr Kładoczny, Adam Rapacki, and Zuzanna Rudzińska-Bluszcz. 2019. "Osiodłać Pegaza: Przestrzeganie praw obywatelskich w działalności służb specjalnych–założenia reformy [How to Saddle Pegasus: Observance of Civil Rights in the Activities of Security Services: Objectives of the Reform]." Warsaw: Commissioner for Human Rights, www.rpo.gov.pl/pl/content/powolajmy-niezalezna-instytucje-do-nadzoru-sluzb-specjalnych-propozycja-ekspertow-i-rpo.

Born, Hans, and Gabriel G. Mesevage. 2012. "Introducing Intelligence Oversight." In *Overseeing Intelligence Services. A Toolkit*, edited by Hans Born, and Aidan Wills, 3–22. Geneva: DCAF.

Caparini, Marina. 2014. "Comparing the Democratization of Intelligence Governance in East Central Europe and the Balkans." *Intelligence and National Security*, 29(4): 498–522.

CBOS–Public Opinion Research Center. 2016. "Internet Surveillance." May 2016, www.cbos.pl/EN/publications/reports/2016/072_16.pdf.

Court of Justice of the European Union. 2013. "Case of ZZ v. Secretary of State for the Home Department." Judgment of 4 June, 2013 (no.C-300/11).

Court of Justice of the European Union. 2014. "Case of Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources, Minister for Justice, Equality and Law Reform, Commissioner of the Garda Síochána, Ireland, The Attorney General and Kärntner Landesregierung, Michael Seitlinger, Christof Tschohl and Others." Judgment of 8 April, 2014 r. (no. C-293/12 and C-594/12).

Court of Justice of the European Union. 2016. "Case of Tele2 Sverige AB v. Post-Och telestyrelsen oraz Secretary of State for the Home Department v. Tom Watson, Peter Brice, Geoffrey Lewis." Judgment of 21 December, 2016 (no. C-203/15 and C-698/15).

European Court of Human Rights. 2018. "Case of Big Brother Watch and Others v. The United Kingdom." Judgment of 13 September, 2018 (application nos. 25198/0258170/13, 62322/14 and 24960/15).

FRA–European Union Agency for Fundamental Rights. 2017a. *Surveillance by Intelligence Services: Fundamental Rights Safeguards and Remedies in the EU. Volume I: Member States' Legal Frameworks*. Luxembourg: Publications Office of the European Union.

FRA–European Union Agency for Fundamental Rights. 2017b. *Surveillance by Intelligence Services: Fundamental Rights Safeguards and Remedies in the EU. Volume II: Field Perspectives and Legal Update*. Luxembourg: Publications Office of the European Union.

Gill, Peter, and Mark Phythian. 2018. *Intelligence in an Insecure World*. Cambridge-Medford: Polity Press.

Grabowska-Moroz, Barbara. 2016. "National Intelligence Authorities and Surveillance in the EU: Fundamental Rights Safeguards and Remedies, Legal Update Poland." https://fra.europa.eu/sites/default/files/fra_uploads/poland-study-data-surveillance-ii-legal-update-pl.pdf

Gruszczak, Artur. 2009. "The Polish Intelligence Services." In *Geheimdienste in Europa. Transformation, Kooperation und Kontrolle*, edited by Thomas Jäger and Anna Daun, 126–51. Wiesbaden: FRG: VS Verlag für Sozialwissenschaften.

Gruszczak, Artur. 2017. "The Polish Intelligence Services and Security Dilemmas of a Frontline State." *Romanian Intelligence Studies Review*, 17–18: 65–80.

Hillebrand, Claudia. 2012. "The Role of News Media in Intelligence Oversight." *Intelligence and National Security*, 27(5): 689–706.

Kolaszyński, Mateusz. 2019. "Surveillance Powers of Law Enforcement and Intelligence Services in Poland." In: *Security Outlook 2018*, edited by Artur Gruszczak, 127–41. Kraków: Księgarnia Akademicka.

Kolaszyński, Mateusz. 2018. "Intelligence Control and Oversight in Poland since 1989." *The International Journal of Intelligence, Security and Public Affairs*, 20(3): 230–51.

Kovanic, Martin, and Aneta Coufalova. 2019. "The Legitimacy of Intelligence Surveillance: The Fight Against Terrorism in the Czech Republic and Slovakia." *Intelligence and National Security*, 34(6): 115–30.

Lefebvre, Stéphane. 2016. "Poland's Attempts to Develop a Democratic and Effective Intelligence System, Phase 1: 1989–1999." *International Journal of Intelligence and Counterintelligence*, 29(3): 470–502.

Łoś, Maria. 1995. "Lustration and Truth Claims: Unfinished Revolutions in Central Europe." *Law and Social Inquiry*, 20(1): 117–61.

Matei, Florina C., and Thomas Bruneau. 2011. "Intelligence Reform in New Democracies: Factors Supporting or Arresting Progress." *Democratization*, 18(3): 602–30.

Persak, Krzysztof, and Łukasz Kamiński. 2005. *A Handbook of the Communist Security Apparatus in East Central Europe: 1944–1989*. Warsaw: Institute of National Remembrance.

Radziewicz, Piotr. 2004. "Glosa do wyroku Trybunału Konstytucyjnego z 20 kwietnia 2004 r. (sygn. akt K 45/02) [Gloss to the Verdict of the Constitutional Tribunal of April 20, 2004 (Act Call No. K 45/02)]." *Przegląd Sejmowy*, 65(6): 163–71.

Rojszczak, Marcin. 2021. "Surveillance, Legal Restraints and Dismantling Democracy: Lessons from Poland." *Democracy and Security*, 17(1): 1–29.

Rzepliński, Andrzej. 2003. "Security Services in Poland and Their Oversight." In Democracy, *Law and Security: Internal Security Services in Contemporary Europe*, edited by Jean P. Brodeur, Peter Gill, and Dennis Töllborg, 110–40. Burlington: Ashgate.

Sarnecki, Paweł. 2010. "Dostęp do akt dokumentujących działania podjęte przez służby specjalne [Access to the Files Documenting Activities Taken by Special Services]." In *Regulamin Sejmu w opiniach Biura Analiz Sejmowych: Vol.* 2 [*The Sejm Regulations According to the Bureau of Research of the Chancellery of the Sejm: Vol.* 2], edited by Wojciech Odrowąż-Sypniewski, 128–30. Warsaw: Wydawnictwo Sejmowe.

Svenonius, Ola, and Fredrika Björklund. 2018. "Explaining Attitudes to Secret Surveillance in Post-Communist Societies." *East European Politics*, 34(2): 123–51.

Svenonius, Ola, Fredrika Björklund, and Paweł Waszkiewicz. 2014. "Surveillance, Lustration and the Open Society: Poland and Eastern Europe." In *Histories of State Surveillance in Europe and Beyond*, edited by Kees Boersma, Rosamunde van Brakel, Chiara Fonio, and Pieter Wagenaar, 95–117. London and New York: Routledge.

Venice Commission–European Commission for Democracy Through Law. 2016. "Opinion on the Act of 15 January 2016 Amending the Police Act and Certain Other Acts." Strasbourg, June 13, 2016 (Opinion no. 839/2016).

Wegge, Njord. 2017. "Intelligence Oversight and the Security of the State." *International Journal of Intelligence and Counterintelligence*, 30(4): 687–700.

Wetzling, Thorsten, and Kilian Vieth. 2018. "Upping the Ante on Bulk Surveillance: An International Compendium of Good Legal Safeguards and Oversight Innovations." *Heinrich Böll Stiftung*, www.stiftung-nv.de/en/publication/upping-ante-bulk-surveillance-international-compendium-good-legal-safeguards-and.

Widacki, Jan. 1999. "System bezpieczeństwa wewnętrznego: ewolucja struktur i funkcji [System of Internal Security: An Evolution of Structures and Functions]." In *Druga fala polskich reform* [*The Second Wave of Polish Reforms*], edited by Lena Kolarska-Bobińska, 216–40. Warsaw: Institute of Public Affairs.

Zybertowicz, Andrzej. 2007. "Transformation of the Polish Secret Services: From Authoritarian to Informal Power Networks." In *Democratic Control of Intelligence Services: Containing Rogue Elephants*, edited by Hans Born and Marina Caparini, 65–82. Hampshire and Burlington: Ashgate.

Chapter 8

Legal safeguards and oversight innovations for bulk surveillance

An international comparative analysis

Thorsten Wetzling and Kilian Vieth

Introduction

All democratic countries rely on intelligence agencies to keep their open societies safe. These agencies provide actionable intelligence to decision-makers on a wide range of security and foreign policy matters. Regardless of whether this concerns terrorism, arms proliferation, or organized crime, information is required beyond that which is publicly available. Intelligence services master a range of clandestine methods to acquire such information. Some methods—including the electronic surveillance of communications data—are difficult to reconcile with the fundamental principles of democratic governance, such as the rule of law, transparency, and accountability. They may also infringe on fundamental human rights and civil liberties, such as the right to privacy as well as the rights to freedom of opinion, of expression, of association, and of assembly. In order to ensure public trust and the legitimacy of intelligence governance, democracies need to place all intelligence activities on a solid legal footing and subject them to rigorous and effective oversight.

The democratization of intelligence and the professionalization of oversight have made significant advances over the last few decades in many established democracies. Parliaments in Europe, North America, and Australasia, for example, have frequently reformed national intelligence laws and extended the remit and the resources of independent oversight bodies over time. In addition, countries such as the United States have introduced transparency principles that commit the intelligence community to providing more information to the public than at any previous time in history (Office of the Director of National Intelligence 2015). Still, as the failures of effective oversight of electronic surveillance prior to the revelations of Snowden have shown, democratic intelligence governance cannot be taken for granted. The stakes are high, and the temptations to abuse privileges such as government secrecy are omnipresent. Effective governance and democratic control of intelligence is the result of a complex, multifaceted effort that cannot be left to a small group of technocrats. Put simply, when democracies allow their intelligence services to deploy digital surveillance powers in the name of national security,

DOI: 10.4324/9781003120827-11

they have to do this within the rubric of the rule of law and checks and balances. And while cultural, political, and constitutional differences across nations render it futile to establish a one-size-fits-all intelligence governance blueprint, it is certainly worthwhile to study how common challenges are met across different systems and to identify and promote innovative solutions so that they may traverse national jurisdictions.

In this chapter, we focus on the bulk surveillance of foreign communications. By this we mean the interception, collection, management, and transfer of enormous troves of communications data that is transmitted via different telecommunications networks (fixed telephone lines, mobile networks, the internet, and satellite networks). Foreign communications are intercepted as electronic signals, comprising various types of metadata as well as content. Bulk surveillance is controversial because it is "non-targeted" or "unselected" or "general"—in other words, not directed at a particular individual. David Anderson, the former UK Reviewer of Terrorism Legislation, warned that the use of bulk powers may have serious adverse human rights implications: such powers

> involve potential access by the state to the data of large numbers of people whom there is not the slightest reason to suspect of threatening national security or engaging in serious crime […] any abuse of those powers could thus have particularly wide ranging effects on the innocent […] even the perception that abuse is possible, and that it could go undetected, can generate corrosive mistrust.
>
> (Anderson 2016, 120)

Bulk surveillance of (foreign) communication has been a standard intelligence practice for decades. Greater public interest in the wake of the Snowden revelations, and the fact that many countries lacked a robust legal framework for it, let alone effective oversight thereof, have led many parliaments to adopt new laws or to amend existing legislation since then. Now that a sweep of new laws, oversight institutions, and control practices are in place it is time to take the national governance regimes at face value. While pending litigation at both national and European courts may still prompt a redesign of some intelligence laws, the very practice of bulk surveillance of communications is unlikely to be abandoned. Quite the contrary, it is here to stay and will remain a key practice of modern intelligence.

This makes it even more important to identify good solutions to the many thorny governance challenges entailed. This is what we aim to provide with our compendium, which we outline here. The full compendium, published by the Heinrich Böll Foundation and available online (Wetzling and Vieth 2018; Wetzling et al. 2020), identifies and contextualizes legal provisions and oversight practices from different democracies on bulk foreign communications surveillance that—by comparison—stand out for either their compatibility

with democratic governance, the rule of law, or the protection of human rights. They are also seen as good practices when they embody an innovative attempt to improve the effectiveness of oversight.

We believe that all countries stand to benefit from a thorough discussion of the growing acquis of good practices regarding the governance and oversight of bulk surveillance of (foreign) communications. Despite the relevant and legitimate criticisms that can be directed at recent intelligence reforms (Lubin 2018), most of them also brought about individual changes that embody significant improvements in governance. When taken together, these promising practices paint a unique picture, which, in turn, can help identify opportunities for progress in national frameworks. Obviously, it takes knowledge to develop a reform agenda and political will to overcome national shortcomings. Yet, if other countries successfully demonstrate that the sky did not fall when they implemented more ambitious solutions to particular governance challenges, then this can be used as a powerful argument to persuade others to follow suit.

Methods

When democracies allow their intelligence services to conduct large-scale electronic surveillance of foreign communications data, they must do so within the limits of the law. They must also ensure that this practice is subject to effective and independent oversight. Yet, what does that mean in practice, and how can one best distinguish between good and poor legal safeguards and efficient and inefficient oversight dynamics?

To find out, we studied a wide range of different public resources, such as commentary on intelligence laws, oversight body reports, strategic litigation materials, as well as commentary on intelligence policy. We developed a scheme of analysis and conducted a series of interviews with a range of different experts (legal scholars, computer scientists, public servants and oversight professionals, industry representatives, etc.) to obtain further information on current practices (see the methodology section in Wetzling et al. 2020). Once we collected enough information, we wrote a draft compendium and organized two expert focus groups to further test and refine our findings. Based on this work, we produced a compendium of *good practices on bulk surveillance of (foreign) communications* from different national intelligence laws and oversight systems across Europe, North America, and Australasia, upon which this chapter is based.

Our focal points were the legal frameworks and oversight regimes regarding nontargeted signals intelligence (SIGINT), with a special emphasis on foreign communications data. This provides intelligence services "mass access […] to data from a population not itself suspected of threat-related activity" (Forcese 2018, 3). Unsurprisingly, then, nontargeted (or "bulk") SIGINT capabilities are often considered to be the "crown jewels" of a national intelligence

community. It is a technically sophisticated and highly complex intelligence-gathering discipline that involves a lot of international cooperation and grew in the shadows of many democracies for quite some time.

What are the relevant aspects that one needs to consider when it comes to creating a legal basis for—and the democratic control of—bulk surveillance? According to what standards and criteria can we assess the quality of either a legal provision or an oversight practice? We consider a practice to be good when, by comparison, it provides an improved safeguard against potential violations of rights, or because it stands out in the way that it solves a common governance challenge, or because it may make innovative use of technology for the benefit of greater oversight effectiveness. Whether or not these standards are then observed in actual practice is another story. This needs to be independently and effectively reviewed based on the actual dynamics of judicial oversight as well as its resources, legal mandate, and technological tools.

Building blocks of the good practice compendium

This chapter devotes a section to each of the eight phases of bulk surveillance governance: (1) strategic planning, (2) application process, (3) authorization, (4) collection and filtering, (5) data processing, (6) analysis, (7) review and evaluation, and (8) reporting. For each phase we discuss good practice recommendations based on actual empirical examples adopted in particular countries; the full compendium available online includes references to specific examples of existing legal safeguards and concrete oversight practices from different systems up to the year 2019.[1]

Phase 1: strategic planning

The first phase of the SIGINT process involves the identification and formulation of certain intelligence needs. Ideally, strategic planning will also draw on insights from previous assessments of collected intelligence and their value after analysis. A clear and specific legal mandate is the precondition for the transparency and accountability of foreign intelligence gathering. The mandate should describe specific legal grounds, against which the permissibility and proportionality of a particular measure can be assessed. It should also stipulate what data sources or types of communications may and may not be included in SIGINT collection.

According to jurisprudence by the European Court of Human Rights and the Court of Justice of the European Union, bulk surveillance is only permissible when it is strictly necessary to protect the democratic institutions of society (European Court of Human Rights 2015, 2016, 2018a, 2018b; Court of Justice of the European Union 2016). This indicates that intelligence services of signatory countries of the European Convention of Human Rights

and the European Union Charter of Fundamental Rights may only engage in bulk collection techniques in relation to clearly confined categories of serious threats to a democratic society. These categories ought to go beyond a general understanding of what constitutes a serious threat.

The actors involved in setting intelligence priorities play a significant role here. There may be both external planning and tasking by government officials or ministers outside the service, and internal planning and tasking by the services. External planning and tasking traditionally focus more on a strategic/political level, whereas internal planning typically includes a stipulation of data sources or types of communications.

Good practices provide answers to questions such as: who can influence and challenge the tasking process? Does an evaluation of previous intelligence cycles feed into the planning of future intelligence collection? If so, how? When it comes to the formulation of concrete intelligence needs, does the process allow those with adversarial positions to challenge what may be taken for granted? Matters concerning cooperation with foreign intelligence agencies must also be addressed at this stage: will the need for cooperation with foreign services be weighed against other factors, such as human rights obligations and other national security interests? If so, how?

The compendium identifies four good practices from existing legal safeguards across a number of different countries. These include: laws ending discrimination based on citizenship; clear rules for setting intelligence priorities; regulating international cooperation; and prohibition of objectives that may not be advanced through bulk collection.[2]

Setting strategic goals and formulating operational priorities is a core competence of the executive. Consequently, we found only very limited involvement of oversight bodies in the tasking and planning phases. Privacy International also found recently that no intelligence oversight body currently possesses the power to authorize decisions to share intelligence (Privacy International 2018). Clearly, this invokes not just legal and operational questions but also political ones. Can a government sufficiently trust a foreign service to engage in new cooperations? Nonetheless, some oversight bodies have recently taken an interest in reviewing the tasking of and cooperation between intelligence services.

Phase 2: application process ("warrantry")

With a warrant, the intelligence service (or, as the case may be, the ministry performing executive control over a particular intelligence service) submits an application for authorization to collect data in bulk. Warrants need to describe and delimit bulk SIGINT measures based on specific criteria regarding both the form and content of the warrant that are set out in law. Warrants are a core element of accountability in intelligence governance, although they have to provide detail and particularity in order to constitute an effective safeguard against overly intrusive surveillance authorities.[3]

In the SIGINT world, warrants might therefore be tied to classes of individuals or activities rather than specific persons. Some jurisdictions apply much stricter limits to the legal concept of a warrant. In the United States and Canada, for instance, warrants always refer to targeted surveillance operations that involve a judge, who has to authorize them. A range of countries in Europe only apply the concept of warrants to criminal investigations and not to intelligence collection. In this conventional understanding, "bulk powers are irreconcilable with the requirements of classic warrants. There is no specificity. By definition, bulk powers are not targeted; they are indiscriminate" (Forcese 2018, 3). Under the United Kingdom's Investigatory Powers Act, on the other hand, the term "warrant" is used for different types of applications for bulk interception or acquisition of data. This, then, implies a class-based warranty system, in which large categories of data can be collected.

Although the terminology is tricky and warrants for untargeted collection or bulk surveillance are not a feature of some legal systems, they are included here as a useful comparative category. Warrants can be a powerful tool to specify the minimization rules, the authorization requirements, and the purpose limitations of a measure. The more specificity a bulk warrant can provide, the better its protective function. Warrants may also be used to exclude certain data categories from collection and limit the use of the data collected. It is important to note that many such limits and conditions could appear in a law governing intelligence surveillance. The major advantage of warrants, though, is the active involvement of an independent judicial authorization body *before* the collection begins (see phase 3), which allows for case-by-case controls. Ideally, a clear legal mandate is combined with obligatory, independent, *ex ante* controls of all applications for bulk data collection.

Warrants also often define the duration of an operation for a specific collection method. This, in turn, triggers a mandatory reassessment of the measure, and potentially the subsequent reapplication and reauthorization. Setting an expiration date is, hence, an accountability mechanism as well as a regular efficacy test that helps to ensure the efficient allocation of resources by the agencies.

Naturally, the more targeted an envisaged surveillance operation, the more specific the warrant can be formulated. Given the focus of this chapter, that is, safeguards and oversight innovation regarding nontargeted communications surveillance, we mostly reviewed types of "bulk" warrants. That said, interesting features in targeted surveillance warrants might be discussed when applicable to the sphere of untargeted collection.

It is common for various intelligence laws to include a list of criteria that each application for a SIGINT measure needs to address. Ideally, these include:

- Purpose(s) of the requested activity;
- Alternative means available;

- Private companies that may be compelled to cooperate;
- Service or services that will be instructed to perform the activity;
- Time frame for assessment and authorization of the warrant, including for emergency situations;
- Geographical zones or organizations or groups of people that a particular measure is directed at;
- Technical device or facility to be tapped;
- Exploratory monitoring or preliminary aptitude tests that have been conducted in preparation;
- Type(s) of data to be retrieved;
- Search terms or selectors used (i.e., a range of IP addresses);
- Types of data use and forms of data exploitation to be performed on the data;
- Duration of the warrant and rules for renewal; and
- Additional background materials to be submitted with the warrant.

The various forms of bulk warrants that now exist in many countries highlight the potential for even broader applications of this accountability mechanism in the field of foreign communications surveillance. There is a need to think more creatively about further relevant criteria and additional aspects that add more precision to bulk warrants. For example, lawmakers could ask the executive to specify the actual use of minimization procedures and how the intelligence services intend to honor data-use limitations.

Phase 3: authorization/approval

After a warrant has been issued, the requested bulk SIGINT measure must be authorized or—as the case may be in different jurisdictions—approved by a review body that assesses the necessity and proportionality. Differences exist across nations as regards the moment when the independent judicial review process comes into play. In some countries, the competent minister or other members of the executive authorize warrants. In the United Kingdom, for example, the *authorization* of warrants is the privilege of the executive. Ministerial authorization, then, has to be *approved* by independent Judicial Commissioners. By contrast, in the German legal framework, warrants are *authorized* by bodies such as the G10 Commission or the Independent Committee.

The independent *ex ante* authorization/approval of data collection is a crucial safeguard against the misuse and abuse of bulk surveillance powers. The legitimacy of surveillance practice depends on the control of executive conduct from the outside. Enacting the control mechanism *prior* to implementation is crucial, because this can both deter and prevent certain actions from being taken. Independent authorization/approval also contains an important learning element, because the competent bodies can improve their controls,

draw lessons from past mistakes, and then declare more assertively that certain measures are not required, or that no sufficient proof was presented.

Across many democracies, a dual system of authorization/approval has emerged that combines a judicial and an executive control function. A judicial oversight body—ideally a court—is best suited to administer a competent legal review of a bulk surveillance application. But, as several discussions with intelligence oversight practitioners have shown, the involvement of the political leadership level, for example, the responsible minister or secretary of state, may also present a relevant safeguard, especially in the realm of foreign intelligence. The acceptance of a surveillance operation may go beyond legal criteria of necessity and proportionality and move into the political domain. Including political considerations, such as possible damage to diplomatic relations with a foreign country, may add an important perspective to the authorization process.

The complexity and confidentiality of the subject matter require that the authorization body be sufficiently qualified (e.g., a specialized court for SIGINT operations) and have the necessary powers and resources to conduct the authorization (e.g., access to all relevant information) (European Court of Human Rights 2015, 275). A fundamental requirement for an authorization/approval body is its independence. Further relevant aspects include:

- Who is involved in the authorization process?
  - How is the independence of the authorization/approval ensured? For example, unified, fully resourced authorization bodies with full access rights are far better equipped to conduct comprehensive reviews.
- When does the review take place? Prior to, or after the implementation of bulk surveillance measures?
- How does the authorization take place?
  - Are all warrants independently authorized, or does the law account for exceptions? For example, are there any exceptions for emergency procedures? If so, are they designed so that they do not unduly open up loopholes for unauthorized operations?
  - What assessment criteria are being used?
  - How explicit are the oversight bodies as regards the use of criteria to assess the legality, necessity, and proportionality in concrete practice?
  - How much time does the oversight body have to assess a warrant?
- Does the law foresee an appeal procedure?
  - Are the authorization decisions legally binding?
  - Is technical and adversarial advice incorporated into the authorization process? If so, how?
- Do the warrants also account for metadata and "secondary data" (Smith 2018)?
- Does the authorization take other (ongoing) surveillance measures into account when assessing a new warrant?

- How is the authorization decision documented? Are there publicly available statistics on the number of rejections and the total number of applications reviewed?

Current good practices in existing legal safeguards include laws that provide a margin of discretion for authorization bodies; mandatory public reporting on individual authorization decisions; adversarial proceedings that provide additional input legitimacy to the authorization/approval decision process; quotas for maximum permissible number of certain surveillance instruments. Good oversight practices include explicit standards for proportionality assessments when approving bulk SIGINT warrants in actual practice. For a detailed discussion of the relevant legislation supporting these practices, see the full compendium (Wetzling and Vieth 2018; Wetzling et al. 2020).

Phase 4: collection and filtering

Once a warrant has been authorized or approved, an intelligence agency can proceed with the implementation of a particular surveillance measure. For this, it intercepts the relevant signals, for example, by tapping an internet service provider's (ISP) fiber optic backbone cable or diverting data at an internet exchange point. Afterward, the collected data has to be filtered for two reasons: first, because of the huge volumes passing through—which would be far too much to be stored long term—gratuitous data that is extremely unlikely to yield any intelligence value is filtered out (e.g., all data from public video feeds); second, the collected data stream has to be filtered so as to abide by legal requirements. Certain data—for example, domestic communications or communications involving lawyers, priests, or other professions relying on the confidentiality of correspondence—may be offered higher levels of protection in national surveillance laws.[4]

Collection

At the collection point, it is critical to clearly define who is in charge of extracting the data and where and how the extraction devices may be installed. Is the collection administered by the intelligence service, or do private entities (e.g., ISPs) do this on behalf of the intelligence services? This distinction is relevant, as provider intermediation can be an important safeguard against overcollection. In principle, intelligence agencies should not have direct access to the facilities of telecommunications providers. Cases have surfaced, however, in which internet companies agreed to search the data they administer on behalf of an agency. Yahoo, for example, secretly scanned all email accounts for information provided by US intelligence agencies (Menn 2016). A legal framework, therefore, has to define how (private) intermediaries may be compelled to cooperate and what means are available for operators to challenge particular measures.

A number of European countries have installed electronic interfaces that give oversight bodies direct access to operational systems and collected data. Such direct access can be an important innovation for oversight, but it also entails risks that have to be addressed. The advantage of direct access to databases is that the oversight body can conduct random checks, unannounced inspections, and potentially also automated controls on the data handling by the intelligence agencies. This has the potential to level the playing field between the controller and the controlled. Traditionally, oversight bodies depend, to a large extent, on the information provided by the intelligence services. If overseers gain direct access, the incentive to comply increases because intelligence officials cannot know whether an incident will be reviewed or not. Technical interfaces might also empower review bodies to monitor statistical anomalies in the databases. This opens a new field of (automated) oversight applications that will support overseers in effectively diverting their limited resources for in-depth compliance auditing. Such an approach—using analytical techniques to identify potential noncompliance—amounts to "predictive oversight" and is already being practiced by institutions entrusted with financial audits in the banking sector.[5]

Granting direct, unfettered access for oversight bodies to the intelligence databases may, however, turn them into attractive targets for foreign espionage and hacking attacks. It is important, therefore, to only grant such access to properly trained oversight personnel and to provide the highest level of cybersecurity to oversight bodies.

Making sense of raw intelligence data and log files is hard. It is not enough for oversight bodies to merely have access. The information advantage that direct access may bring comes from data analytics. In other words, oversight bodies need to engage with the data that they now have access to. In order to learn how much more rigorous their controlling could become, overseers may want to learn from financial audit bodies and will need special training.

Filtering

Once data has been acquired by means of untargeted electronic surveillance, it may be subject to additional filtering, depending on the national surveillance regulations. The specifics of the data minimization and filtering processes should be subject to critical review, for they may reveal the extent to which intelligence agencies abide by constitutional and human rights standards. For example, some intelligence laws grant enhanced privacy protection to professions that depend on the confidentiality of information. This may pertain to communications involving priests, lawyers, journalists, and physicians. Whether and how data minimization and filter tools are capable of accommodating such communications in practice should be of interest to oversight bodies. This may also extend to the review of protected health data and DNA-related information.

In addition, there are technical questions that come to mind, as they, too, reveal interesting information about the independence of oversight bodies and the extent to which data minimization is an actual priority (or not) within the intelligence community. For instance, how is "surplus information" treated in the collection and filtering process? When data minimization systems, such as the Massive Volume Reduction (MVR) systems of the United Kingdom's Government Communications Headquarters (GCHQ), are being used, are they subject to independent oversight? More specifically, are the technical equipment and filter programs regularly subject to independent verification, or do the oversight bodies merely rely on the assurances of the intelligence agencies that the data minimization and filtering processes are fit for purpose?

The independent verification of data minimization techniques deserves greater attention from oversight bodies (Vieth and Wetzling 2019, 18ff). They ought to investigate the technical implementation of the filtering process and the independent auditing of filter effectiveness. Similarly, the deletion of data is an ongoing oversight challenge that many review bodies are gradually waking up to. Here, we find that mutual learning from regular exchanges with other oversight bodies in other countries and the promotion of systematic dialogues with external experts should be intensified.

Phase 5: data processing

Once data has been collected and filtered, it must be stored, tagged, and later removed or destroyed. This phase of the SIGINT process is particularly relevant for oversight and the services because lawful and efficient data management is the basis for relevant data analysis. For the sake of clarity, this phase is divided into four subcategories reflecting the different facets of data processing: storage, maintenance, sharing, and deletion.

Data storage

Due to different retention periods, it may become necessary to keep separate databases, for example, for encrypted data, metadata, and content data, or in order to distinguish data pools according to their legal basis or warranted purposes. It can therefore be relevant whether there are isolated data storage locations. Increasingly, bulk surveillance governance relies on the verifiable technical or institutional separation between the authority to intercept and the authority to analyze the data. In order to honor data protection obligations, a surveillance law should further restrict the extent to which databases may be linked or accumulated.

Transnational threats prompt closer transborder cooperation among intelligence services, not least for neighboring countries. Intelligence data—both unevaluated and evaluated—is therefore not just shared bilaterally but also stored in joint intelligence databases for different threats and purposes.

When we speak of *joint databases*, we refer to a multilateral exchange of data that can be hosted either on national territory or abroad. Typically, joint databases are run multilaterally, with all participating services adding and accessing data.

The European Counter Terrorism Group (CTG), for example, runs a database that facilitates the multilateral exchange of evaluated data on individuals who have traveled to and returned from certain conflict areas (CTIVD 2018, 10; see also van Eijk and Ryngaert 2017). This database became operational in July 2016, is administered on servers in the Netherlands, and makes information available in (near-) real time to the 30 participating services of the CTG. Interestingly, unevaluated data may also be exchanged within the CTG, although not via the database. It may be jointly stored and processed within standard SIGINT cooperations (CTIVD 2018, 9).

Existing good practices in legal safeguards include laws that protect all data categories and, in particular, that allow for no distinction between rules regulating metadata and content data retention since both are worthy of protection; explicit obligations regarding joint databases with foreign intelligence services, including obligations to keep a file classification scheme, appropriations clauses for joint databases, and equalized retention rules for citizens and noncitizens.[6]

Data maintenance

This comprises all practices that concern the labeling and registration of intelligence databases. Data upkeep is not only required by data protection regulations but also serves a practical end: it ensures that the services keep only relevant and accurate data.

Relevant aspects for good practices include: how is bulk data tagged? And what authority do data protection agencies have to investigate the sound implementation of databases? For auditing purposes, data must be traceable throughout the entire lifecycle. It is also important to anonymize data to the greatest extent possible. The security and quality of the databases must be ensured to protect sensitive information from being stolen or compromised. Adequate data maintenance also builds on clear restrictions of data access. Is the access to the stored data regulated by law and restricted to specialized personnel only? Or is data access for operational teams limited by data exploitation warrants (see phase 2)?

Existing good practices in legal safeguards include legally imposed *duty of care* with regard to data processing, including the use of algorithms, avoiding data breaches, and insuring the validity and integrity of processed data; the mandatory tagging of all bulk SIGINT data as a precondition for meaningful data protection controls. In terms of oversight, good practices include the obligation to perform regular reviews of intelligence registration and data processing.

Data sharing

Sharing data with foreign services entails a responsibility to assess and mitigate the risk of misuse of the shared data. Although SIGINT burden-sharing among partner services is a common practice, what rules and procedures are in place to evaluate partner services' data quality and data veracity? Oversight of—and accountability for—data-sharing agreements and joint databases must be ensured. Finally, in times of advanced joint intelligence databases, how do oversight bodies cooperate internationally to control the permissible use of international data pools? Current good practices include rules for oversight body access to shared data and random sample checks on automatic transfers of personal data to foreign intelligence services.

Data deletion

The proper deletion of data is an enormous challenge. Technically, it is not as easy as one may think to securely "get rid" of data. This is because "deleting" a file typically only marks the space it occupies as usable. Until the disk space is overwritten, the data is still there and can be retrieved. To ensure that the deleted data cannot be retrieved any longer, the physical records on a storage medium must be overwritten with other data several times (minimum of seven times as per the US Federal government's guidelines) (Dorion 2008). But simply overwriting the storage space on a physical medium with new data does not necessarily guarantee that none of the old data is gone for good. Although there are technical means to ensure that deleted data is actually unretrievable, it seems necessary to develop more detailed standards for what constitutes the proper deletion of data. Errors in this process could result in millions of datasets being falsely stored for years.

Moreover, it is now also "more costly to delete data, than retain it" (OECD 2013, 100). Therefore, legislators have found it difficult to insert the proper legal definitions or public standards for what "deletion" or "destruction" of data means into intelligence laws.[7] By extension, then, the deletion problem also becomes a veritable oversight challenge. This is because review bodies need accurate audit trails to be able to check services' compliance with data deletion requirements. This may include the automated destruction of data after legal retention periods have lapsed or if the relevant authorization for collecting data has ended.

There is also a need for better guidelines on what data should be deleted at what point in time. Storage periods (see part one of phase 5 above), for that matter, define maximum times for which data may be retained. With adequate normative criteria at hand, the services or the competent oversight bodies could, theoretically, also decide to apply a shorter storage period. For example, if a system flags data that has not been used for a certain time period, this should then prompt a check as to whether this specific dataset is still needed.

Intelligence law should outline specific and short retention periods, after which the data must be permanently and unmistakably destroyed. There might be special requirements for the deletion of large amounts of data. For example, the NSA's XKeyscore system may have a rolling buffer so that new incoming data automatically overwrites the old data. It is also relevant how data destruction is documented and controlled by the competent oversight body. For example, is stored data linked to specific warrants, and does it have traceable time stamps for full and proper deletion? Adequate records of the data destruction are also important for possible notification purposes.

Relevant aspects for good practices include: how are storage and deletion implemented in practice? Should intelligence data be stored in "clouds"? Even in the sphere of national security, we witness close cooperation with commercial third parties, such as private cloud storage services (Konkel 2014). How can it be ensured that such outsourcing—entailing the risk of shifting responsibility for a crucial phase of data processing to private companies—does not undermine democratic accountability and oversight?

Existing legal safeguards include legal obligations to immediately delete data tied to rejected applications; obligations to destroy data from bulk collection that is deemed irrelevant; and obligations to delete health data in foreign datasets. Good existing oversight practices include running statistical pattern analysis on the amount of deleted material and independent review of compliance with deletion obligations.

Phase 6: analysis

A wide range of data use is relevant for this phase. There are, of course, overlaps between data processing and data analysis. Whereas data processing refers to data registration and other formal or technical data management practices, in this phase data becomes information that is relevant for political decision-making. Different automated data analysis methods serve different purposes and are governed by their own specific rules. Bulk datasets are used both to "establish links between known subjects of interest" as well as to "search for traces of activity by individuals who may not yet be known but who surface in the course of an investigation, or to identify patterns of activity that might indicate a threat" (UK Home Office 2017, 52). For example, contact chaining is one common method used for target discovery:

> Starting from a seed selector (perhaps obtained from HUMINT), by looking at the people whom the seed communicates with, and the people they in turn communicate with (the 2-out neighbourhood from the seed), the analyst begins a painstaking process of assembling information about a terrorist cell or network.
>
> (GCHQ 2011, 12)

Automated pattern analysis and anomaly detection increasingly rely on artificial intelligence (AI) methods such as machine learning and predictive analytics. "AI is expected to be particularly useful in intelligence due to the large datasets available for analysis" (Hoadley and Lucas 2018, 13). The risks and benefits generally associated with AI also challenge existing oversight methods and push legislators as well as oversight practitioners to creatively engage with AI as a dual-use technology. In intelligence, AI "is intended to automate the work of human analysts who currently spend hours sifting through data for actionable information. It may free them to make more efficient and timely decisions based on the data" (Hoadley and Lucas 2018, 9). Conversely, malicious use of AI creates new security threats that have to be mitigated (Brundage et al. 2018).

Good practices need to consider the following questions: what types of data use are permissible in a given legal framework, and are there specific rules for different forms of data use? For example, there should be procedures for each type of use, specifying the circumstances under which that specific use is permitted. There should also be independent oversight (internal and external) over bulk data analysis techniques, including rules and safeguards as concerns the use of AI. How is the level of privacy intrusion of specific data-analysis tools measured? And what kind of material is fed into query-focused databases? How is the convergence of different databases/data sources regulated? For example, may bulk communications data be matched with other stored data (such as data gathered via sensors or in hacking operations) or publicly available data? If so, does such enrichment of material happen automatically?

Current good legal safeguards include human-in-the-loop safeguards for automated data analysis that prohibit action on the basis of automated results alone, as well as legally required specialized training for analysts. Good oversight practices include automated internal compliance systems for data analysis and *ex ante* review of AI experiments and novel data analysis techniques.

Phase 7: review and evaluation

Compliance with legal safeguards must be ensured through comprehensive and regular judicial oversight. Examining the effectiveness of data collection measures is equally important. Overseers need to know about this to assess the political value, the cost efficiency, and the need for the reauthorization of warrants. Identifying suitable metrics and methods for this remains a considerable challenge. For example, if data from a certain program or collection stream never feeds into the production of intelligence reports, does this mean that the particular data collection is superfluous and a strain on the limited resources of the intelligence community? Or, in contrast, would this be tantamount to someone canceling a fire insurance policy simply because, thus far, their house has not caught fire?

The scope of the review mandate of the oversight body is a core factor. Effective review presupposes that there are no gaps in the control mandate. Control remits should be defined functionally, covering all aspects of intelligence collection, as recommended by the Council of Europe (Council of Europe 2015). Does the competent oversight body have the sufficient resources (staff, time, money, technical expertise) to conduct meaningful reviews? Intelligence law should also define the role for oversight in assessing the political relevance of finished intelligence operations and assign the duty to the executive branch to demonstrate the efficiency of its bulk surveillance measures, despite the ubiquitous presence of open-source information.

Existing good legal safeguards include laws that expand the scope of oversight and put in place a holistic review of SIGINT practices across different agencies; mandatory reauthorization of legislation and verification of effectiveness before renewal of authorization; and criminal liability for non-compliance with oversight requests. Good oversight practices include early and systematic oversight involvement; obligatory quarterly self-reporting of incidents to the Inspector General; and international cooperation of oversight bodies, including joint review and mutual learning sessions.

Phase 8: reporting

After a SIGINT collection cycle has been completed, both government and oversight bodies need to be transparent and provide adequate information about both the surveillance activities undertaken by the state and their specific oversight activities thereon. To enhance public trust, the intelligence services should proactively declassify key legal documents of public interest.[8] Such releases have, for example, allowed the creation of rare public and quite comprehensive accounts of different types and patterns of compliance violations over the duration of the Section 702 program.[9] Although full transparency of oversight activities may not be possible due to secrecy requirements, the regular reporting by oversight bodies is a crucial means for public trust and accountability. For this, it ought to be as comprehensive and timely as possible.

Relevant considerations include: what rules are in place regarding mandatory, periodical public reporting on surveillance measures and their democratic control? Information on oversight methods and capacities, especially with a view to bulk surveillance, should be provided to the greatest extent possible. Reports should draw a holistic picture of all intelligence activities. What contextual material and statistical information is provided to the public? What outreach activities are pursued, and how does the oversight body communicate with the public?

Existing good practices in legal safeguards include allowances for deviations from the norm of classification and options for declassification, and legal obligations to inform about errors. Good practices in oversight include

reporting on nonconformities with selectors; oversight bodies pushing for declassification; and institutional support and protection for whistleblowers.

Conclusion

Our initial review of legal safeguards and oversight innovations in different stages of the bulk surveillance governance process features 64 good practices. These range from ending discrimination based on citizenship to more specific authorization regimes and additional safeguards for international intelligence cooperation. Each pertains to different aspects of surveillance governance. More specifically, this includes:

- Restriction of bulk surveillance powers;
- Transparency;
- Access;
- Oversight professionalism;
- International cooperation;
- Direct government responsibility;
- Sanctions; and
- Private-sector involvement.

Reforms of bulk surveillance post-Snowden have been limited and underwhelming in the eyes of many observers. Yet, the debate about rights-based and democratically controlled surveillance governance is far from over. Although courts such as the European Court of Human Rights tend to grant a broad leeway to national governments to implement bulk surveillance, they also insist on adequate safeguards. What this means in practice, however, will not be decided by the courts. Rather, it involves the hard work of taking the lessons about ineffective oversight and applying better practices through the slow and steady channels of democratic institutions. In this spirit, we continue to collect and compare international good legal safeguards and promising oversight practices (Wetzling et al. 2020). This may not be the Snowden legacy that some expected. Yet, it is the difficult and necessary work of democratic governance.

Notes

1 An up-to-date collection of international good practices is available at: www.intelligence-oversight.org.
2 References to empirical examples in phase 1 can be found here: www.intelligence-oversight.org/phases/strategic-planning/.
3 Laura Donohue interviewed by Henry Farrell in Farrell (2016).
4 As established earlier, it is not always technically possible to filter out the communications of protected categories such as certain professions.

5 For a detailed analysis of potential applications for direct oversight access to operational surveillance systems, see Vieth and Wetzling (2019).
6 References to the individual good practices in the data processing phase are available at: www.intelligence-oversight.org/phases/data-processing/.
7 We are grateful to Professor Nico van Eijk, who presented valuable information on the legal and technical challenges of data deletion during our workshop on May 14, 2018.
8 The US intelligence community, for example, has released official documentation of intelligence activities and procedures, such as declassified FISC opinions, quarterly reports, and semiannual assessments. Many of these documents can be found at www.icontherecord.tumblr.com. A guide to released documents is available here: www.dni.gov/files/CLPT/documents/Guide_to_Posted_Documents.pdf. A searchable database of all documents is available at: www.intel.gov/ic-on-the-record-database.
9 Robyn Greene has compiled highly informative documentation that informs the public about how unintentional violations may threaten the privacy of protected communications over a longer period of time "with significant and prolonged impact" (Greene 2017). For a summary of compliance reports under Section 702 of FISA, see Greene (2017).

References

Anderson, David. 2016. "Report of the Bulk Powers Review." London: Independent Reviewer, https://terrorismlegislationreviewer.independent.gov.uk/wp-content/uploads/2016/08/Bulk-Powers-Review-final-report.pdf.

Brundage, Miles, Shahar Avin, Jack Clark, Helen Toner, Peter Eckersley, Ben Garfinkel, Allan Dafoe, et al. 2018. "The Malicious Use of Artificial Intelligence: Forecasting, Prevention and Migration." February 2018, https://arxiv.org/ftp/arxiv/papers/1802/1802.07228.pdf.

Council of Europe. 2015. "Democratic and Effective Oversight of National Security Services." Strasbourg, https://rm.coe.int/democratic-and-effective-oversight-of-national-security-services-issue/16806daadb.

Court of Justice of the European Union. 2016. "C-203/15 Tele2 Sverige AB v Post-Och Telestyrelsen and C-698/15 SSHD v Tom Watson & Others." December 2016, http://curia.europa.eu/juris/document/document_print.jsf?doclang=EN&text=&pageIndex=0&part=1&mode=lst&docid=186492&occ=first&dir=&cid=406338.

CTIVD–Commissie van Toezicht op de Inlichtingen-en Veiligheidsdiensten. 2018. "Review Report: The Multilateral Exchange of Data on (Alleged) Jihadists by the AIVD." CTIVD No. 56, https://english.ctivd.nl/documents/review-reports/2018/04/24/index.

Dorion, Pierre. 2008. "Data Deletion or Data Destruction?" *SearchDataBackup*. July 2008, https://searchdatabackup.techtarget.com/tip/Data-deletion-or-data-destruction.

Eijk, Nico van, and Cedric Ryngaert. 2017. "Expert Opinion—Legal Basis for Multilateral Exchange of Information," Appendix IV of CTIVD Rapport No. 56 to the Review Report on the Multilateral Exchange of Data on (Alleged) Jihadists by the AIVD, https://pure.uva.nl/ws/files/36129088/Expert_opinion_CTIVD.pdf

European Court of Human Rights. 2015. "Case of Roman Zakharov v. Russia (Application No. 47143/06)." Strasbourg, http://hudoc.echr.coe.int/eng?i=001-159324.

European Court of Human Rights. 2016. "Case of Szabó and Vissy v. Hungary (Application No. 37138/14)." Strasbourg, http://hudoc.echr.coe.int/eng?i=001-160020.

European Court of Human Rights. 2018a. "Case of Paul Popescu v. Romania (Application No. 64162/10)." Strasbourg, http://hudoc.echr.coe.int/eng?i=001-80353.

European Court of Human Rights. 2018b. "Case of Centrum För Rättvisa v. Sweden (Application No. 35252/08)." Strasbourg, http://hudoc.echr.coe.int/eng?i=001-183863.

Farrell, Henry. 2016. "America's Founders Hated General Warrants. So Why Has the Government Resurrected Them?" *Washington Post*, June 14, 2016, www.washingtonpost.com/news/monkey-cage/wp/2016/06/14/americas-founders-hated-general-warrants-so-why-has-the-government-resurrected-them/.

Forcese, Craig. 2018. "Bill C-59 and the Judicialization of Intelligence Collection. Draft Working Paper 04-06-18." *Ottawa Faculty of Law Working Paper No. 2018–13*.

GCHQ–Government Communications Headquarters. 2011. "HIMR Data Mining Research Problem Book." September 20, 2011, www.documentcloud.org/documents/2702948-Problem-Book-Redacted.html.

Greene, Robyn. 2017. "A History of FISA Section 702 Compliance Violations." *New America.* September 28, 2017, www.newamerica.org/oti/blog/history-fisa-section-702-compliance-violations/.

Hoadley, Daniel S., and Nathan J. Lucas. 2018. "Artificial Intelligence and National Security." *Congressional Research Service*. April 26, 2018, https://fas.org/sgp/crs/natsec/R45178.pdf.

Konkel, Frank. 2014. "The Details About the CIA's Deal with Amazon." *The Atlantic*, July 17, 2014, www.theatlantic.com/technology/archive/2014/07/the-details-about-the-cias-deal-with-amazon/374632/.

Lubin, Asaf. 2018. "Legitimizing Foreign Mass Surveillance in the European Court of Human Rights." *Just Security*, August 2, 2018, www.justsecurity.org/59923/legitimizing-foreign-mass-surveillance-european-court-human-rights/.

Menn, Joseph. 2016. "Exclusive: Yahoo Secretly Scanned Customer Emails for U.S. Intelligence Sources." October 5, 2016, www.reuters.com/article/us-yahoo-nsa-exclusive/yahoo-secretly-scanned-customer-emails-for-u-s-intelligence-sources-idUSKCN1241YT.

OECD–Organisation for Economic Co-Operation and Development. 2013. "The OECD Privacy Framework," www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf.

Office of the Director of National Intelligence. 2015. "US Principles of Intelligence Transparency for the Intelligence Community," www.dni.gov/index.php/ic-legal-reference-book/the-principles-of-intelligence-transparency-for-the-ic.

Privacy International. 2018. "Secret Global Surveillance Networks: Intelligence Sharing Between Governments and the Need for Safeguards," http://privacyinternational.org/feature/1742/new-privacy-international-report-reveals-dangerous-lack-oversight-secret-global.

Smith, Graham. 2018. "Illuminating the Investigatory Powers Act." *Cyberleagle*, February 22, 2018, www.cyberleagle.com/2018/02/illuminating-investigatory-powers-act.html.

UK Home Office. 2017. "Interception of Communications. Pursuant to Schedule 7 to the Investigatory Powers Act 2016. Draft Code of Practice." December 2017, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/593748/IP_Act_-_Draft_Interception_code_of_practice_Feb2017_FINAL_WEB.pdf.

Vieth, Kilian, and Thorsten Wetzling. 2019. "Data-Driven Intelligence Oversight: Recommendations for a System Update." November 2019, https://guardint.org/2019/11/28/data-driven-intelligence-oversight-recommendations-for-a-system-update/.

Wetzling, Thorsten, and Kilian Vieth. 2018. "Upping the Ante on Bulk Surveillance: An International Compendium of Good Legal Safeguards and Oversight Innovations." Heinrich Böll Stiftung, www.stiftung-nv.de/en/publication/upping-ante-bulk-surveillance-international-compendium-good-legal-safeguards-and.

Wetzling, Thorsten, Kilian Vieth, and Charlotte Dietrich. 2020. "Intelligence in Democracies: International Repository of Legal Safeguards and Oversight Innovation," www.intelligence-oversight.org.

Chapter 9

Transparency and surveillance of end users on social media platforms

A view of structural economic factors

Abel Reiberg

Introduction

Over the past two decades users of social media platforms have been subject to intensive surveillance by various actors. Surveillance has been used by, for example, end users in cases of digital stalking, private companies providing third-party apps in cases like the Cambridge Analytica scandal, and government agencies, as in the case of the National Security Agency's surveillance programs. These actors, however, were able to engage in surveillance only because platform providers have designed platforms to accumulate vast amounts of personal data. In this sense, it is the providers of the platform who enable surveillance. It is first and foremost they who initiate, oversee, and steer the flows of information on the platform. In order to explain the interaction of transparency and surveillance on social media platforms, therefore, the interests of platform providers need to be studied. This chapter addresses the question of why platform providers have furthered transparency and surveillance of end users by investigating the providers' economic interests.

The structure of this chapter is as follows: the second section of this chapter discusses the relationship between transparency and surveillance. It is argued that transparency allows actors to carry out the monitoring that is an essential part of surveillance and that transparency can therefore be understood as a precondition to surveillance. The third section then addresses the question of why providers of social media platforms have both the ability and the interest in furthering transparency and surveillance of end users on their platforms. Here it is argued that the ability to further the transparency of end users relies on the centralization in markets for social media and that this centralization, in turn, is due to economies of scale, particularly those on the demand side. Furthermore, it is argued that the underlying interest in furthering transparency and surveillance relies on the particular multisided market strategies of the platform providers. In order to illustrate the argument, the strategies applied by Facebook, the provider of the largest social media platform, with regard to end users, developers, and advertising clients are considered.

DOI: 10.4324/9781003120827-12

A summary of this chapter's results and limitations is provided in the concluding section.

On the relationship between transparency and surveillance

References to transparency in political discourse usually have a positive connotation; there are, however, telling exceptions. On December 14, 1996, the German newspaper *Süddeutsche Zeitung*[1] published a commentary titled "the transparent citizen." With surprising foresight, the data protection officer of the state of Bavaria criticized policies providing the German foreign intelligence agency with competences which, as the leaks of Edward Snowden would later reveal, were then used for the illegal surveillance of German citizens. In the commentary, as in similar contributions to the discourse on security surveillance, the metaphor of the "transparent citizen" stands for the transparency of a citizen's personal traits, preferences, or behavior to the "eye" of a surveilling other—in this case the intelligence agencies.

The metaphor illustrates a specific perspective on the relationship between transparency and surveillance: one in which transparency, understood as the absence of an obstacle in the process of observation, is a precondition for surveillance, as it allows actors "to oversee"—from the French *sur* [over] + *veiller* [watch]—others. Surveillance, in turn, entails observation or the gathering of information, not as passive monitoring but for the purpose of "discipline" (Foucault 1995), "behavioral modification" (Zuboff 2015), or "influence, management [or] protection" (Lyon 2007); that is, forms of social control. Thus transparency empowers surveillance and therefore might not be seen as a solely positive but as an ambivalent condition—depending on who it is that is empowered in relation to whom.

The commonplace positive connotation of transparency seems to rely on the equally common assumption that an increase in transparency usually benefits the weaker actors in asymmetric power relations, for example, the citizens in their relations to elected officials. However, it may more often be the case that it is the stronger actors who are able to define the terms of transparency and who can use the possibilities transparency offers.

In order to determine whether an increase in transparency in a specific situation is desirable or not, it is (among other things) important to clarify which actors the increase in transparency might enable to carry out surveillance and which actors might be subjected to that surveillance—although this analytical task has generally not become easier in the past decades. With the rise of new information and communication technologies, the practice of surveillance has disseminated throughout society. An increasing number of actors are involved in acts of surveillance, often simultaneously playing both the role of the surveillant and the role of the surveilled. This is particularly the case in the context of social media. The transparency available in the setting

of social media platforms is utilized by actors such as the end users, third-party developers, advertising clients, government agencies, and the platform providers themselves. Furthermore, these actors often switch between roles in acts of surveillance. End users may, for example surveil other end users while at the same time being themselves surveilled by platform providers.

These diverse actors, however, vary in their degree of agency. As Trottier puts it, "On first pass it seems that all social media users have the potential to watch over each other. But those who manage [the platform] have a privileged view of its contents" (Trottier 2011). Because providers are developing and deploying the software at the heart of platforms and are defining their terms of use, they have more control over the platforms than any other group of actors. It is the providers that first and foremost decide who will be transparent for whom. Therefore, it is the providers and their interaction with other relevant actors that is the focus of this article. The question addressed in the following is why and how providers are furthering transparency and surveillance of the largest and most exposed group of actors, the platform's end users.

As authors like Fuchs (2012, 2014) and Zuboff (2015, 2019) have shown, answers to this question can be found by analyzing the economic function of surveillance in platform economies. From a Marxist perspective, they have argued that surveillance has become the key component of a new mode of production that constitutes a new variant of the capitalist economic order, which Zuboff (2015, 2019) calls "surveillance capitalism." This chapter follows Fuchs and Zuboff insofar as it highlights the economic function of surveillance on platforms. However, it does so not from a Marxist macroeconomic perspective but by relying on concepts of microeconomic literature on platform economics, which help to further the understanding of why and how specific firms (namely, the most successful firms) in specific markets (namely, markets for social media) are deciding to make surveillance an integral part of their business. Particularly useful are the concepts of "network effects" and "multi-sided markets," which have been advanced in the last two decades by works of authors such as Rochet and Tirole (2003), Weyl (2010), and others. In the next section, the concept of network effects will be touched upon in order to explain why concentration in markets for social media occurs and how this affects user privacy. The section thereafter will explain how the multisided market strategy of a social media platform provider may create interest in surveillance. The discussion will be illustrated with examples from Facebook, Inc., which, based on the number of end users, is the provider of the largest social media platform.

Economic underpinnings of surveillance and transparency on social media platforms

Today, providers of social media platforms belong to the most successful companies in the world. Facebook, Inc., for example, ranks fifth among the most

valuable corporations (Wikipedia 2020; Handelsblatt 2018). An important reason for the high market capitalization of the platform providers (676 billion US dollars in the case of Facebook) is the degree of concentration in the respective markets. Most of the platforms dominate specific markets, which becomes visible when looking at the number of end users of these platforms, which in some cases is not only high in relative but also in absolute numbers. The platforms run by Facebook are a good example, among which are the platforms Facebook, Instagram and WhatsApp with 2.76 billion daily active users in total (Facebook 2021). For comparison, in the relatively competitive sector of instant messaging the closest competitor to Facebook, Inc.—Snap—has around 293 million daily active users on its platform Snapchat (Snap 2021). As interactions are increasingly concentrated on individual platforms, it is not surprising that the monetization of these interactions has led to a strong concentration of capital at the platform providers. However, the market concentration has not only economic or financial consequences but also consequences for the privacy of the platforms' end users.

Concentration in markets for social media and its implications for mass surveillance

As authors like Helen Nissenbaum (2004) have argued, privacy is highly context-specific as people usually do not object to sharing information per se, but to sharing specific information depending on the social context. They may, for example, want to share personal health information with their physician but oppose sharing the very same information with their neighbors. Thus, in order to safeguard privacy, it is necessary to ensure that information shared is appropriate to and contained within the social context it was meant to be shared. Hypothetically, a decentralized ecosystem of platforms, in which a multitude of platforms exists, would be able to cater to different social contexts—such as specific platforms for communication with family members and other platforms for communication with friends or colleagues, and so on. In a fully centralized ecosystem, in contrast, interactions relating to various social contexts take place on a single individual platform, which has several consequences for user privacy.

One of the consequences of centralization is that end users can be monitored in a wider range of contexts. This is not only a difference in quantity. As has been acknowledged, for example, in court rulings regarding violations of privacy,[2] the combining of apparently insignificant bits of information can enable the creation of significant data profiles of the persons in question.

A telling example is Facebook's patent on methods that allow the company to use the "staggering" amount of information shared by users—"by sharing photos, real-time status updates, and playing social games" including "information describing recent moves to a new city, graduations, births, engagements, marriages, and the like" (Sullivan et al. 2018)—in order to

create a profile that provides inferential information regarding other key aspects, such as household income. In short, it is possible to create much more detailed "data doubles" (Ericson and Haggerty 2000) of end users in a centralized ecosystem than in a decentralized one.

Furthermore, the data obtained from users can be distributed more widely in a centralized ecosystem. Users are therefore much more likely to experience what Trottier (2011) with reference to Facebook described as the "leaking" of information from one context to another. They may, for example, share certain information assuming that this information is relevant for their friends, while not realizing that the same information will be disseminated among their family members or colleagues who are present on the same platform. With the very design of the platform, providers like Facebook, Inc. are facilitating the leakage of information, as will be argued below with reference to the examples of the Facebook Beacon and Facebook Timeline.

Finally, in a centralized ecosystem the end users have fewer options to react to unwanted behavior of the platform provider. While they might still be able to voice concerns, their options to exit the relationship to the platform are reduced. Therefore, it is less likely that end users will have leverage to keep the platform provider from introducing problematic practices such as surveillance practices. As authors like Srinivasan (2019) have argued, users on Facebook are unable to react to breaches of their privacy due to Facebook's monopoly status.

To summarize, factors that are conducive for centralization in markets for social media are also conducive for transparency and surveillance of end users on social media platforms. Therefore, it is important to understand the working of such factors. While many different factors may be furthering the concentration of markets, one set of factors that is of particular relevance (and specifically in markets for social media) is economies of scale. Economies of scale may exist both on the supply and the demand side.

On the supply side, economies of scale exist when the average costs of production decrease as outputs increase. Typical examples can often be found in markets for infrastructure. In the case of railways, for example, offering a customer the service in question (transportation by train) incurs almost the same cost in the case of one customer as compared to the case of a thousand customers. There are high fixed costs for the construction of the railway system and relatively low variable costs, such as personnel costs, for its operation. In other words, once the infrastructure is in place, the costs per customer fall rapidly so that a large provider can operate more cost-efficiently than a small provider.

The same logic applies to a different degree to social media. Offering the communication services of a social media platform to a single customer is almost as expensive as offering the same service to a thousand customers. In both cases, the key component of the platform, its software, has to be developed and deployed. Thus, the same high fixed costs apply to both large

and small numbers of users. These include costs of research and development, which in the case of Facebook, Inc. amounted to over 10 billion dollars in 2018. Additionally, there are relatively low variable costs to bear, such as costs for the operation of the hardware of the platform.[3]

As a result, providers that can rely on a large customer base have a cost advantage and can offer their services at lower prices than providers with a small customer base. Therefore, once a provider has established a large customer base, it is unlikely that a newly entering provider with an initially small customer base can compete. The respective market therefore tends to a monopoly.

While economies of scale on the supply side promote centralization in the context of social media, centralization is further strengthened by economies of scale on the demand side. Varian, Farrell, and Shapiro (2004, 33) use the term "demand side economies of scale" interchangeably with the more widespread term "network effects." The terms refer to a situation in which the marginal utility of a product increases with the number of its users. In such a situation, the service in question provides only minimal utility for an individual user, but a larger group of users increases the utility for each user. Good examples are again the classic and the new markets for infrastructure. Writing about the infrastructure for telephony, for example, Theodore Vail, the President of AT&T, noted in the company's 1908 annual report to shareholders:

> A telephone—without a connection at the other end of the line—is not even a toy or a scientific instrument. It is one of the most useless things in the world. Its value depends on the connection with the other telephone—and increases with the number of connections.
>
> (AT&T 1908)

This is also the case with social media platforms. If the platform were used by only one individual, it would be absolutely useless. If, however, the number of users increases, the utility of the platform for each user also increases.

Fortunately, today's telephone customers can contact any other telephone customer regardless of which specific telecommunications provider they use. This is not the case for social media users. A Facebook customer, for instance, is not able to contact a customer on another platform, such as Diaspora. In this situation, customers have strong incentives to select the provider catering to the larger number of end users. Therefore, once a provider has established a large user base it is likely to dominate the market.

This may even lead to a lock-in situation (Varian, Farrell, and Shapiro 2004, 21). In such a case, even if a majority of users would prefer to switch providers, they are unable to do so collectively and therefore remain. In this case, users are de facto missing one of the fundamental options for reacting to a decrease in service quality, namely the option to exit the relationship with the provider and to select an alternative provider. As Srinivasan (2019) argues,

Facebook is one example of such a lock-in. Srinivasan considers Facebook's extensive use of user data as a decrease in the quality of Facebook's service, yet end users are unable to react against it by exiting, due to Facebook's monopoly position.

To summarize, economies of scale contribute to the competitive advantages of large platforms and therefore allow providers like Facebook, Inc. to acquire a dominant position in the market for social media. This results in a situation in which the communicative processes of large parts of society are concentrated on individual platforms. In this situation a single platform provider has the ability to oversee a large variety of interactions of users and to expose users to a large variety of settings. Furthermore, it limits the users' ability to react to that oversight and exposure. While therefore the tendency for concentration in markets of social media explains why platform providers acquire a position that is particularly suited for surveillance of end users, it does not explain why the providers are actually interested in using this position. In order to understand the providers' interests, it is necessary to consider their best options for beneficial economic exchanges with their counterparts. Here it is necessary to consider that, in contrast to more traditional companies, platform providers do not have only one key market in which they are active but rather face so-called multisided markets.

A multisided market strategy and its implications for mass surveillance

By definition platform providers[3] mediate between different groups of market participants (Evans and Schmalensee 2016). The main function of a platform is to enable interaction among these groups. In order to understand not only how a provider of a specific platform is generating revenue but also whether and how the provider relies on transparency and surveillance to do so, it is necessary to look at how the different groups of actors are being integrated and how externalities among them are managed.

Which groups of actors are integrated into a platform and in what way depends mainly on the strategy chosen by the individual platform provider. According to the definition of social media, end users always take part in the interactions on a platform. However, depending on the particular strategy applied by the provider in question and the resulting design of the platform, additional groups often also take part. In the case of Facebook, for example, there are arguably three main groups of actors, which are the end users, third-party developers, and advertising clients. The following will describe the strategies that Facebook applies toward the three main groups of actors on its platform, in order to elaborate the nature of its business model, which seems to have become the dominant model for providers of platforms not only but particularly in social media.

Strategy toward end users

It is a constitutive aspect of social media that end users are able not only to consume but also to produce content. Therefore, end users take two different roles on social media platforms: on the one hand, they create a supply of data, and on the other hand, they also create a demand for that data. Platform providers like Facebook, Inc. enable supply and demand to meet. In this constellation the providers (and also the end users) benefit from such network effects. Among the end users, these network effects are bilateral.[4] The more supply-generating end users the platform has, the more relevant it is for demand-generating end users; and the more demand-generating end users a platform has, the more supply-generating end users it will attract. As argued above, these network effects enable rapid growth of platforms.

For this reason, platform providers try to strengthen the network effects with both their pricing as well as the design of their platform. With their pricing, providers often lower the barriers to entry of end users by setting prices extremely low—often at zero. In this way the providers try to ensure that they succeed in the competition for end users, which—due to the network effects—has a winner-takes-all characteristic. On the other hand, this means that no revenue is provided from the end users directly and that the revenue necessary to sustain the platform has to be derived from other groups of actors. As will be discussed below, in the case of Facebook, these are mainly the advertising clients.

Regarding the platform design, the platform providers have to ensure that it serves the function of matching demand and supply for data as effectively as possible, since only then can network effects reach their maximum intensity. In the case of social media, this may already have implications for the transparency of end users, as it encourages users to seek information about others, even if this imposes costs on those users who experience a breach of their privacy. Indeed, it seems that some platform providers, in their goal to maximize interaction among end users on the platform, have come to the conclusion that a "forced matching"—a matching that lies beyond the supply/demand of information that would occur if end users had full control—may result in more interaction. Such a forced matching implies either extracting more data from existing end users (in their role as suppliers) than intended by them, or forcing more data on end users (in their role as customers) than actively demanded by them, or both.

Looking at the case of Facebook, Inc. there are several major design decisions that seem to be a result of both strategies. Arguably the most striking examples are the introduction of Facebook's News Feed and Facebook Beacon. Facebook's Newsfeed was introduced in 2006. According to Wikipedia, News Feed is "the primary system through which users are exposed to content posted on the network" (Wikipedia 2019). With the introduction of News Feed, Facebook began to extract the personal information

of end users from the specific context it was placed in (their profile page) and placed in a much wider context (the News Feed) of—at least potentially—the landing page shown to each of the contacts of the end user. Unsurprisingly, at least when considering Nissenbaum's contextual understanding of privacy mentioned above, many users saw the introduction of the News Feed as a violation of their privacy (Zuckerberg 2006a; Bunz 2006). These users were comfortable with sharing information on their profile page; however, they were uncomfortable with the broadcasting of this information over the landing pages of their contacts. Only after massive protests by users did Facebook introduce options for users to better control the flow of their personal information to the News Feed (Zuckerberg 2006b). However, it did not make the News Feed an optional feature.

Facebook Beacon, introduced in 2007, allowed participating third parties to send information about Facebook users' activities on their websites to Facebook. Online shops, for example, were sending data about the purchases of users to the platform. This data was then placed on the News Feed. In the case of Beacon, users were given little option to control the flow of personal information. The option to opt-out of the service was made available only after user protests, and it prevented only the publishing of the data, not its collection (Zuckerberg 2007). Several protests and a class-action lawsuit were initiated as a response by users. In the course of the lawsuit Beacon was finally terminated (Perez 2009).

As these two examples show, the platform providers' aim of maximizing interaction among users in the case of Facebook already implies a furthering of transparency and surveillance of users. In order to gain a more complete understanding of the providers' interests it is necessary to also consider the providers' strategy toward the other groups of actors integrated into the platform, among them the developers of third-party apps and the advertising clients.

Strategy toward developers

The developers can be considered as another side in the multisided market that providers like Facebook cater to. In the case of Facebook, developers turn to the platform in order to find consumers for their games and applications. For users, in turn, the games and applications are products to consume. Facebook enables the exchange between the two groups and, by doing so, again benefits from bilateral network effects. The more demand by end users, the more attractive the platform is for developers; conversely, the more applications offered by developers, the more attractive the platform is for users. In this case, too, the company is interested in strengthening the network effects and acts accordingly.

How this goal is followed with a particular strategy for the pricing and design of the platform can be studied particularly well in the case

of Facebook, since during the Cambridge Analytica scandal that shook the company a large number of documents were published showing how the company developed, exercised, and refined its strategy toward third-party developers. Revealing in this context is the correspondence between Facebook's founder and CEO Mark Zuckerberg and other executives of the company, in which the basic principles for the interaction with developers were discussed on the occasion of a new release of Facebook's API (named "Platform"). As becomes clear in this correspondence, it was decided to keep the price for the developers' engagement as low as possible in order to guarantee their presence on the platform. At the same time, ensuring access to data collected by the developers was defined as an overarching principle. This principle has been described with the term "data reciprocity." Mark Zuckerberg explains:

> After thinking about platform business model for a long time, I wanted to send out a note explaining where I'm leaning on this. […] The quick summary is that I think we should go with full reciprocity and access to app friends for no charge. Full reciprocity means that apps are required to give any user who connects to FS a prominent option to share all of their social content within that service […] back to Facebook.
>
> (Zuckerberg 2012)

He explains further:

> [T]he very first question I developed an opinion on was what we should be optimizing for. There's a clear tension between platform ubiquity and charging, so it's important to first fully explore what we're trying to get out of platform. The answer I came to is that we're trying to enable people to share everything they want, and to do it on Facebook. Sometimes the best way to enable people to share something is to have a developer build a special purpose app or network for that type of content and to make that app social by having Facebook plug into it. However, that may be good for the world but it's not good for us unless people also share back to Facebook and that content increases the value of our network. So ultimately, I think the purpose of platform—even the read side—is to increase sharing back into Facebook.
>
> (Zuckerberg 2012)

What becomes clear here is that from the perspective of the provider Facebook, Inc., interaction with developers has a primarily instrumental purpose. The developers are intended to contribute to the transparency and surveillance of end users. In order to ensure this, the provider minimizes barriers to the participation of the developers while obligating them to assist via their apps in the collection of data on the platform.

How significant the collection of data from third-party developers is becomes particularly clear when considering the case of Cambridge Analytica. In this case, an app (named "thisisyourdigitallife"), developed by a third party, namely Global Science Research, was used to gather the personal information of around 50 million Facebook users. The data was then acquired by the company Cambridge Analytica in order to use it for manipulating end users during several US elections, including the presidential election of 2016. The case was widely perceived as the greatest surveillance scandal in the history of Facebook.

Strategy toward advertising clients

A third set of relevant actors that needs to be considered in order to understand the platform providers' interest in transparency and surveillance, in this case consists of those individuals and organizations that use the platform for the purpose of advertising. The advertising clients can be understood as resembling another demand side in the multisided market that Facebook decided to cater to. On the opposite side are the end users whose attention is supplied to the advertising clients. The network effects here, however, are unilateral. An increase in the number of users leads to an increase in the value of the platform for advertisers. Conversely, an increase in the number of advertisers does not (or at least only in a very small fraction of cases) lead to an increase in the value of the platform for users. In such a situation, the option preferred by the platform provider is usually not (as in the case of the end users or the developers) to lower the barriers of entry to the platform as far as possible. In contrast, the preferred option is to restrict and price this access. Facebook's annual reports state that in the year 2020, more than 98% of the revenue of Facebook was derived neither from end users nor developers but from advertising clients (Facebook 2020). As this number shows, Facebook is following a subsidizing strategy according to which profits are generated on the part of advertising clients to finance the participation on the part of end users and developers. This strategy allows Facebook to strengthen desired network effects regarding end users and developers while at the same time ensuring revenue from the advertising clients, thus ensuring successful competition and ultimately profit maximization.

However, this strategy also comes with obligations regarding the platform's design. The platform must be designed in such a way that it provides a particularly useful service for the only customers directly financing the platform—the advertisers. At this point, it is important to emphasize that the service that advertisers are purchasing is the modification of the end users' behavior, which rests on the surveillance of these end users and their contacts (Zuboff 2019, 68). Most of the demand for this service derives from companies that want to ensure that end users purchase certain products or services that they would not purchase otherwise. The spectrum of decisions affected in these

cases is far ranging, from a decision about the brand of one's next winter coat, for example, to a decision regarding a future place of residence or the choice of one's next employer. However, the spectrum of affected suser decisions ranges even further since it is not only actors with economic interests that are demanding the service. Religious groups, political movements, political parties, NGOs, and government authorities may also have an interest in influencing a platform's end users. Decisions that can be affected thus also include, for example, the users' religious and political orientation. The advertising systems of Facebook are open to a wide range of clients and mainly leave it to the clients to decide the content used for the advertising.

In any case the effectiveness of the advertising is furthered by relying on the gathering of large amounts of data. First, the data is used to allow clients to select those end users whose behavior they deem particularly easy or particularly useful to manipulate. For a client advertising for yoga courses it may be important to address users who are interested in yoga. For a political party it may be particularly relevant to address users who are "swing voters," or who live in "swing states." Second, the information on end users allows the clients to address the users in particularly effective ways. A user may, for example, be informed that a contact is interested in a yoga course or particular political content. Thus, the users' trust in their contacts and their contacts' decisions is utilized for the advertising. Importantly, the information gathered on end users allows clients to evaluate whether a particular marketing campaign was successful or not. The client may learn which advertising was most successful by considering the percentage of users that reacted to their content by following external links, for example. Thus, the advertising clients may learn and find the optimal approach for running an advertising campaign. As this shows, the effectiveness of advertisement rests to a high degree on the surveillance of end users. Only if the provider, in this case Facebook, has extensive information about the end users can it target those end users whose manipulation is profitable. Only extensive information about these end users allows effective modification of their behavior, and only continuous monitoring allows the advertising clients to learn from their attempts.

To summarize, Facebook's goals of maximizing the participation of end users, third-party developers, and advertising clients leads it to promote the transparency of its end users. What bears mentioning is that this transparency of end users stands in stark contrast to the level of transparency of the platform provider itself. One telling example also in this context is again Facebook's internal communication (Facebook 2013). Among this communication is an email from February 2015 in which Michael LeBeau, then a product manager at Facebook, informed his colleagues about plans to use the Facebook app for gathering data on users' call history—another important step toward increased end user transparency and surveillance. In order to enable the gathering of data, the permissions for the app needed to be changed, which was expected to trigger the Android operating system to start a dialog

with the users and to inform them about new far-reaching authorizations. Knowing that users would likely object to this step toward more transparency and surveillance of themselves, and knowing that the change would therefore be "a pretty high-risk thing to do from a PR perspective" (LeBeau 2015), Facebook's managers searched for a solution. What they finally proposed was a procedure that "would allow [them] to upgrade users without subjecting them to an Android permissions dialog at all" (Kwon 2015). Thus, as the internal communication shows, the goal of the platform provider here was not to find alternatives to the newly introduced surveillance practice but to simply leave users unaware of it.

As the example shows, the relation between end users and the platform provider Facebook can be described as highly asymmetrical. Facebook has acquired a favorable position in a highly centralized market, and it uses this position to further surveillance and behavioral modification while it also uses the position to shield itself from critical views.

Conclusion: (asymmetric) transparency and surveillance on social media platforms

In academic as well as in public discourse, transparency is usually described as a positive feature. In the context of surveillance, however, it proves to be of ambivalent character. As has been argued in this chapter, transparency can be considered a precondition of surveillance. Surveillance, in turn, is a problematic practice insofar as it implies power imbalances. Such imbalances become visible in single incidents of surveillance in which a surveillant is always able to exercise control over a surveilled other. Furthermore, imbalances are visible also at the macro level, as the means of surveillance are not evenly distributed in society but rather concentrated with specific actors. As authors like Trottier (2011, 2012), Fuchs (2012, 2014), and Zuboff (2015, 2019) have pointed out, in the last decades the means for surveillance have become accumulated particularly by specific economic actors, among which social media platforms play a central role.

In order to understand the reasons for the providers' engagement in surveillance, it is necessary to identify the economic factors affecting these corporate actors' interests. Among these, two specific factors are particularly important. Firstly, economies of scale cause the markets for social media to take a centralized form and promote a situation in which individual providers have the possibility to surveil a large number of end users. Secondly, the fact that the providers utilize this possibility is due to the nature of the multisided markets in which the providers operate. Many providers offer communication services for end users, while their revenue is generated by customers paying for influence over these end users. In order to explain the intensified surveillance taking place on social media platforms, it is important to understand the working of these factors. This chapter described some of the key

factors relevant to explaining transparency and surveillance on social media platforms like Facebook.

In order to gain a more complete picture of the political economy of social media surveillance it is imperative for future research to consider additional aspects of the platform economy. These should include additional factors conducive to platform surveillance, such as mergers and acquisitions among platform providers, which further the centralization of markets and possibilities for platform surveillance. Such research should also include, however, factors that work against platform surveillance (which were not the focus of this chapter), such as the practice of multihoming, which reduces centralization of markets and possibilities for platform surveillance.

Notes

1 The nontabloid newspaper with the largest circulation in Germany.
2 See, for example, the ruling of the German Supreme Court of December 15, 1983, in which it acknowledged the so-called "right to informational self-determination" as one of the constitutional rights.
3 This chapter differentiates between the platform provider (an organization, usually a corporation as in the case of Facebook, Inc.) and the platform—a technical artifact.
4 In this chapter, the end users are divided conceptually into two groups, and the network effects are therefore categorized as indirect (between groups of actors) and bilateral. If, in contrast, the end users were considered as one homogenous group, the network effects would have to be categorized as direct (among one group of actors).

References

AT&T. 1908. "Annual Report of the Directors of American Telephone and Telegraph Company to the Stockholders of the Year Ending December 31, 1908," https://beatriceco.com/bti/porticus/bell/pdf/1908ATTar_Complete.pdf.

Bunz, Mercedes. 2006. "Facebook Users Protest over News Feed." *The Guardian*, www.theguardian.com/media/pda/2009/oct/27/new-facebook-newsfeed-protest.

Ericson, Richard V., and Kevin D. Haggerty. 2000. "The Surveillant Assemblage." *British Journal of Sociology* 51(4): 605–22.

Evans, David S., and Richard Schmalensee. 2016. *Matchmakers: The New Economics of Multisided Platforms*. Boston: Harvard Business Review Press.

Facebook. 2013. "Industry Update," www.parliament.uk/documents/commons-committees/culture-media-and-sport/Note-by-Chair-and-selected-documents-ordered-from-Six4Three.pdf.

Facebook. 2021. "Facebook Reports First Quarter 2021 Results" https://investor.fb.com/investor-news/press-release-details/2021/Facebook-Reports-First-Quarter-2021-Results.

Foucault, Michel. 1995. *Discipline and Punish: The Birth of the Prison*, 2nd Edition. New York: Vintage.

Fuchs, Christian. 2012. "Google Capitalism." *TripleC: Communication, Capitalism & Critique. Open Access Journal for a Global Sustainable Information Society* 10(1): 42–8.

Fuchs, Christian. 2014. *Social Media: A Critical Introduction*. Los Angeles: Sage.

Handelsblatt. 2018. "Apple, Google, Amazon: Das sind die Zehn Wertvollsten Unternehmen der Welt." *Handelsblatt*, www.handelsblatt.com/finanzen/anlagestrategie/trends/apple-google-amazon-das-sind-die-zehn-wertvollsten-unternehmen-der-welt/22856326.html.

Kwon, Yul. 2015. "Note by Damian Collins MP, Chair of the DCMS Committee." E-mail Message, February 4, 2015, www.parliament.uk/documents/commons-committees/culture-media-and-sport/Note-by-Chair-and-selected-documents-ordered-from-Six4Three.pdf.

LeBeau, Michael. 2015. "Message Summary [id.663395043771422]." E-mail Message, February 4, 2015, www.parliament.uk/documents/commons-committees/culture-media-and-sport/Note-by-Chair-and-selected-documents-ordered-from-Six4Three.pdf.

Lyon, David. 2007. *Surveillance Studies: An Overview*. Cambridge; Malden: Polity Press.

Nissenbaum, Helen. 2004. "Privacy as Contextual Integrity." *Washington Law Review* 79(1): 119–57.

Perez, Juan Carlos. 2009. "Facebook Will Shut Down Beacon to Settle Lawsuit." *The New York Times*, https://archive.nytimes.com/www.nytimes.com/external/idg/2009/09/19/19idg-facebook-will-shut-down-beacon-to-settle-lawsuit-53916.html.

Rochet, Jean-Charles, and Jean Tirole. 2003. "Platform Competition in Two-Sided Markets." *Journal of the European Economic Association* 1(4): 990–1029.

Snap 2021. "Snap Inc. Announces First Quarter 2021 Financial Results" https://investor.snap.com/news/news-details/2021/Snap-Inc.-Announces-First-Quarter-2021-Financial-Results.

Srinivasan, Dina. 2019. "The Antitrust Case Against Facebook: A Monopolist's Journey Towards Pervasive Surveillance in Spite of Consumers' Preference for Privacy." *Berkeley Business Law Journal* 16(1): 39.

Sullivan, Brendan M., Gopikrishna Karthikeyan, Zuli Liu, Wouter Lode Paul Massa, and Mahima Gupta. 2018. "Socioeconomic Group Classification Based on User Features." United States US20180032883A1, filed July 27, 2016, and issued February 1, 2018, https://patents.google.com/patent/US20180032883A1/en.

Trottier, Daniel. 2011. "A Research Agenda for Social Media Surveillance." *Fast Capitalism* 8(1): 59–68.

Trottier, Daniel. 2012. *Social Media as Surveillance: Rethinking Visibility in a Converging World*. Farnham and Burlington: Ashgate.

Varian, Hal R., Joseph Farrell, and Carl Shapiro. 2004. *The Economics of Information Technology: An Introduction*. Cambridge: Cambridge University Press.

Weyl, E. Glen. 2010. "A Price Theory of Multi-Sided Platforms." *American Economic Review* 100(4): 1642–72.

Wikipedia. 2019. "News Feed," https://en.wikipedia.org/w/index.php?title=News_Feed&oldid=925280364.

Wikipedia. 2020. "List of Public Corporations by Market Capitalization," https://en.wikipedia.org/wiki/List_of_public_corporations_by_market_capitalization#2020.

Zuboff, Shoshana. 2015. "Big Other: Surveillance Capitalism and the Prospects of an Information Civilization." *Journal of Information Technology* 30(1): 75–89.

Zuboff, Shoshana. 2019. *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. New York: PublicAffairs.

Zuckerberg, Mark. 2006a. "Calm Down. Breathe. We Hear You." The Zuckerberg Files, https://epublications.marquette.edu/zuckerberg_files_transcripts/114.

Zuckerberg, Mark. 2006b. "An Open Letter from Mark Zuckerberg." The Zuckerberg Files, https://epublications.marquette.edu/zuckerberg_files_transcripts/12.

Zuckerberg, Mark. 2007. "Thoughts on Beacon." The Zuckerberg Files, https://epublications.marquette.edu/zuckerberg_files_transcripts/14.

Zuckerberg, Mark. 2012. "Platform Model Thoughts." E-mail message, November 19, 2012, www.parliament.uk/documents/commons-committees/culture-media-and-sport/Note-by-Chair-and-selected-documents-ordered-from-Six4Three.pdf.

Part III

Sources of trust and virtues of mistrust in an age of surveillance

Chapter 10

Trust and surveillance

An odd couple or a perfect pair?

Fredrika Björklund

Introduction

Fifteen years ago, David Lyon predicted that the introduction of pervasive surveillance would destroy trust between individuals and trust between citizens and governments (Lyon 2003). Indeed, at first glimpse trust and surveillance appear to be an odd couple. The surveillance relationship between government (public institutions) and citizens is asymmetrical and built on a basis of distrust. In general terms, a society completely based on trust should have no need for surveillance, while a society based on distrust should more readily perform and justify logics of surveillance such as control, monitoring, and verification.

However, recent empirical studies based on social surveys tell a different story and register a positive correspondence between trust in public institutions and acceptance of surveillance (Friedewald et al. 2015; Pavone, Degli-Esposti, and Santiago 2015). In these studies, high levels of trust predict positive attitudes to surveillance. Thus, trustful citizens allow state authorities to monitor them; or, formulated in a more pejorative way, citizens give legitimacy to (trust) governments, which in turn distrust their citizens. How can we make sense of this counterintuitive finding? This chapter asks how these results from social surveys should be theorized and understood in relation to more dystopic forecasts about the effects of surveillance on trust.

Without doubt, "[t]rust is a primary constituent of the relational dynamic of most surveillance systems" (Ellis, Harper, and Tucker 2013, 1). Still, interest in the relationship between trust and surveillance has been low as compared to the interest in how surveillance impinges on other social goods. Normally, the fundamental opposition in the surveillance context is situated as the individual right to *privacy* versus surveillance (Goold 2009, 207). Although scholarship has recognized that privacy also has public value and can be considered a constitutive public good that is a basic ingredient of a democratic system (Bennett 2011, 486; Raab 2012), public framing of privacy as the main problem with intrusive surveillance policies continues to stress threats to the individual and, in so doing, directs the public discourse

DOI: 10.4324/9781003120827-14

into an individualization of the risks associated with surveillance. Obviously, individual security and privacy must be protected, and surveillance must be performed in ways that are consistent with citizens' personal integrity. But this is too narrow a perspective on the problems with surveillance. I argue that we need to focus more on the impact of surveillance on *societal* values and *societal* well-being, and thinking about trust is a productive way to do this. Trust is recognized as a collective asset essential for "the most basic cooperation in our economic, political, and social relationships" (Freitag and Bühlmann 2009, 1538). Trust enables and makes meaningful citizen contribution and participation in social and political activities. But, if trust flourishes also in the presence of surveillance, as suggested by social survey research, what is the problem? Notwithstanding the importance of the issue, the findings from social surveys concerning trust and surveillance are not sufficiently theorized. We don't know how this seemingly contradictory positive correlation between trust and acceptance of surveillance comes about.

This article aims at mapping some issues that must be carefully probed in order to theorize convincingly the relationship between trust and surveillance. It suggests a reasonable way to construe the relationships found in empirical research by focusing on our understandings of trust. Three main issues will be addressed: first, what is the nature of the causal connection between trust and surveillance; what is expected to explain what and under which conditions? The fact that there is an association between trust and affirmative attitudes to surveillance does not automatically mean that trust explains surveillance attitudes—although studies based on social surveys often more or less take for granted that trust should be considered the independent variable (Patil et al. 2014; Svenonius and Björklund 2018; Friedewald et al. 2016). But, in theory, surveillance may also produce trust—if, for example, citizens feel safer knowing that an area is monitored this might increase the inclination to trust. The chicken and egg problem of temporality needs to be addressed in a theoretically informed way. Certainly, in this context it is also important to discriminate between different kinds of surveillance—I attend to this issue below.

Second, we need to make sense of the positive association found between trust and acceptance of surveillance. In order to do this, the very origins of trust need to be explored. What does it mean to trust, and how should the emergence of trust be explained? Trust is a highly disputed academic concept, and different conceptualizations of trust must be addressed since this affects the way we construe the trust–surveillance nexus. The crucial issue here is whether we consider trust as an outcome of institutional performance or whether we see it as determined by sociocultural factors.

Third, the chapter ends by problematizing the idea of trust as practiced in contemporary societies. A deeper understanding of modern surveillance practices implies that we need to consider how the meaning of trust might change over time and, especially, to consider what trust might look like in the future.

The relationship between trust and surveillance

Does trust really predict particular attitudes to surveillance, as demonstrated in social surveys, or does extensive surveillance undermine trust, as suggested by David Lyon? There is a plenitude of studies engaged in the ways in which trust predicts issues such as the presence of corruption (Richey 2010; Bjørnskov and Tinggaard Svendsen 2013; Graeff and Tinggaard Svendsen 2013), the size of the welfare state (Rothstein 2010; Bjørnskov and Tinggaard Svendsen 2013), democratic success (Inglehart 1990; Jamal and Nooruddin 2010), as well as the relationship between different kinds of trust (Mishler and Rose 2001; Rothstein and Stolle 2008; Sønderskov and Thisted Dinesen 2016). These studies relate trust—regularly understood to be a good quality—to social conditions and phenomena that we normally consider desirable. Surveillance, in contrast, is hardly regarded as inherently good, at best rather as a necessary evil that serves functional purposes such as the reduction of crime levels. Therefore, we should expect the relationship between trust and surveillance to be more complex. Surveillance ought to have the potential to ruin trust given its often highly intrusive measures.

Still, trust in public institutions and governments is, in several quantitative survey studies, found to be associated with an affirmative attitude toward surveillance. The PRISMS (Friedewald et al. 2015, 2016), the SurPRISE (Pavone, Degli-Esposti, and Santiago 2015), and the PACT (Patil et al. 2014) surveys covering citizens in European states report these findings. The PRISMS project, whose main focus was on privacy and security but also covered trust, uses a number of items to measure attitudes to different kinds of surveillance, from foreign state surveillance to police surveys of football matches. Trust in institutions is measured as a composite variable consisting of five items, among them trust in government. The study concludes that among European citizens "trust in institutions has a strong and significant effect on the acceptability of the described surveillance practices" (Friedewald et al. 2015, 76). The SurPRISE project focuses on trust in security agencies specifically and finds that trust in these institutions affects acceptance of surveillance-oriented security technologies (SOSTs) positively (Pavone, Degli-Esposti, and Santiago 2015, 135). The PACT project, also covering citizens in European states, uses trust in government as one component (besides confidence in the voting system, the role of technology, and attitudes to business) in an index variable labeled as "general trust" and finds that this is associated with positive attitudes to surveillance (Patil et al. 2014). In addition to institutional trust, social trust—that is, trust in other people—also has been shown to have a positive, although weaker, correlation with positive attitudes to surveillance (Friedewald et al. 2015). But, as Friedewald et al. (2015, 93–94) note, social trust is a predictor of institutional trust, and although it has a weak independent effect it is indirectly relevant for attitudes to surveillance. The more

people trust in public institutions (and in each other) the more content they are with surveillance.

The abovementioned studies focus mainly on open surveillance and not on secret surveillance. But there is some evidence that the findings on association between institutional trust and surveillance hold also for the latter. In studying three postcommunist societies, Poland, Estonia, and Serbia, Svenonius and Björklund (2018) find that trust in institutions (measured as trust in the police, the intelligence agency, the courts, the tax agency, and in government) predicts acceptance of secret surveillance. Surveillance in the aftermath of terrorist attacks has aroused similar academic interest. In a survey on support for surveillance and security legislation in Canada and the United States after 9/11, Nakhaie and de Lint find that trust in the government, trust in airport officials, and low tolerance of minorities are key predictors. They argue that these factors, and in particular trust in government, tend to drive people "to cede civil liberties for security and surveillance" (Nakhaie and de Lint 2013, 160). Denemark (2012) notes a difference between countries when it comes to acceptance of counterterrorism surveillance policies. In countries with a legacy of a controlling state (in this case Russia and Taiwan), trust deficits work as a constraint against support for extending police surveillance, while in traditional liberal democracies, trust in government seems to be irrelevant to surveillance attitudes. The evaluation of institutional past performance is a better explanation in these cases. Since recognition of performance is frequently regarded as a condition for institutional trust, Denemark's findings are not immediately comparable with other studies. But his study points to democratic traditions as an underlying factor that might explain how trust interacts with surveillance attitudes. Steinfeld, also engaged in the issue of counterterrorism, finds that political (institutional) trust, among other factors, plays into opinions on surveillance. She argues that, when confronted with terrorism, citizens show "a tendency to just trust authorities and surveillance systems" (Steinfeld 2017, 1671). In addition, Steinfeld distinguishes between private sector surveillance and state surveillance and finds that they are predicted in different ways.

The studies discussed above all have in common that they attend to trust as the explanatory factor accounting for surveillance attitudes. However, Pavone, Degli-Esposti, and Santiago (2015, 142) point out that the opposite may also be true, namely, that the use of more acceptable technologies might increase trust in security agencies. This remark leads us on to studies with a different approach to trust and surveillance, i.e. studies that highlight the (negative) effects of surveillance.

In addition to social surveys, there are several qualitatively oriented case studies, representing various disciplines, that address the relationship between trust and surveillance. Frequently, these studies concern the consequences that surveillance has or may have on trust and other social or individual qualities. One example is Maras (2012), who studied the effects of the EU

Data Retention Directive and forecasted, among other things, a loss in citizens' trust as a consequence of this regulation. In another study, Ali (2016) explores police monitoring of Muslim students and community organizations in New York City following 9/11. He finds that monitoring resulted in decreasing intercommunity trust as well as a decreasing sense of solidarity within the Muslim group (but also self-censoring and a culture of fear). Alam and Husband (2013) draw similar conclusions in a study of British counterterrorism policies toward Muslim communities. The securitization of urban life, including surveillance, that affects these communities not only resulted in a breakdown of trust toward state agencies but also caused declining trust between community members. In a similar vein, Duck (2017) notes that constant surveillance activities toward residents in black neighborhoods may corrode trust between residents and law enforcement agencies. Craven, Monahan, and Regan (2015) highlight the complex relationship between state surveillance and public trust with an empirical study of Department of Homeland Security Fusion Centers (with the objective of enabling different agencies to share resources and information relevant for counterterrorism activities). Sorell (2011) contrasts intrusive surveillance techniques, among them secret bugging, wiretapping, email, and covert camera surveillance of suspects in public places, against the value of building trustful relations with the community for combating terrorist crimes. But we see similar effects also in welfare institutions. Perry-Hazan and Birnhack (2018, 60), for example, investigate the increasingly widespread use of CCTV in schools and draw the conclusion that surveillance changes the nature of school activities by diverting "the educational realm to the semi-legal realm" and by signaling to children that they cannot be trusted. Szrubka (2013) studies the effect of surveillance on the Polish healthcare system, such as cameras in ambulances, and finds that this kind of surveillance has the potential to alter the meaning of trust. Thus, from the abovementioned case studies, we learn that surveillance may produce distrust.

In sum, empirical studies point in different directions and draw conflicting conclusions. Quantitative survey studies tend to see trust as the cause of more positive surveillance attitudes, while the qualitative cases studies referred to above see surveillance as a practice that has a harmful impact on trust. How can we make sense of this contradiction in findings? Rather than reducing the explanation to a problem of methodological differences, I instead suggest that the incompatibility of findings might be best explained by considering the different types of trust addressed.

While survey studies focus on institutional trust and so-called generalized social trust—the *abstract* trust in "all others"—the case studies often concern social trust on a more relational level between people living in a community, and trust as it is enacted in direct contact with a particular institution, such as the police. The latter is commonly called particular social trust—in contrast to generalized social trust. Thus, there is reason to reflect on the

features of different types of trust, as well as on how institutional and social forms of trust relate to each other. Are they totally different constructs, or should they be regarded as interrelated? In order to further discuss this issue, we need to investigate how trust emerges. In the literature, we find two disciplinary orientations, the institutionalist perspective and the socio-cultural perspective, that represent different beliefs on the origins of trust. The relationship between institutional and social trust, I propose, is at the very heart of the academic debate on the relationship between trust and surveillance.

The emergence of trust

Some scholars distinguish between three kinds of trust: trust in institutions (political trust), generalized social trust, and particular social trust (Newton and Zmerli 2011). Institutional trust refers to people's confidence in public institutions of various kinds, including trust in governments and political entities. In social surveys, institutional trust often refers to a composite variable bringing together several survey items regarding trust in specific institutions. The definition of institutional trust may vary from study to study, but trust in government, trust in the police, trust in intelligence agencies, trust in tax agencies, and trust in courts are common items used that, when combined, are regarded as a representation of institutional trust (Svenonius and Björklund 2018).

Social trust, in contrast, refers to trust in fellow human beings, and generalized social trust concerns whether people trust the anonymous other. It is a mental model of the trustworthiness of people you don't know (Rothstein and Eek 2009, 83). Typically, generalized trust is measured by the survey question, "Generally speaking, would you say that most people can be trusted, or that you can't be too careful in dealing with people?" (Nannestad 2008; Björklund 2019). These two kinds of trust—institutional trust and generalized social trust—are often, in difference to particular trust, ascribed the role of important building blocks for a good democratic society (Newton and Zmerli 2011).

Particular social trust refers to trust in close relationships such as within the family, among neighbors, and in social networks or communities. There is a growing academic interest in this kind of trust, although until recently it did not appear in social surveys. Two issues dominate studies on particular trust. First, is it related to the more abstract generalized social trust and, if so, in what ways (Freitag and Traunmüller 2009; Newton and Zmerli 2011; Welzel and Delhey 2015; Cao et al. 2015)? Second, may trust in close relations substitute for generalized social trust and institutional trust in societies where these kinds of trust score low—and thus have political significance in its own right (Gibson 2001; Khodyakov 2007; Ford 2017)? The discussion below ties into both of these matters.

Scholars find that trust in institutions and trust in other people (general social trust) often covary in people's attitudes (Rothstein and Stolle 2008; Sønderskov and Thisted Dinesen 2016). This seems also to be the case concerning trust and attitudes to surveillance (Friedewald et al. 2015; Svenonius and Björklund 2018). Still, the core question is whether institutional trust should be understood as the ultimate origin in the explanatory chain or whether social trust is the building block on which institutional trust rests. As we shall see, this is important for correctly understanding the association between trust and surveillance.

Theories on how trust emerges concern, to a large extent, the association between different kinds of trust. Roughly speaking, the literature provides two approaches with different takes on the relationship between institutional trust, generalized social trust, and particular social trust: the institutionalist perspective (Rothstein 2004, 2005) and the sociocultural orientation, or social capital theory (Sztompka 1999, 2005; Putnam 1993; Inglehart 1990). Simply put, the difference between these two schools of thought may be described as different ways of understanding the order in which the types of trust occur. While institutionalist theorists set trust in institutions as the origin of social trust, sociocultural theorists see social trust (Lühiste 2006, 478; Mishler and Rose 2001), and especially particular social trust, as the root of all other kinds of trust. Institutionalists care less about particular trust.

Institutionalist scholars argue that "social trust comes from above and is destroyed from above" (Rothstein 2005, 199). The root to trust in a society is a well-performing and noncorrupt public administration (Freitag and Bühlmann 2009). Good quality of public institutions is a fundamental condition that allows trust in these institutions as well as general social trust to develop (Rothstein and Stolle 2008; Rothstein and Eek 2009). Trust relies on the condition that institutions are fair, efficient, and ruled by law. If this is the case, people will learn that, in relation to these institutions, and in meeting representatives of public institutions, the best strategy is to trust and to be trustworthy (e.g., refraining from offering bribes). Since institutional officers are human beings, trust in them spills over also to people in general (Rothstein 2004; Rothstein and Stolle 2008). Not only will people be more likely to act honestly, but they will also expect others to refrain from corruption, and thus trust becomes a general quality. If public institutions do not live up to noncorrupt and fair standards, people will be forced to adapt to the current practice and also engage in corruption—and will expect others to do so as well.

Thus, institutionalist theories of trust lean on the evaluation of performance. This means that trust comes from rational deliberation on the basis of information that we have on the trustee's previous behavior (Coleman 1994; Offe 1999; Gambetta 2000). The level of trust in public institutions rests on citizens' expectations, which are based on previous experiences of good or bad governance. If, for example, the police authority acts in a way that is fair

and efficient, trust in this institution will be high. If the police have done a bad job, trust will diminish. Thus, trust is quite vulnerable and changes if expectations are not met.

In contrast, according to Luhmann (the foremost theorist among those who represent a sociological perspective on trust), trust is a communicative means to reduce complexity (Luhmann 1979, 8). It should be separated from confidence, which corresponds to systemic trust and comes from socialization. The latter concerns functional systems such as the economy and politics and is not founded on interpersonal relations, but as with trust it works in a complexity-reducing way (Luhmann 1979, 102). Luhmann's seminal work is a source of inspiration to sociocultural approaches to trust.

From a sociocultural perspective, in contrast to institutionalist theory, trust emerges from below. Sociocultural theory on trust provides an alternative view of trust as dependent on societal patterns and attitudes based on people's personal and social history. It accommodates several different orientations with partly different focuses, such as normative standards as a condition for trust (Uslaner), social capital theory (Putnam), and trust understood as routinized behavior (Giddens). But bringing these together is the idea that trust has other causes than rationalist deliberation on the performance of the trustee. From Putnam we learn that the root of any kind of trust is found in close relationships within a strong civil society and in social networks, which lay the foundation for social capital (Putnam 1993). Giddens separates trust between people—facework commitments—from trust as faceless commitments. The latter concern the way people handle the uncertainty associated with what he calls the abstract incomprehensible systems that comprise modern societies. For Giddens (1990, 1991), both kinds of trust rely on the continuity of daily life and habitual routines, that is, the ability to "bracket ignorance." Uslaner (2013, 630), who developed the idea of trust as a norm, argues that trust is "the belief that we ought to trust others because they are part of our moral community." Moral dispositions to trust are grounded in close relations and in early childhood, where trust is learned from families and relatives (Uslaner 2000, 571). This is where essential particular trust is built. Positive experiences of particular social trust will gain a norm-like quality, and this positively affects the confidence in people whom you don't know (general social trust). Norms work as guidelines in our social contacts and do not require rationalist deliberations in every situation.

From a sociocultural perspective, trust between people close to you, that is, particular trust, is where it all begins. Trustful experiences in families, neighborhoods, communities, and networks create a social capital of trustfulness and normative structures favorable to more abstract kinds of trust in a society. It would be a misunderstanding to think that sociocultural theorists are less interested in institutional trust than institutionalists. Rather, they argue that trust in public institutions originates not in performance but in social conditions and levels of social trust in a society. Institutional trust

emerges out of particular social trust or, formulated from a different conceptual angle, social capital. From trust in close relationships, social trust is generalized to wider circles of people and also promotes political trust (trust in institutions) (Newton and Zmerli 2011).

A sociocultural perspective also means that trust and distrust are regarded as quite stable things, once established. In a society long characterized by distrust, it is likely that distrust will persist. Trust and distrust are only to a very small extent sensitive to how institutions (or people) perform in the short run. This is a crucial difference when comparing this perspective to an institutionalist theory focusing on the evaluation of performance. Performance-based institutionalist theories imply that there is no relevant difference between different societies other than the quality of government and institutions. The fact that trust is higher in some states than in others results from better functioning state administrations, in which it is appropriate to trust. From the sociocultural perspective, in contrast, variations in institutional trust should be traced to legacies or structures not directly related to institutional performance. These legacies may be theorized in terms of social capital, norms, early socialization into trustful dispositions, or routinized behavior.

The institutionalist take on trust and surveillance attitudes

Since surveys find a stronger association between institutional trust, as opposed to social trust, and positive attitudes toward surveillance, it may seem reasonable to assume that the institutionalist perspective has explanatory leverage. This would mean that people's attitudes toward surveillance follow from their evaluation of institutional performance. An institutional perspective requires that people have an opinion on the performance of institutions (quality of government) in the country in which they live. If people appreciate government, which is most likely in democratic countries, they should also be more content with being monitored by the state—or to put it differently, they should be less concerned about the risk of governmental abuse when it comes to surveillance (Denemark 2012). Thus, the arrow goes from institutional trust to affirmation of surveillance.

However, the relationship between evaluation of institutions, or government in general, and trust remains obscure—a problem that is manifested in the practice of using a composite variable when operationalizing institutional trust in social surveys. There is a cumbersome gap between trust in a number of institutions and attitudes to surveillance. Therefore, Watson, Finn, and Barnard-Wills (2017) argue that rather than studying institutional trust in general, studies ought to focus more on trust in particular surveillance institutions. If we are interested in what performance means for attitudes to surveillance, we should probably be as specific as possible concerning institutions. Relevant

institutions need to be defined for the type of surveillance that respondents are asked to relate to. Enumerative definitions are sometimes useful, but they are also problematic, since they often have a rather weak theoretical foundation (Schneider 2017). Likewise, it is important to carefully define what kind of surveillance respondents are asked to have an opinion about (Steinfeld 2017). Narrowing the take on institutions—for example, a focus on secret surveillance agencies or the police—as well as specifying the type of surveillance in question make it possible to theorize more thoroughly on the direction of the causal arrow. In fact, from an institutionalist perspective focusing on performance, it seems reasonable to treat surveillance, and not trust, as the independent variable. Surveillance is institutional performance and may go into the evaluation of the institution, underpinning or undermining trust.

Still, in order to bring about trust in an institution, knowledge about institutional performance is needed. Knowledge, in this context, usually comes from access to information. Thus, transparency is a fundamental ingredient in a performance-based approach to trust, and this is a difficult thing when it comes to surveillance policies, which often, by nature, lack transparency. Certainly, some surveillance activities are more open than others, and sometimes governments prescribe a certain amount of transparency, for example, in requiring signs indicating camera monitoring. Generally, however, surveillance is based on the condition that everything cannot be made transparent. In the words of Monahan and Regan (2012), surveillance practices create "zones of opacity."

The importance of transparent institutions has been a focus of both academic debate and public policies for some time (Kafer 2016). On the one hand, transparency is associated with governmental accountability and legitimacy (Taylor 2011; Brucato 2015) and discussed as a measure to enhance trust in governments and public institutions (Cucciniello and Nasi 2014; Kim and Lee 2012). On the other hand, Moore (2018) and others relativize the apparent objectivity in transparent policies and argue that facts and information are not always intelligible without contextual references. Grimmelikhuijsen (2012) finds that the effect of transparency on trust in government is small. Since trust is a mix between knowledge and feelings, increased knowledge stemming from open government may have a very limited effect. More disclosure when it comes to police brutality in the United States, for example, did not change public attitudes toward the police (Brucato 2015). Mason, Hillenbrand, and Money (2014), in a study on attitudes toward the British police, find that respondents with more initial trust did not change their opinion regardless of whether they were exposed to negative or positive information on police performance. Other conditions, beyond facts, influenced their opinion. In some cultural contexts, increased transparency may even have a negative impact on trust. Where the power distance between government and citizens is traditionally large, citizens may be sensitive to a disclosure that "construes their government in a less competent light" (Grimmelikhuijsen et al. 2013, 583).

In sum, there are three interrelated problems with applying an institutionalist perspective to the results of survey studies. First, it can hardly account for the idea that institutional trust affects surveillance attitudes unless we circumscribe trust to mean trust in particular surveillance institutions. Second, if we do this, we still have the problem that surveillance policies are seldom open to scrutiny by the public and, thus, cannot be fully evaluated. Third, the closer we get to particular surveillance agencies and particular types of surveillance, the harder it becomes to discern the causal direction, making the chicken and egg problem intractable without further theorizing.

Thus, this discussion casts doubt on the direction of the causal arrow from institutional trust to surveillance attitudes. Since surveillance policies are performance, and performance is regarded as the basis of trust, the sensible conclusion should be that attitudes to surveillance may also influence trust in institutions. Moreover, the institutionalist perspective is particularly problematic in the surveillance context since surveillance policies and practices, to a large extent, are not open for rational deliberation. Trust in the context of surveillance policies seems to come from other sources than information about institutional performance. This is where sociocultural aspects enter the discussion.

A sociocultural perspective on trust and surveillance

Is the relationship between trust and positive attitudes to surveillance easier to grasp if we understand trust in terms of norms rather than performance? Norms are less sensitive to facts than what is required for evaluations of performance—at least in the short run. Trust toward people or institutions is not based on rational consideration but on more unreflected practices—a personal or collective code of behavior.

Although there are large variations in levels of trust in public institutions in democratic societies, it is still common for a fairly large group of people state that they trust institutions at least to some extent. From a sociocultural perspective, it should be argued that the reason for this is not primarily that people have made an evaluation of the quality of government. Rather people may trust authorities simply because they adhere to a societal norm (or routines) to trust governmental institutions. People who trust the government in this way should be prone to accept policies, such as surveillance, without reflecting so much on its implications. Thus, the causal arrow goes from trust in institutions to attitudes to surveillance, and a positive association makes sense even in the absence of satisfactory performance. Possibly, these trust norms strengthen in times of perceived threats from crime and terrorism (Steinfeld 2017). However, the problem here is that, if we take this approach too far, we run the risk of underestimating people's ability to think for themselves and to evaluate the pros and cons of surveillance. If we are completely subordinated to social norms, debates on surveillance practices will be harder to accomplish.

The real merit of a sociocultural perspective on trust and surveillance is that it can account for movements coming from below that reflect what happens in people's everyday lives. Norms are not easily changed, but from a sociocultural perspective trust as a norm originates in experiences that we have from people we meet in our daily contacts and personal networks. Therefore, a sociocultural perspective accommodates the possibility that surveillance may destroy trust as we know it. If trust is about socialization and comes from experiences in close relations, then negative experiences with, for example, the local police may destroy trust from below with long-term effects on other types of trust and on norms of trust in a society (Ali 2016; Alam and Husband 2013; Duck 2017). Thus, although social survey studies find a positive relationship between trust and acceptance of surveillance, the more qualitative case studies referred to above, indicating a negative association, may tell something about what we should expect from the future. The sociocultural perspective opens space for considering how social changes may affect the trust–surveillance relationship (see, e.g., Lyon 2018). This perspective also promotes a discussion on alternative ways to enact trust.

A short historical retrospective will help to illustrate this argument. Scholars with a sociocultural orientation suggest that trust develops in relation to the overall organization of social relations in a society (Misztal 1996). Premodern agrarian society was characterized by closed and predictable social structures at the local level. Small-scale relations dominated, and rules, roles, and social control associated with these relations set the agenda for trust—which were confined mostly to people with whom one was already familiar. Modern societies are more complex, and in order to adapt to the anonymous relations featured in large markets and welfare states, more general and abstract forms of trust were required (Seligman 1997). But is this the last step, or may other forms of trust and ways of enacting trust emerge? We need to reflect on the fact that social trust levels are dropping in many countries and relate these findings to increased surveillance in society (Craven, Monahan, and Regan 2015). Is it that surveillance destroys trust, or do we witness a transformation in the way people relate to each other that mirrors alternative forms of the social contract? These questions can be addressed by exploring the relationship between trust and control. With control I here mean the social control over individuals within a society that substantiates a social order.

From a sociocultural perspective, social trust is to a certain extent about control. Trustworthiness and compliance with norms favoring trust may form the basis for social inclusion, while noncompliance might justify exclusion. General social trust can be described as a control-like norm-conformity (Offe 1999).

> (W)hen actors generalize trust, in the sense that within particular social structures the assumption of benevolent agency is no longer tied to individual actors, but expected of all actors concerned (…), then this

> generalized trust gains a control-like quality as actors become embedded in it.
>
> (Möllering 2005, 292)

Knights et al. (2001, 315) refer to "the production and maintenance of 'trust' as itself closely related to particular systems of power and control." The control element in social trust is crucial to the understanding of the trust–surveillance nexus as it appears in the late modern era of constantly expanding surveillance policies.

Normally, we perceive trust as associated with informal social control. But increasingly complex societies set the scene for different ways to pursue control (Giddens 1990). Today, "people do not need to trust one another since they can rely upon institutions to rectify problems that arise" (Gibson 2001, 66). A bit simplified one could say that you don't need to build trust between yourself and your neighbors since the police will do it for you—which is frequently accomplished with the use of cameras or other surveillance methods. The eyes of cameras replace the eyes of people (Fyfe and Bannister 1998). Social informal control is replaced by institutional "control at a distance" (Monahan 2009). Differently put, citizens trust governments and public institutions, such as the police, to distrust (and control) their fellow citizens—those who are suspected of not having "pure flour in their bags" (Björklund 2011). Szrubka (2013) gives a telling illustration of how traditional informal social control—trust—may be replaced by control at a distance—i.e. surveillance. In his study on the use of cameras in Polish ambulances, he notes that cameras in the cars transform trust between the personnel and the patient. The intention behind camera surveillance is to protect the patients against theft in a situation where they cannot protect their belongings and to protect the personnel from theft accusations. Thus, surveillance of medical authorities (at a distance) replaces trust between human beings or, in other words, the nature of trust changes. To the satisfaction of all involved, trust is enacted as surveillance.

A sociocultural perspective, allowing for changes in the very nature of trust, opens space for new interpretations of the positive relationship between institutional trust and the acceptance of surveillance. It implies that the positive relationship mirrors a new understanding of trust, one that conflates trust with surveillance and thus makes the question of what explains what in trust and surveillance less relevant. Surveillance fills a trust deficit, which becomes increasingly significant, thus altering the very meaning of trust.

Conclusion

Now we can revisit the tension outlined in the introduction between survey results that show a positive correlation between trust and surveillance and

the more dire expectation that surveillance has a destructive effect on trust. The discussion above shows that although trust may be related to positive attitudes to surveillance, it is hard to comprehend this in terms of institutional performance. From a sociocultural perspective, predictions from social survey studies on the positive association between trust and surveillance attitudes do not stand in opposition to warnings about a future ruled by distrust. This perspective also opens space for studying transformations in the idea of trust over time and suggests that this might be a fruitful direction for further research.

Findings that trust in institutions increases the likelihood to consent to surveillance do not make much sense in the absence of a theory of the origins and dynamics of social trust relations. Trust approached as a social practice seems to offer more explanatory leverage to the contradictory empirical results with respect to surveillance. In this context, it is of great importance to focus on the relationship between trust and surveillance at the micro level, in local communities, and trust between people and toward the local police. Most likely, it is here that processes begin that may in the end erode or transform trust between people. This insight suggests that we need more empirical research on the effects of surveillance in peoples' everyday lives. This could be, for example, long-term studies on how the introduction of camera surveillance affects the relations between residents in a living area. Does it have any effect on how people practice trust, and in case it has—how so exactly?

In this chapter, I demonstrate that the way trust is approached affects the analysis of the trust and surveillance relationship. The results from survey studies on the relationship between (institutional) trust and attitudes to surveillance are of little interest if we do not engage in a theoretical discussion on what these results really stand for. The narrower take offered by an institutionalist perspective on trust is not sufficient in this context, and since it rests on institutional performance its applicability is limited in the context of a surveillance that is mostly hidden from the public. A sociocultural approach to trust, in contrast, has great benefits if we want to gain a deeper understanding of the trust and surveillance nexus. We should not be content with noting that the association between social trust and attitudes to surveillance is weak according to findings in social surveys. There are social mechanisms around trust and surveillance that may affect the association and reveal that surveillance tends to become a substitute for social trust. Control at a distance, in terms of technology, replaces informal control, in terms of social trust. A sociocultural perspective gives the opportunity to contextualize the relationship between trust and attitudes to surveillance and to substantially contribute to the understanding of how this relationship may work in the long run. A sociocultural approach helps us to understand how trust works with surveillance in societies where surveillance has become, more or less, the new normal.

References

Alam, Yunis, and Charles Husband. 2013. "Islamophobia, Community Cohesion and Counter-Terrorism Policies in Britain." *Patterns of Prejudice* 47(3): 235–52.

Ali, Arshad I. 2016. "Citizens under Suspicion: Responsive Research with Community under Surveillance." *Anthropology & Education Quarterly* 47(1): 78–95.

Bennett, Colin J. 2011. "Review. In Defence of Privacy: The Concept and the Regime." *Surveillance & Society* 8(4): 485–96.

Björklund, Fredrika. 2011. "Pure Flour in Your Bag: Governmental Rationalities of Camera Surveillance in Sweden." *Information Polity* 16(4): 355–68.

Björklund, Fredrika. 2019. "Vilken roll spelar risk i tillit? En diskussion om begreppet generaliserad tillit." *Statsvetenskaplig Tidskrift* 121(1): 45–63.

Bjørnskov, Christian, and Gert Tinggaard Svendsen. 2013. "Does Social Trust Determine the Size of the Welfare State? Evidence Using Historical Identification." *Public Choice* 157: 269–86.

Brucato, Ben. 2015. "The New Transparency: Police Violence in the Context of Ubiquitous Surveillance." *Media and Communication* 3(3): 39–55.

Cao, Liqun, Jihong Zhao, Ling Ren, and Ruohui Zhao. 2015. "Do In-Group and Out-Group Forms of Trust Matter in Predicting Confidence in the Order Institutions? A Study of Three Culturally Distinct Countries." *International Sociology* 30(6): 674–93.

Coleman, James S. 1994. *Foundations of Social Theory.* Cambridge: Belknap.

Craven, Krista, Torin Monahan, and Priscilla Regan. 2015. "Compromised Trust: DHS Fusion Centers' Policing of the Occupy Wall Street Movement." *Sociological Research Online* 20(3): 5, DOI:10.5153/sro.3608.

Cucciniello, Maria, and Greta Nasi. 2014. "Transparency for Trust in Government: How Effective is Formal Transparency?" *International Journal of Public Administration* 37(13): 911–21.

Denemark, David. 2012. "Trust, Efficacy and Opposition to Anti-Terrorism Police Power: Australia in Comparative Perspective." *Australian Journal of Political Science* 47(1): 91–113.

Duck, Waverly. 2017. "The Complex Dynamics of Trust and Legitimacy: Understanding Interactions between the Police and Poor Black Neighborhood Residents." *ANNALS AAPSS* 673: 132–49.

Ellis, Darren, David Harper, and Ian Tucker. 2013. "The Dynamics of Impersonal Trust and Distrust in Surveillance Systems." *Sociological Research Online* 18(3): 8, DOI:10.5153/sr0.3091.

Ford, Nicole M. 2017. *Measuring Trust in Post-Communist States; Making the Case for Particularized Trust.* University of South Florida: Scholar Commons. Dissertation.

Freitag, Markus, and Marc Bühlmann. 2009. "Crafting Trust: The Role of Political Institutions in a Comparative Perspective." *Comparative Political Studies* 42(12): 1537–66.

Freitag, Markus, and Richard Traunmüller. 2009. "Spheres of Trust: An Empirical Analysis of the Foundations of Particularised and Generalised Trust." *European Journal of Political Research* 48: 782–803.

Friedewald, Michael, Marc van Lieshout, Sven Rung, and Merel Ooms. 2016. "The Context-Dependence of Citizens' Attitudes and Preferences Regarding Privacy and Security." In *Data Protection on the Move: Current Developments in ICT and*

Privacy/Data Protection, edited by Serge Gutwirth, Ronald Leenes, and Paul De Hert, 51–74. Dordrecht: Springer.

Friedewald, Michael, Sven Rung, Marc van Lieshout, Merel Ooms, and Jelmer Ypma. 2015. *Report on Statistical Analysis of the PRISMS Survey.* PRISMS project deliverable 10.1. Karlsruhe: Fraunhofer Institute for Systems and Innovation Research.

Fyfe, Nicholas R., and Jonathan Bannister. 1998. "The 'Eyes Upon the Street': Closed Circuit Television Surveillance and the City." In *Images of the Street: Representation, Experience and Control in Public Space*, edited by Nicholas R. Fyfe, 254–67. London: Routledge.

Gambetta, Diego. 2000. "Can We Trust Trust?" In *Trust: Making and Breaking of Cooperative Relations* (Electronic Edition), edited by Diego Gambetta, 213–37. Oxford: Basil Blackwell, www.sociology.ox.ac.uk/papers/ gambetta213-237.pdf.

Gibson, James L. 2001. "Social Networks, Civil Society, and the Prospects for Consolidating Russia's Democratic Transition." *American Journal of Political Science* 45(1): 51–68.

Giddens, Anthony. 1990. *The Consequences of Modernity.* Stanford: Stanford University Press.

Giddens, Anthony. 1991. *Modernity and Self-Identity: Self and Society in the Late Modern Age*. Cambridge: Polity Press.

Goold, Benjamin. 2009. "Technologies of Surveillance and the Erosion of Institutional Trust." In *Technologies of Insecurity: The Surveillance of Everyday Life*, edited by Katja Frank Aas, Helene Oppen Gundhus, and Heidi Mork Lomell, Chapter 10. Oxon: Routledge.

Graeff, Peter, and Gert Tinggaard Svendsen. 2013. "Trust and Corruption: The Influence of Positive and Negative Social Capital on the Economic Development in the European Union." *Quality and Quantity* 47: 2829–46.

Grimmelikhuijsen, Stephan. 2012. "Linking Transparency, Knowledge and Citizen Trust in Government: An Experiment." *International Review of Administrative Sciences* 78(1): 50–73.

Grimmelikhuijsen, Stephan, Gregory Porumbescu, Boram Hong, and Tobin Im. 2013. "The Effects of Transparency in Trust in Government: A Cross National Comparative Experiment." *Public Administration Review* 73(4): 575–86.

Inglehart, Ronald. 1990. *Cultural Shift in Advanced Industrial Society*. Princeton: Princeton University Press.

Jamal, Amaney, and Irfan Nooruddin. 2010. "The Democratic Utility of Trust: A Cross National Analysis." *The Journal of Politics* 72(1): 45–59.

Kafer, Gary. 2016. "Reimaging Resistance: Performing Transparency and Anonymity in Surveillance Art." *Surveillance & Society* 14(2): 227–39.

Khodyakov, Dmitry. 2007. "Trust as a Process: A Three-Dimensional Approach." *Sociology* 41(1): 115–32.

Kim, Soonhee, and Jooho Lee. 2012. "E-participation, Transparency and Trust in Local Government." *Public Administration Review* 72(6): 819–28.

Knights, David, Faith Noble, Theo Vurdubakis, and Hugh Willmott. 2001. "Chasing Shadows: Control, Virtuality and the Production of Trust." *Organization Studies* 22(2): 311–36.

Lühiste, Kadri. 2006. "Explaining Trust in Political Institutions: Some Illustrations from the Baltic States." *Communist and Post-Communist Studies* 39(4): 475–96.

Luhmann, Niklas. 1979. *Trust and Power.* Chichester: Wiley.
Lyon, David. 2003. *Surveillance after September 11.* London: Polity Press.
Lyon, David. 2018. *The Culture of Surveillance: Watching as a Way of Life*. London: Polity Press.
Maras, Marie-Helen. 2012. "The Social Consequences of a Mass Surveillance Measure: What Happens When We Become the 'Others'?" *International Journal of Law, Crime and Justice* 40: 65–81.
Mason, David, Carola Hillenbrand, and Kevin Money. 2014. "Are Informed Citizens More Trusting? Transparency of Performance Data and Trust Towards a British Police Force." *Journal of Business Ethics* 112: 321–41.
Mishler, William, and Richard Rose. 2001. "What Are the Origins of Political Trust? Testing Institutional and Cultural Theories in Post-Communist Societies." *Comparative Political Studies* 34(1): 30–62.
Misztal, Barbara, A. 1996. *Trust in Modern Societies.* Oxford: Polity Press.
Monahan, Torin. 2009. "Dreams of Control at a Distance: Gender, Surveillance and Social Control." *Cultural Studies, Critical Methodologies* 9(2): 286–305.
Monahan, Torin, and Priscilla M. Regan. 2012. "Zones of Opacity: Data Fusion in Post-9/11 Security Organizations." *Canadian Journal of Law and Society* 27(3): 301–17.
Möllering, Guido. 2005. "The Trust/Control Duality: An Integrative Perspective on Positive Expectations of Others." *International Sociology* 20(3): 283–305.
Moore, Sarah. 2018. "Towards a Sociology of Institutional Transparency: Openness, Deception and the Problem of Public Trust." *Sociology* 52(2): 416–30.
Nakhaie, Reza, and Willem de Lint. 2013. "Trust and Support for Surveillance Policies in Canadian and American Opinion." *International Criminal Justice Review* 23(2): 149–69.
Nannestad, Peter. 2008. "What Have We Learned About Generalized Trust, If Anything?" *Annual Review of Political Science* 11: 413–36.
Newton, Ken, and Sonja Zmerli. 2011. "Three Forms of Trust and Their Association." *European Political Science Review* 3(2): 169–200.
Offe, Claus. 1999. "Trust and Knowledge, Rules and Decisions: Exploring a Difficult Conceptual Terrain." In *Democracy and Trust*, edited by Mark E. Warren, 42–87. Cambridge: Cambridge University Press.
Patil, Sunil, Bhanu Patruni, Hui Lu, Fay Dunkerley, James Fox, Dimitris Potoglou, and Neil Robinson. 2014. *Public Perceptions of Security and Privacy: Results of the Comprehensive Analysis of PACT's Pan-European Survey.* PACT project deliverable 4.2. Brussels: RAND Europe.
Pavone, Vincenzo, Sara Degli-Esposti, and Elvira Santiago. 2015. *Key Factors Affecting Public Acceptance and Acceptability of Surveillance-Oriented Security Technologies (SOSTs).* SurPRISE project deliverable 2.4. Florence: European University Institute.
Perry-Hazan, Lotem, and Michael Birnhack. 2018. "The Hidden Human-Rights Curriculum of Surveillance Cameras in Schools: Due Process, Privacy and Trust." *Cambridge Journal of Education* 48 (1): 47–64.
Putnam, Robert D. 1993. *Making Democracy Work: Civic Traditions in Modern Italy.* Princeton: Princeton University Press.
Raab, Charles. 2012. "Privacy, Social Values and the Public Interest." *PVS* 46: 129–51.

Richey, Sean. 2010. "The Impact of Corruption on Social Trust." *American Politics Research* 38(4): 676–90.
Rothstein, Bo. 2004. "Social Trust and Honesty in Government: A Causal Mechanisms Approach." In *Creating Social Trust in Post-Socialist Transition*, edited by János Kornai, Bo Rothstein, and Susan Rose-Ackerman, 13–30. New York: Palgrave Macmillan.
Rothstein, Bo. 2005. *Social Traps and the Problem of Trust.* Cambridge: Cambridge University Press.
Rothstein, Bo. 2010. "Happiness and the Welfare State." *Social Research* 77(2): 441–68.
Rothstein, Bo, and Daniel Eek. 2009. "Political Corruption and Social Trust: An Experimental Approach." *Rationality and Society* 21(1): 81–112.
Rothstein, Bo, and Dietlind Stolle. 2008. "The State and Social Capital: An Institutional Theory of Generalized Trust." *Comparative Politics* 40(4): 441–59.
Schneider, Irena. 2017. "Can We Trust Measures of Political Trust? Assessing Measurement Equivalence in Diverse Regime Types." *Social Indicators Research* 133: 963–84.
Seligman, Adam B. 1997. *The Problem of Trust.* Princeton: Princeton University Press.
Sønderskov, Kim M., and Peter Thisted Dinesen. 2016. "Trusting the State, Trusting Each Other? The Effect of Institutional Trust on Social Trust." *Political Behavior* 38: 179–202.
Sorell, Tom. 2011. "Preventive Policing, Surveillance, and European Counter-Terrorism." *Criminal Justice Ethics* 30(1): 1–22.
Steinfeld, Nili. 2017. "Track Me, Track Me Not: Support and Consent to State and Private Sector Surveillance." *Telematics and Informatics* 34: 1663–72.
Svenonius, Ola, and Fredrika Björklund. 2018. "Explaining Attitudes to Secret Surveillance in Post-Communist Societies." *East European Politics* 34(2): 123–51.
Szrubka, Wojciech. 2013. "Video Surveillance and the Question of Trust." *In Video Surveillance and Social Control in a Comparative Perspective*, edited by Fredrika Björklund, and Ola Svenonius, 131–52. New York: Routledge.
Sztompka, Piotr. 1999. *Trust: A Sociological Theory.* Cambridge: Cambridge University Press.
Sztompka, Piotr. 2005. "Comments on Paul Dumouchel." *Archives Europeennes De Sociologie* 46(3): 432–6.
Taylor, Nick. 2011. "A Conceptual Legal Framework for Privacy, Accountability and Transparency in Visual Surveillance Systems." *Surveillance & Society* 8(4): 455–70.
Uslaner, Eric M. 2000. "Producing and Consuming Trust." *Political Science Quarterly* 115(4): 569–90.
Uslaner, Eric M. 2013. "Trust as an Alternative to Risk." *Public Choice* 157 (3–4): 629–39.
Watson, Hayley, Rachel L. Finn, and David Barnard-Wills. 2017. "A Gap in the Market: The Conceptualization of Surveillance, Security, Privacy and Trust in Public Opinion Surveys." *Surveillance & Society* 15(2): 269–85.
Welzel, Christian, and Jan Delhey. 2015. "Generalizing Trust: The Benign Force of Emancipation." *Journal of Cross-Cultural Psychology* 46(7): 875–96.

Chapter 11

Trustworthy humans and machines

Vulnerable trustors and the need for trustee competence, integrity, and benevolence in digital systems

Sara Degli-Esposti and David Arroyo

Introduction: trust and digital mediation

In the future happening today coders dream of erasing discrimination and corruption by replacing traditional institutions with new digital systems such as Distributed Ledger Technologies, or DLTs, in an attempt to restructure old institutions by means of computer code rather than through collective action. Satoshi Nakamoto's (2008) blockchain proposal to generate electronic transactions and cryptocurrency "without relying on trust" exemplifies this attitude, namely the use of *lex cryptographia* to restore institutions (De Filippi and Loveluck 2016). The problem with these kinds of proposals is that dependence on Information and Communication Technologies (ICT) may lead to an overabundance of trust in untrustworthy, yet credible and sometimes dependable, systems.

Our objective in this chapter is to discuss issues of dependence in the trust relationship that limit the ability of transparency to guarantee the trustworthiness of the trustee. We embrace Onora O'Neill's (2017) invitation to focus on what really matters about trust, which is people's ability to trust the trustworthy and distrust the untrustworthy in the context of digitally mediated interactions, where cryptography is reshaping the relationship between computer code and legal compliance in unforeseeable ways. We deal with the need to establish mechanisms to ensure that trustees—those humans who design and operate the machines on behalf of others whose life depends on those systems and machines—are trustworthy.

We argue that a fundamental distinction needs to be drawn between dependability and trustworthiness. We agree with Helen Nissenbaum's (2004) view that visions of trust as security lead to surety—that is, safety and certainty—in a best-case scenario, but not to trust conceived as "the accepted vulnerability to another's possible but not expected ill will (or lack of good will) toward one" (Baier 1986, 235). We contend that we need to move from dependability to trustworthiness to be able to deal with uncertainty. Under "unknown unknowns," which are risks that come from situations that are unexpected—a topic widely discussed in security studies—mechanisms to guarantee the

DOI: 10.4324/9781003120827-15

trustees' competence, integrity, and benevolence are necessary to build trust in institutions and organizations (Mayer, Davis, and Schoorman 1995). Similarly, when trustors are highly vulnerable and dependent—for example, in the case of citizens versus law enforcement agents—transparency plays a limited role in giving them control over trustees' actions. Under these types of circumstances, those interested in designing resilient organizational or technical systems would look for mechanisms to ensure trustees' competence, integrity, and benevolence. Benevolence, for example, has been demonstrated to be particularly important for trust relationships in the context of digital surveillance technologies used by law enforcement agencies (Degli Esposti, Ball, and Dibb 2021).

This chapter hopes to contribute to the dialogue between social science and computer science by replacing the traditional trust-as-control paradigm with a vision of trust-as-care. We focus on the implications of this view of trust for the field of security engineering, which is devoted to ensuring the dependability of systems and devices. We argue that this new vision would be better suited to articulating the relationship between humans and machines, so important in the path toward trustworthy artificial intelligence, or AI (AI-HLEG 2019a, 2019b).

Trust as control: the rationalistic instrumental paradigm

Trust represents a sort of leap of faith in another person's willingness to cooperate with us. A trust relationship involves two specific parties: a trusting party—that is, the individual rendering trust judgments (trustor)—and a party to be trusted (trustee) (Jones and Shah 2016). The trustee seems to be motivated either by self-interest or by benevolence toward the trustor. Hardin's (2002, 4) influential definition of trust as "encapsulated self-interest"—"I trust you because I think it is in your interest to attend to my interest in the relevant matter"—represents the mainstream approach foregrounding self-interest. According to Hardin (2002), there are three mechanisms by which the trustee can encapsulate the interest of the trustor. First, the two of them have established an ongoing relationship, which is valuable for the trustee. Second, the trustee loves or is a friend of the trustor; thus, the trustor can count on the trustee's benevolence. Third, the trustee wants to maintain his or her good reputation, which provides motivation to behave in a trustworthy manner.

The rationalistic instrumental paradigm of trust has been criticized for its individualistic, utilitarian assumptions, which emphasize individual self-interest over collective benefits. Experimental methods, games and abstract dilemmas, and disembodied human interactions have repeatedly questioned the validity of this approach. According to Michael Hechter (1992, 34), there is "ample reason to be skeptical of the sufficiency of game theory for

the solution of real-world collective action problems." As many empirical studies show, there is no society in which behavior is consistent with the selfishness axiom (Henrich et al. 2004). The problem is that self-interest does not explain sacrifice; sacrifice generated by affection or by a duty of care is central to the experience of those who care about other people's survival. In the view of psychologist Roderick Kramer (2009), "human beings are naturally predisposed to trust" because "it's a survival mechanism that has served our species well." The "care-giving we provide to others is as fundamental to human nature as our selfishness or aggression" (Taylor 2014, 4). Trustors' and trustees' shared experiences and destinies irreversibly forge their identities. This vision of intertwining paths, which should lead toward beneficial collective outcomes, is ignored by players trapped within a utilitarian logic.

Another limitation of the rationalistic instrumental paradigm is its tendency to deny the role of history and social norms. Collective history offers guidance to individuals on whether norms of trust and reciprocity exist and will be respected in each context (Berg, Dickhaut, and McCabe 1995). Some scholars argue that people appear to follow an "injunctive norm," which impels them to trust the character of the other person (see e.g., Fetchenhauer, Dunning, and Shlösser 2017). Those who believe that cooperation is beneficial and are willing to cooperate are also more inclined to believe that other people will share the same view and will behave accordingly. In ongoing relationships, expectations of reciprocity facilitate cooperation (Axelrod 1997) and may also influence perceptions of trustworthiness, which relates to the trustor's confidence in the trustee based on experiences or beliefs (Berg, Dickhaut, and McCabe 1995). Of course, when the relationship is sporadic—so that the trustee does not face any negative consequence caused by the trustor's lack of future cooperation—the incentives to deceive the other person may increase.

To conclude, we may assume that a good proportion of humans are wise and willing to care for human survival and thus acknowledge the value of cooperation and reciprocity. These humans may decide to set trust as a default systemic parameter. The assumption that trust—rather than distrust—is taken as the default position in many cultures finds additional support in the next section, where we consider some psychological studies and introduce a new characterization of the trustee–trustor relationship.

Trust as care: on the trustor's vulnerability and the trustee's benevolence

Mayer, Davis, and Schoorman (1995, 712) interpret trust as "the willingness of a party to be vulnerable to the actions of another party based on the expectation that the other will perform a particular action important to the trustor, irrespective of the ability to monitor or control that other party." In their theoretical model, the level of trust is determined by the trustee's ability, benevolence, and integrity and by the trustor's propensity to trust.

The way the trustor interprets the context of the relationship affects the need for trust, risk assessment, and the evaluation of the trustee's trustworthiness. The tendency to trust another party is a function of the type of motivation attributed to the other: the more a person perceives another person to be benevolently motivated, the more likely they are to like and trust that person (Colquitt, Scott, and LePine 2007; Van Lange, Rockenbach, and Yamagishi 2017).

Thus, questions of trust seem to arise when an individual is in a relationship that entails some risk of becoming vulnerable to the actions or decisions of another person (Levi and Stoker 2000). There are scholars who see a moral component in trust relationships. For instance, LaRue Hosmer (1995, 393) defines trust as

> the reliance by one person, group, or firm upon a voluntarily accepted duty on the part of another person, group, or firm to recognize and protect the rights and interests of all others engaged in a joint endeavor or economic exchange.

Within this second group, we agree with those scholars who highlight the vulnerability of the trustor. However, what prevents trustees from taking advantage of the vulnerability of the trustors? In other words, what is it that makes trustees trustworthy?

The *empowering theory of trust* suggests that by manifestly relying on another person B—by exercising trust—a person A may not only cause B to exercise their existing capacity for trust-responsiveness, but A may also cause B to *develop* that capacity, achieving a higher degree of dependability or durability. According to McGeer and Pettit (2017), three psychological effects contribute to what they call the "situational enhancement of dependability." The first is that when player A trusts player B, they display and communicate a belief in B's capacity to be motivated by A's manifest reliance, thereby encouraging B to prove reliable. The second is that when A trusts B to do something, A often makes a request, explicit or implicit, that B should do what is requested. And the third is that when A trusts B, A displays a good opinion of B's dependability, thereby giving B an extra esteem-based motive for not letting A down (see also Elster 2007). When player A decides to trust player B, this decision has a positive, empowering impact on B's psychology (Pettit 2002).

Thus, the mere fact of trusting—or declaring that one trusts—creates an obligation for the trustee to honor that trust, which (assuming some moral responsiveness to obligation on the part of the trustee) increases the probability that the trustee will demonstrate greater trustworthiness than originally expected. From an instrumental, utilitarian perspective, these reflections leave open questions on how to secure trustworthiness in the absence of transparency and control but in the presence of vulnerability and dependence. The

problem of discretion and lack of trustor's control over the trustee is well represented in the principal(trustor)–agent(trustee) model. The principal (e.g., a patient) has to delegate a task to an agent (e.g., a doctor) because the former lacks the ability to perform it. From a rationalistic, instrumental view, the principals can monitor the agents or create economic incentives to ensure they act in a trustworthy manner, that is, in the best interest of the principals.

The problem with the principal–agent framework is that it assumes the agent knows what is in the best interest of the principal. In other words, the theory assumes the agent's competence. It also assumes the principal has the power and the information to make the agent accountable. However, if we observe trust from the vantage point of the vulnerable—the newborn baby, the dependent elderly, the sick person—information loses its value and power is completely imbalanced. The newborn cannot assess its caregiver's intention or ability, even though survival depends on the caregiver's benevolence and competence. A capital of trust is handed over to the trustee as a blank check. The return of that investment will become visible in the long term with limited initial accountability. In the case presented here, we assume that the benevolence of the agents-trustees will motivate them to become competent and to act with integrity. Nonetheless, the principals-trustors' vulnerability prevents any meaningful expression of control through transparency on the other side of the relationship.

To sum up, we contend that the rationalistic instrumental paradigm offers an illusion of freedom and a denial of dependence, which are both dangerously misleading. The trust-as-control paradigm resolves any moral hazard problem by means of transparency, today achieved through digital surveillance. This vision generates widespread reliance on risk-based methodologies across different areas and a growing demand for data. We contend that mechanisms such as transparency cannot be effective in the presence of a high imbalance of power and that only agents on a level playing field can exercise meaningful mutual oversight. Furthermore, the trust-as-control paradigm offers no indication as to how to inscribe competence and moral principles into a trustee's identity. We stress the importance of benevolence in the trust relationship in the presence of vulnerable trustors. Benevolence in this scenario matters because it determines whether humans in power will decide to deceive other dependent and vulnerable humans or treat them with care and respect.

To better articulate these reflections, in the next section we propose an alternative characterization of the trustor–trustee relationship: the *caring one* (trustee) and the *vulnerable other* (trustor). This vision of trust as embracing the care of the vulnerable resembles the one adopted by Gus Hurwitz (2012), who takes trust to mean "reliance without recourse" in the context of online interactions. It also resonates with Annette Baier's (1986, 240) definition, which says that "[trust] is letting other persons (natural or artificial, such as

firms, nations, etc.) take care of something the trustor cares about, where such 'caring for' involves some exercise of discretionary powers."

The caring one (trustee) and the vulnerable other (trustor)

In the presence of vulnerable and dependent trustors, trustees need to demonstrate their competence, honesty, and benevolence in order to be considered trustworthy, that is, *able to meet the promise of care intrinsic to their role*. When trustors are vulnerable and dependent, trustees have to care for them in the absence of direct instructions on what the trustors need. The instrumental paradigm of trust-as-control offers the transparency of trustees' actions as a solution to any moral hazard or conflict of interests. However, this framework assumes trustees know how to act in the best interest of the trustors.

But, even assuming benevolence, how can trustees know what is beneficial for the trustors? We argue that the trustor needs not only the trustee's *dependability* but also their trustworthiness, that is, a mixture of *learned new knowledge* and *moral considerations* that will lead to some type of *wisdom*. The learning process leading to the creation of this knowledge base would start from a capital of affection that would make the trustee responsible for the wellbeing of the trustor. This capital, allocated without having previous knowledge of the trustworthiness of the trustee, would trigger a learning process that would lead the trustee to investigate a trustor's needs.

When the role is not defined by deep affection, duty of care principles could replace affection in guaranteeing effort is allocated to learning about a trustor's needs. Professional codes can instruct about the need to develop specific methodologies and about the necessity to embed empathy into trustees' professional identities (Kultgen 1988). Even though disciplinary methods can be applied to achieve transparency or to monitor professionalism (Fournier 1999), there are different domination and knowledge-generation dynamics at play in each case. In the trust-as-care scenario, norms of care are defined and voluntarily embraced by trustees within their epistemic communities (Haas 1992).

Mechanisms to foster professionalism differ from those transparency measures envisioned by supporters of the trust-as-control paradigm. Even though peer-pressure mechanisms may be present, it is the adoption of shared norms and mutual learning that makes trustees willing to become competent and that keeps them honest in the trust-as-care case. In other words, despite both being normative systems, the type of norms operative in the trust-as-control paradigm differs from that preached in the trust-as-care case. We next move this discussion to the implications of adopting the trust-as-care perspective in the fluid boundary where "the ordinary language systems terminate in the special sort of machine known as a human being" (Wiener 1988, 79).

From credible machines to dependable systems: drawing a distinction between dependability and trustworthiness

As machines are built by humans, we began by talking about the trustworthiness of those human beings acting in institutional or other organizational settings who create or operate technological systems. We now move to discuss the trustworthiness of the technical system itself; in the end we will reconcile the discussion about the trustworthiness of the machines and of their creators.

If we think about whether we trust computers, we will probably see them as reliable devices that enable us to perform daily activities such as reading emails, managing meetings, or editing and sharing documents. As noticed by Fogg and Tseng (1999), mass reliance on ICT would not be possible in a world where people were unwilling to trust credible computers. However, users' trust perceptions do not necessarily reflect trustworthiness attributes: malware or spear phishing attacks, for example, exploit systems' credibility to insert malicious code into the machines of their victims (Mitnick and Simon 2011).

The risks associated with the existence of malevolent agents, software, and untrusted hardware render trust a broad research topic, which spans areas as diverse as security and access control in computer networks, reliability in distributed systems, and policies for decision-making under uncertainty (Artz and Gil 2007). Even though the concept of trust in these different communities varies in how it is represented, computed, and used, overall we may say that "a trusted system or component is one whose failure can break the security policy, while a trustworthy system or component is one that won't fail" (Anderson 2008, 13). For instance, in the realm of the so-called Internet of Things (IoT), trust management implies ensuring that the physical perception layer made of sensors and actuators cooperates with the network layer, which transforms and processes sensed environment data, and with the application layer, which offers context-aware intelligent services (Sicari et al. 2015).

"Dependability is the system property that integrates such attributes as reliability, availability, safety, security, survivability, maintainability" (Avizienis, Laprie, and Randell 2001, 1). Dependable systems have integrity: they perform their intended functions in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation of the system (Greene 2014). To ensure the dependability of software and infrastructures, secure systems need to be able to operate within a context of adversity (Danezis 2014). Dependable systems are resilient[1]: they are able to resist and recover from disruptions and attacks.[2] Attackers can be passive or active, internal or external, and local or global with respect to the system they want to attack. A number of model-based evaluation techniques are available along with experimental red team-based approaches (Nicol, Sanders, and Trivedi 2004). In general, we may say that a trusted computing base (TCB) is a minimal set of components of a

system upon which the security of the entire system depends (Lysne 2018).[3] The objective of security engineering is "to design systems that are resilient in the face of malice, that degrade gracefully, and whose security can be recovered simply once the attack is past" (Anderson 2008, 212).

Authentic trustworthy trustees would be willing to draft security and privacy policies that ensure system dependability across all hardware and software layers. From the root of trust up to the automated decision support system, roles and responsibilities of human and machine trustees would become more visible and auditable by enabling algorithmic explainability and, hopefully, contestability (Vaccaro et al. 2019). We argue that trustworthiness and dependability represent distinct ideas, which need to be treated differently.[4] The distinction between trustworthiness and dependability reflects the difference between writing a policy and applying a policy. We expect trustworthy trustees to write the security policy on behalf of vulnerable trustors by taking into consideration both system owners' and end users' preferences. This distinction is important when it comes to discussing privacy/security–usability tradeoffs. If we think of digital platforms it is easy to see the conflict between platform surveillance capacity and end users' privacy. To ensure that privacy and security policies respond to trustors' needs, trustees need to be competent, honest, and benevolent toward all types of trustors. Extending trustees' benevolence to all trustors of a digital system requires the creation of governance mechanisms promoting ethics-of-care by design, professionalism, and integrity.

Trustworthy trustees writing information security and privacy policies

If we assume that those who have the ability to design and develop the system are the trustees, and that those who use or own the system are the trustors, we may explore their relationship in terms of dependence and vulnerability, to guarantee the respect of a duty of care in the development and application of security/privacy policies and procedures. Trustor-users, who do not design or deploy the system but still use it, tend to be dependent and vulnerable. Dependence derives from limited knowledge and a lack of convenient alternatives. The vulnerability and dependence of digital system end users are often discussed in the computer science literature. Under the famous "Why Johnny can't encrypt" lemma, several studies demonstrate users' reticence to adopt information security measures mostly because of the limited usability of available solutions (Whitten and Tygar 1999; Sheng et al. 2006; Ruoti et al. 2015). These problems affect individual users as well as entire industries, nation-states, and corporations, as pointed out by scholars working in the field of information security economics (Anderson and Moore 2006).

Widespread adoption of privacy-preserving measures is even more challenging. Privacy policies represent a good example of the reason why we claim

that under dependence and vulnerability, transparency is meaningless or even detrimental. Privacy policies are very long, obscure, and seldom read or understood by end users (McDonald and Cranor 2008; Vail, Earp, and Antón 2008). This implies that privacy policies do not help firms keep their privacy promises—which are viewed by consumers as not credible—or increase transparency and market efficiency (Farrell 2012). Despite all the efforts made to increase the readability and usability of these policies (Acquisti, Adjerid, and Brandimarte 2013), they still ineffectively communicate privacy risks and do not contribute to raising information security and privacy awareness.

Because trust is not interpreted as care but as control, corporations (trustees) have no intrinsic motivation or experience no peer pressure to protect their users' (trustors') privacy. Current available measures are designed to leverage data controllers' fear of losing their good reputation. An example of such mechanisms is the data breach notification provision present in the EU General Data Protection Regulation (GDPR), which relies on sanctions and negative publicity to force corporations to improve their information security procedures. Despite this measure being promising, we argue that information transparency is of limited use when the trustors are vulnerable—having no ability to technically engage with the system—yet still depend on the system. This implies that giving trustors more transparency over the decisions of trustees will not serve to increase the latter's trustworthiness.

By acknowledging the vulnerability of trustors, we implicitly admit how difficult it would be for this constituency to effectively negotiate security and privacy policies beneficial to them. An ethic of care, not utilitarianism, should inform and guide decisions taken by trustees on behalf of trustors—with the trustees being the programmers, standardization body members, scientists, and cryptographers, and the trustors being anyone who depends on the ICT system. We argue that the adoption of a vision of trust-as-care would foster the creation of other types of mechanisms. In the remaining part of the chapter, we try to sketch some proposals, after reviewing current mechanisms to establish the trustworthiness of the trustees.

On the authenticity of trustworthy trustees: authentication and authorization

"Whom do you trust?" and "for doing what?" are typical questions in conversations about trust. Are there identity traits or attributes that make someone naturally trustworthy? In the field of information security, the authenticity of one's identity—and, most importantly, the attributes of that identity—are taken as a given (or assumed as authentic) unless we suspect that we are dealing with a malicious entity that is lying about their identity to perform an attack. Authentication is a key element of information security. Through authentication, we assign information disclosure privileges, assess the reliability and integrity of a piece of information, authorize transactions, and

conduct audits. Multifactor authentication, which is required by the National Institute of Standards and Technology (NIST 2017) and compulsory for the Fintech sector in Europe,[5] is increasingly used to ensure proper authentication. Trust anchoring and oracles are other mechanisms widely applied in this domain. While trust anchoring involves the association of information about an object from reliable sources, oracles can be human beings or automated agents. These solutions can only be effective if we ensure the traceability and linkability of digital information with its original source. For instance, the main requirement in designing machine oracles is that the authenticity of the data must be publicly verifiable (van der Laan 2018).

During daily activities, the trustworthiness of another human being and the authenticity of their identity are established through face-to-face interactions. An example of how physical identities mutate into digital identities are *key signing parties*, which are get-togethers of people who use the PGP[6] encryption system. A Public Key Infrastructure (PKI)[7] is an arrangement that binds public keys with respective identities of entities (i.e., people or organizations). "Key signing" refers to the act of digitally signing a public key packet and a user ID packet; the aim is to verify that a given user ID and public key really belong to the entity that appears to own the key; in other words, to verify that the representation of identity in the user ID packet is valid. Usually, this means that the name on the PGP key matches the name on the identification that the person presents to you when asking that you sign their key.

In other words, physical, face-to-face contact is needed to assess the authenticity of one's identity. Bureaucratic systems also envisage analog entry points to establish the trustworthiness of the counterparty and the intermediary and to set up dispute resolution mechanisms (Werbach 2018a). The European eIDAS regulation (EU 2014), for instance, forces people to prove physical identity in front of an authority, which is assumed to be a trustworthy intermediary. The intervention of real humans is also necessary to set up dispute resolution mechanisms. For instance, the dream of blockchain as a disembodied trustless trust solution ended on June 17, 2016, when cryptocurrency worth USD 55 million was siphoned off by an anonymous user who exploited a loophole in the source code of the Ethereum Blockchain platform (Reyes 2019). The operation was legitimate from the perspective of the software, which could not distinguish a customer from a thief (Werbach 2018b). It was also technically irreversible and immutable, which implied that human intervention was needed to create a hard-fork, namely a bifurcation of the blockchain from the moment before the theft happened and a reimbursement to those affected by the illicit operation. Thus, human intervention was required to resolve the dispute triggered by the theft and to shape the history of the two parallel platforms, known as Ethereum and Ethereum Classic, which now exist.

Several authentication procedures exist to establish authenticity, that is, to establish that the being or thing that one is communicating with is

who or what they claim to be. No procedure, however, asks the entity to prove its competence, integrity, and benevolence. Here we argue for the need to establish the trustworthiness of the original source, namely, of the humans building and operating the system, that is, the trustees. We can imagine some sort of "artistic" irreversible signature left by the designer and administrators of the system that certifies their benevolence, competence, and integrity. Authorship mechanisms may help foster peer-review accountability among trustees, show their benevolence, and foster their trustworthiness.

Mechanisms to extend the roots of trust

Along the course of this chapter, we have rejected the trust-as-control paradigm and adopted a vision of trust as care in order to ask questions on how to distinguish trustworthy trustees from untrustworthy ones and how to build dependability and trustworthiness from the root of trust up to the interface. A trust-as-care vision of information security would expand the root of trust from the technical layer to the human component by reinforcing peer-review mechanisms among trustees who are designers and system administrators. New frameworks would see technical authentication mechanisms complemented by governance mechanisms designed to inscribe competence, honesty, and benevolence into the identities of the human trustees, who would guarantee the dependability of the system and the respect of policies. Technologists (trustees) need to unite in an epistemic community of practice informed by the highest ethical and professional standards to be able to generate the knowledge needed to produce next-generation trustworthy technology, so important especially in the case of AI-driven critical infrastructures. We argue that emerging technologies such as quantum computing demand the creation of new spaces of critical and constructive dialogue, enabling trustees to learn about trustors' needs.

Trustees' trustworthiness is generated by trustees' competence, which demands the leveraging of expert knowledge; integrity, which requires training and application of ethical codes of conduct; and benevolence, which demands that trustees learn about trustors' needs and openly discuss their corporate mission, business rationale, and technical and organizational methods with the needs of clients or users in mind. If the trustee has a duty of care toward the trustor, the respect of this duty of care should be guaranteed by other trustees within collegial bodies that underwrite codes of conduct and codes of principles, and through mentoring, training, and education (ECA 2019). Professionalism, knowledge generation, and peer review should be guaranteed and fostered through collegial bodies supporting the activities of, and decisions taken by, the trustees. Examples of collegial bodies are standardization authorities,[8] professional associations and forums, and the scholarly and scientific community.

Mechanisms to reinforce collaboration and mutual accountability among trustees can protect society against the risk of technological determinism and herding behavior in policy and R&D investment decisions. Technological determinism and herding behavior may lead policymakers to ignore certain policy stages, such as problem structuring and definition, as noticed by Veale (2019), or certain problems (assessing the usefulness of computing in any given context), while spending time and effort on issues related to economic competitiveness (e.g., increasing the availability or intensity of European AI). As competition may prevent beneficial exchanges of knowledge and expertise, the creation of nonmonetary social markets for auditability and accountability could facilitate the exchange of confidential information among trustees working in the security and digital surveillance domains. Of course, soft coordination mechanisms like these need to be anchored in other types of strong enforcement procedures in order to ensure prompt conflict resolution and intervention. Ben Wagner (2019, 89–99) suggests providing "a mechanism for external independent (not necessarily public) oversight" and "a clear statement on the relationship between the commitments made and existing legal or regulatory frameworks, in particular on what happens when the two are in conflict."

To foster a vision of security as a public good, new legal instruments and governance methods to facilitate security audits (see e.g., Sanchez-Gomez et al. 2018 in the domain of cloud storage) should be envisioned in order to facilitate the discovery of system vulnerabilities and other privacy and security issues. In the domain of machine and deep learning, "blind trust" mechanisms could be devised to enable algorithm auditing and the sharing of training datasets. Imagine a scenario in which the management of a company developing a predictive algorithm wants to understand the system's privacy and reidentification risks. Data and code could be anonymously sent to a Digital Blind Trust (DBT) with instructions on the tasks to be performed. The Trust would open a bid and assign the task to an anonymous research team, after controlling for potential conflicts of interest. The anonymous team would perform the analysis. Results would be sent to the client for rebuttal. The revised version of the study would be published on the trusted network and made public according to confidentiality agreements, which would balance individual and collective interests. This and similar types of systems could be designed to enable peer pressure and peer review among trustees.

The considerations and proposals made here are not meant to undermine the role of trustors in fostering the trust relationship. The High-Level Expert Group on Artificial Intelligence (AI-HLEG 2019b, 12), in its second report on "Policy and investment recommendations for trustworthy Artificial Intelligence," suggests

> [i]ntroduc[ing] a mandatory self-identification of AI systems … [Given that] there is a reasonable likelihood that end users could be led to believe

> that they are interacting with a human, deployers of AI systems should be attributed a general responsibility to disclose that in reality the system is non-human.

We want to clarify that a focus on the trustworthiness of the trustees does not preclude "[p]romoting the ability of individuals and society as a whole to understand and reflect critically in the information society," which is an important recommendation made by the Data Ethics Commission for the Federal Government's Strategy on Artificial Intelligence (DEK 2018, 1). If trustees have a duty of care toward trustors, they have an obligation to maintain a permanent dialogue with the trustors, understand their needs and demands, and increase their awareness and literacy. Furthermore, we suggest that trustors should retain some degree of skepticism in the form of *parrhesia* (Foucault 1983) to denounce untrustworthy trustees and wrongdoing. Trustors could also be willing to play *parrhesiastic games* to help trustees demonstrate their ability to listen and calibrate their actions in their best interest. Trustees should review each other's actions and decisions to help enhance their knowledge of how to better care for the trustors.

Conclusion

The problem at the core of this article is how we can ensure that we trust the trustworthy and distrust the untrustworthy when we are confronted with disembodiment and automated beings to which we cannot direct our gaze. Information technology introduces a conception of trust as dependability, reliability, or credibility compatible with visions of trust-as-control rooted in the rationalistic instrumental paradigm. However, as noted by Olav Lysne (2018, 18), "we should not make Hardin's kind of trust a basis for our security concerns about equipment in a country's critical infrastructure." While the necessity of shedding light on economic incentives and psychological biases that shape security policy decisions has been acknowledged (Anderson and Moore 2009, 2006), the role that ethics and moral principles should play in defining next-generation security policies has received little attention.

In this chapter we have challenged the underlying assumption, present in the rationalistic instrumental visions of trust, that the trustor enjoys the freedom not to trust the trustee. By presenting the caring-one and vulnerable-other dyad as an alternative to the utilitarian trustor–trustee dyad, we have argued for the need to embed an ethic of care, and not simply a logic of control, into the trustors. In the presence of dependence and vulnerability we argue that the logic of control, based on transparency, sanctions, and incentives, is useless, even detrimental. The issue then becomes how to foster the trustee's trustworthiness, beyond the trust-as-dependability currently pursued and enacted in the information security domain. Trustworthiness concerns the

confidence of the trustor that the trustee has attributes, such as competence or integrity, that serve the trustee in a beneficial manner (Gabarro 2014). We trust our doctor, or the pilot of the plane, to do their job in a professional manner; in other words, we expect professionals to perform their duties—that is, to follow certain established social norms by showing high levels of competence, integrity, and benevolence.

The emphasis on trustworthiness is meant to reconcile functional, privacy, and security requirements with multiparty-negotiated policies and foreground the pivotal role of coders' and operators' competence, integrity, and benevolence. We acknowledge the continuity between the trust-as-control and the trust-as-care models, and simply clarify that in the presence of highly vulnerable trustors a logic of trust-as-care should be preferred over a logic of trust-as-control, which is better suited for scenarios featuring low dependence and low vulnerability. We argue that in a scenario where the trustor has enough autonomy to exercise a certain degree of control over the trustee, all they need is the trustee's dependability. In the opposite case, when the trustor is highly vulnerable and depends on the trustee, with limited or no control or exit strategy, the trustee needs to demonstrate trustworthiness, that is, the ability to take care of the trustor in the absence of control, but in the presence of an ethic of care.

If we are truly moving toward a future in which computer code is the new law, the only chance we have to program sensible machines is to train a new generation of culturally, morally, and socially sophisticated coders able to confront the challenge and embrace the normativity and performativity of the system they are designing. From a security engineering perspective, the question "is the system trusted?" is underdefined unless we answer other related questions, such as "By whom? For which attributes? Against what adversary?" As in everyday reality, the question, "Do you trust them?" should be qualified with "trust them to do what?" to take into consideration the ability of the trustees to deliver on their promise of care.

Some commentators claim that cryptography has a role to play in keeping power in check,[9] whether in protecting those resisting authoritarian regimes or in bringing more transparency to democratic ones (Rogaway 2015). We hope that our reflections will help inspire new generations of coders (cryptographers and lawmakers) willing to cooperate in the name of human flourishing and security as a public good. We also hope that these coders will be inspired by new expressions of moral philosophy, different from those which replicate "uncaring forms of justice and unjust forms of care" (Clement 2018, 2) that amplify unfairness through the denial of basic human conditions, such as dependence and vulnerability and the need of care.[10] We hope that a vision of trust based on a philosophy of care could help us better reflect on the relationship between transparency and digital surveillance in new policy and technology terms.

Acknowledgments

This work was partially funded by the "TRESCA—Trustworthy, Reliable, and Engaging Scientific Communication Approaches" project, funded by the European Union's Horizon 2020 Research and Innovation Program under grant agreement no. 872855, and by the project "CYNAMON—Cybersecurity, Network Analysis, and Monitoring for the Next Generation Internet," sponsored by "Programas de Actividades de I+D entre grupos de investigación de la Comunidad de Madrid en tecnologías 2018" (P2018/TCS-4566), cofinanced with FSE and FEDER EU funds.

Notes

1 Dependability represents "the ability to deliver service that can justifiably be trusted," while resilience is "the persistence of service delivery that can justifiably be trusted, when facing changes" (Laprie 2008, 8).
2 Typical examples are: denial-of-service attacks, which limit or jeopardize data or system availability; man-in-the-middle attacks, which disrupt the confidentiality of communications; zero-day or SQL-injection attacks, which disrupt system integrity through vulnerability exploitation or code injection; and adversarial attacks on neural networks (deep learning) that compromise data integrity and system performance.
3 It is worth noticing that "[e]ach virtual machine presumes the correctness (integrity) of whatever virtual or real machines underlie its own operation" (Arbaugh et al. 1997, 1). In other words, a technical system is made of many interdependent layers; the security of each layer is dependent on assumptions made about the functioning of previous layers.
4 Of course, we are adopting a reductionist logic to produce binary categories and we acknowledge that reality is the gray zone which lies in-between these two extreme scenarios and that the two ideas need to coexist and complement each other.
5 Payment services (PSD 2)—Directive (EU) 2015/2366, URL: https://ec.europa.eu/info/law/payment-services-psd-2-directive-eu-2015-2366_en. NIST Special Publication 800-63B "Digital Identity Guidelines," URL: https://pages.nist.gov/800-63-3/sp800-63b.html
6 PGP stands for "pretty good privacy (data encryption)." Public key cryptography infrastructure (PKI) has two main implementations. One is done using certificates and certificate authorities (CAs) and is described in the X.509 standard. It is best suited for structured organizational hierarchies with an implicitly trusted authority that vouches for all issued certificates. It is the standard that is behind SSL/TLS and S/MIME email encryption. However, there is also another widely used standard for PKI, which was developed with the explicit intention of avoiding centralized certification authorities, and instead relies on trust relationships built between regular users. It was first implemented in the original PGP software back in 1991 and, since then, has developed into a robust open standard, known as OpenPGP (openpgp.org) for email encryption.
7 PKI is a set of protocols, standards, and procedures to manage public key encryption and digital certificates (Adams and Lloyd 1999).

8 E.g., ISO International Standards; the National Institute of Standards and Technology (NIST), part of the US Department of Commerce; "Bundesamt für Sicherheit in der Informationstechnik" (BSI).
9 For instance, Tor (www.torproject.org) has found considerable success as a censorship-circumvention tool.
10 Of course, engaging with ideas of care and control leads us to face two famous stereotypical constructions: womanhood (Clement 2018) and blackness (Mbembe 2017).

References

Acquisti, Alessandro, Idris Adjerid, and Laura Brandimarte. 2013. "Gone in 15 Seconds: The Limits of Privacy Transparency and Control." *IEEE Security & Privacy* 11(4): 72–4.

Adams, Carlisle, and Steve Lloyd. 1999. *Understanding Public-Key Infrastructure: Concepts, Standards, and Deployment Considerations*. Indianapolis: Sams Publishing.

AI-HLEG. 2019a. *Ethics Guidelines for Trustworthy AI.* High-Level Expert Group on Artificial Intelligence, European Commission. April 8, https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai.

AI-HLEG. 2019b. *Policy and Investment Recommendations for Trustworthy Artificial Intelligence.* High-Level Expert Group on Artificial Intelligence, European Commission, https://ec.europa.eu/digital-single-market/en/news/policy-and-investment-recommendations-trustworthy-artificial-intelligence.

Anderson, Ross. 2008. *Security Engineering: A Guide to Building Dependable Distributed Systems*. Indianapolis: Wiley.

Anderson, Ross, and Tyler Moore. 2006. "The Economics of Information Security." *Science* 314(5799): 610–3.

Anderson, Ross, and Tyler Moore. 2009. "Information Security: Where Computer Science, Economics and Psychology Meet." *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences* 367(1898): 2717–27.

Arbaugh, William A., Angelos D. Keromytis, David J. Farber, and Jonathan M. Smith. 1997. "Automated Recovery in a Secure Bootstrap Process." *University of Pennsylvania Department of Computer and Information Science Technical Report No. MS-CIS-97–13*.

Artz, Donovan, and Yolanda Gil. 2007. "A Survey of Trust in Computer Science and the Semantic Web." *Web Semantics: Science, Services and Agents on the World Wide Web* 5(2): 58–71.

Avizienis, Algirdas, Jean-Claude Laprie, and Brian Randell. 2001. Fundamental Concepts of Dependability. *UCLA CSD Report no. 010028; LAAS Report No. 01–145; Newcastle University Report No. CS-TR-739, 2001*, https://pld.ttu.ee/IAF0530/16/avi1.pdf.

Axelrod, Robert. 1997. *The Complexity of Cooperation: Agent-Based Models of Competition and Collaboration*. Vol. 3. Princeton: Princeton University Press.

Baier, Annette. 1986. "Trust and Antitrust." *Ethics* 96(2): 231–60.

Berg, Joyce, John Dickhaut, and Kevin McCabe. 1995. "Trust, Reciprocity, and Social History." *Games and Economic Behavior* 10(1): 122–42.

Clement, Grace. 2018. *Care, Autonomy, and Justice: Feminism and the Ethic of Care*. New York: Routledge.

Colquitt, Jason A., Brent A. Scott, and Jeffery A. LePine. 2007. "Trust, Trustworthiness, and Trust Propensity: A Meta-Analytic Test of their Unique Relationships with Risk Taking and Job Performance." *Journal of Applied Psychology* 92(4): 909–27.

Danezis, George. 2014. "Trust as a Methodological Tool in Security Engineering." In *Trust, Computing and Society*, edited by Richard H. R. Harper, 68–91. Cambridge: Cambridge University Press.

De Filippi, Primavera, and Benjamin Loveluck. 2016. "The Invisible Politics of Bitcoin: Governance Crisis of a Decentralized Infrastructure." *Internet Policy Review* 5(3): 1–28.

Degli Esposti, Sara, Kirstie Ball, and Sally Dibb. 2021. "What's In It For Us? Benevolence, National Security, and Digital Surveillance." *Public Administration Review*: 1–12, doi.org/10.1111/puar.13362.

DEK. 2018. *Recommendations of the Data Ethics Commission for the Federal Government's Strategy on Artificial Intelligence.* Data Ethics Commission for the Federal Government's Strategy on Artificial Intelligence, www.bmjv.de/SharedDocs/Downloads/DE/Ministerium/ForschungUndWissenschaft/DEK_Empfehlungen_englisch.html?nn=11678512.

ECA. 2019. *Challenges to Effective EU Cybersecurity Policy: Briefing Paper.* European Court of Auditors, European Union, www.eca.europa.eu/Lists/ECADocuments/BRP_CYBERSECURITY/BRP_CYBERSECURITY_EN.pdf.

Elster, Jon. 2007. *Explaining Social Behavior. More Nuts and Bolts for the Social Sciences*. Cambridge: Cambridge University Press.

EU. 2014. "Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on Electronic Identification and Trust Services for Electronic Transactions in the Internal Market and Repealing Directive 1999/93/EC." *Official Journal of the European Union*, https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32014R0910.

Farrell, Joseph. 2012. "Can Privacy Be Just Another Good." *Journal on Telecommunications and High Technology Law* 10: 251–64.

Fetchenhauer, Detlef, David Dunning, and Thomas Shlösser. 2017. "The Mysteries of Trust. Trusting Too Little and Too Much at the Same Time." In *Trust in Social Dilemmas*, edited by Paul A. M. Van Lange, Bettina Rockenbach, and Toshio Yamagishi. Oxford: Oxford University Press.

Fogg, BJ, and Hsiang Tseng. 1999. "The Elements of Computer Credibility." Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, Pittsburgh, PA: Association for Computing Machinery (ACM).

Foucault, Michel. 1983. "Discourse and Truth: The Problematization of Parrhesia." Six Lectures Given at the University of California at Berkeley, Berkeley, October–November, https://foucault.info/parrhesia/.

Fournier, Valérie. 1999. "The Appeal to 'Professionalism' as a Disciplinary Mechanism." *The Sociological Review* 47(2): 280–307.

Gabarro, John J. 2014. "The Development of Working Relationships." In *Intellectual Teamwork: Social and Technological Foundations of Cooperative Work*, edited by Jolene Galegher, Robert E. Kraut, and Carmen Egido, 79–110. New York: Psychology Press.

Greene, Sari. 2014. *Security Program and Policies: Principles and Practices*. 2nd Edition. Indianapolis, IN: Pearson IT Certification.

Haas, Peter M. 1992. "Introduction: Epistemic Communities and International Policy Coordination." *International Organization* 46(1): 1–35.

Hardin, Russell. 2002. *Trust and Trustworthiness*. *The Russell Sage Foundation Series on Trust*. New York: Russell Sage Foundation Publications.

Hechter, Michael. 1992. "The Insufficiency of Game Theory for the Resolution of Real-World Collective Action Problems." *Rationality and Society* 4(1): 33–40.

Henrich, Joseph Patrick, Robert Boyd, Samuel Bowles, Ernst Fehr, Colin Camerer, and Herbert Gintis. 2004. *Foundations of Human Sociality: Economic Experiments and Ethnographic Evidence from Fifteen Small-Scale Societies*. Oxford: Oxford University Press on Demand.

Hosmer, LaRue Tone. 1995. "Trust: The Connecting Link Between Organizational Theory and Philosophical Ethics." *Academy of Management Review* 20(2): 379–403.

Hurwitz, Justin. 2012. "Trust and Online Interaction." *University of Pennsylvania Law Review* 161: 1579–622.

Jones, Stephen L., and Priti Pradhan Shah. 2016. "Diagnosing the Locus of Trust: A Temporal Perspective for Trustor, Trustee, and Dyadic Influences on Perceived Trustworthiness." *Journal of Applied Psychology* 101(3): 392–414.

Kramer, Roderick M. 2009. "Rethinking Trust." *Harvard Business Review*, June 2009, https://hbr.org/2009/06/rethinking-trust.

Kultgen, John H. 1988. *Ethics and Professionalism*. Philadelphia: University of Pennsylvania Press.

Laprie, Jean-Claude. 2008. "From Dependability to Resilience." 38th Annual IEEE/IFIP International Conference on Dependable Systems and Networks, Anchorage, USA.

Levi, Margaret, and Laura Stoker. 2000. "Political Trust and Trustworthiness." *Annual Review of Political Science* 3(1): 475–507.

Lysne, Olav. 2018. *The Huawei and Snowden Questions: Can Electronic Equipment from Untrusted Vendors Be Verified? Can an Untrusted Vendor Build Trust into Electronic Equipment?* Vol. 4. Cham, Switzerland: Springer.

Mayer, Roger C., James H. Davis, and F. David Schoorman. 1995. "An Integrative Model of Organizational Trust." *Academy of Management Review* 20(3): 709–34.

Mbembe, Achille. 2017. *Critique of Black Reason.* Translated and with an introduction by Laurent Dubois. Durham, NC: Duke University Press.

McDonald, Aleecia M., and Lorrie Faith Cranor. 2008. "The Cost of Reading Privacy Policies." *ISJLP* 4: 543–68.

McGeer, Victoria, and Philip Pettit. 2017. "The Empowering Theory of Trust." In *The Philosophy of Trust*, edited by Paul Faulkner and Thomas Simpson, 14–34. Oxford: Oxford University Press.

Mitnick, Kevin D., and William L. Simon. 2011. *The Art of Deception: Controlling the Human Element of Security*. Indianapolis: John Wiley.

Nakamoto, Satoshi. 2008. "Bitcoin: A Peer-to-Peer Electronic Cash System." Bitcoin Whitepaper, Satoshi Nakamoto Institute.

Nicol, David M., William H. Sanders, and Kishor S. Trivedi. 2004. "Model-Based Evaluation: From Dependability to Security." *IEEE Transactions on dependable and secure computing* 1(1): 48–65.

Nissenbaum, Helen. 2004. "Will Security Enhance Trust Online, or Supplant It?" In *Trust and Distrust Within Organizations: Emerging Perspectives, Enduring Questions*, edited by R. Kramer and K. Cook, 155–88. New York: Russell Sage Publications.

NIST. 2017. *Digital Identity Guidelines: Authentication and Lifecycle Management*. Gaithersburg, MD: National Institute of Standards and Technology (NIST), U.S. Department of Commerce.

O'Neill, Onora. 2017. "Trust, Trustworthiness and Transparency. Output of a Breakfast Briefing held on 24th January 2017." www.britac.ac.uk/sites/default/files/Trust%2C%20Trustworthiness%20And%20Transparency%20briefing%20note%2024%20January%202017.pdf.

Pettit, Philip. 2002. *Rules, Reasons, and Norms*. Oxford: Oxford University Press.

Reyes, Carla L. 2019. "If Rockefeller Were a Coder." *George Washington Law Review* 87: 373–429.

Rogaway, Phillip. 2015. "The Moral Character of Cryptographic Work." 2015 IACR Distinguished Lecture Given at Asiacrypt 2015 on December 2, 2015, in Auckland, New Zealand.

Ruoti, Scott, Jeff Andersen, Daniel Zappala, and Kent Seamons. 2015. "Why Johnny Still, Still Can't Encrypt: Evaluating the Usability of a Modern PGP Client." arXiv preprint arXiv:1510.08555.

Sanchez-Gomez, Alejandro, Jesus Diaz, Luis Hernandez-Encinas, and David Arroyo. 2018. "Review of the Main Security Threats and Challenges in Free-Access Public Cloud Storage Servers." In *Computer and Network Security Essentials*, edited by Kevin Daimi, 263–81, 263–81. Cham, Switzerland: Springer.

Sheng, Steve, Levi Broderick, Colleen Alison Koranda, and Jeremy J. Hyland. 2006. "Why Johnny Still Can't Encrypt: Evaluating the Usability of Email Encryption Software." Symposium on Usable Privacy and Security, Pittsburgh, PA, July 12–14.

Sicari, Sabrina, Alessandra Rizzardi, Luigi Alfredo Grieco, and Alberto Coen-Porisini. 2015. "Security, Privacy and Trust in Internet of Things: The Road Ahead." *Computer Networks* 76: 146–64.

Taylor, Shelley E. 2014. *The Tending Instinct: Women, Men, and the Biology of Nurturing*. New York: Times Books.

Vaccaro, Kristen, Karrie Karahalios, Deirdre K. Mulligan, Daniel Kluttz, and Tad Hirsch. 2019. "Contestability in Algorithmic Systems." Conference Companion Publication of the 2019 on Computer Supported Cooperative Work and Social Computing, Austin, TX, USA.

Vail, Matthew W., Julia B. Earp, and Annie L. Antón. 2008. "An Empirical Study of Consumer Perceptions and Comprehension of Web Site Privacy Policies." *IEEE Transactions on Engineering Management* 55(3): 442–54.

van der Laan, Bjorn. 2018. "Publicly Verifiable Authenticity of Data from Multiple External Sources for Smart Contracts Using Aggregate Signatures." Master of Science in Computer Science, Department of Intelligent Systems, Faculty of Electrical Engineering, Mathematics & Computer Science, Delft University of Technology.

Van Lange, Paul A. M., Bettina Rockenbach, and Toshio Yamagishi. 2017. *Trust in Social Dilemmas*. Oxford: Oxford University Press.

Veale, Michael. 2019. "A Critical Take on the Policy Recommendations of the EU High-Level Expert Group on Artificial Intelligence." *European Journal of Risk Regulation*: 1–10, doi.org/10.1017/err.2019.65.

Wagner, Ben. 2019. "Ethics as an Escape from Regulation: From Ethics-Washing to Ethics-Shopping." In *Being Profiled: Cogitas Ergo Sum*, edited by Irina

Baraliuc, Emre Bayamlıoğlu, Mireille Hildebrandt, and Liisa Janssens, 84–90. Amsterdam: Amsterdam University Press.

Werbach, Kevin. 2018a. *The Blockchain and the New Architecture of Trust*. Cambridge: MIT Press.

Werbach, Kevin. 2018b. "Trust, but Verify: Why the Blockchain Needs the Law." *Berkeley Technology Law Journal* 33: 487–550.

Whitten, Alma, and J. Doug Tygar. 1999. "Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0." In *Security and Usability: Designing Secure Systems that People Can Use*, edited by Lorrie Faith Cranor and Simson Garfinkel, 679–702. Boston: O'Reilly.

Wiener, Norbert. 1988. *The Human Use of Human Beings: Cybernetics and Society*. New York: Da Capo Press.

Chapter 12

Why a militantly democratic lack of trust in state surveillance can enable better and more democratic security

Miguelángel Verde Garrido

Introduction

Contemporary societies are characterized by a global culture of surveillance, that is, structured by multiple social, economic, and political policies and practices that deploy surveillance to achieve various goals (Verde Garrido 2015). Surveillance can be understood as "the operations and experiences of gathering and analysing personal data for influence, entitlement, and management," mostly performed by states and corporations, but "may also be carried out by people in everyday life" (Lyon 2018, 6). Additionally, there exists a politically and economically "neutral watching or sensing," termed "veillance," which eschews social hierarchies and asymmetric relations of power and knowledge (Verde Garrido 2015, 163–4). Considering these different modalities of collection, analysis, and application of physical, social, and digital data is crucial to understanding contemporary notions and practices of privacy, security, and trust (Verde Garrido 2015, 164). When Edward Snowden's revelations were reported, it became evident that "global surveillance is not only confined to intelligence agencies' deployment of surveillance technologies, but extends also to the very cultural and economic characteristics of contemporary society" (Verde Garrido 2015, 155). Global public outrage followed the realization that mass surveillance infringed on the right to privacy as well as other vital human rights (Verde Garrido 2015, 164). In order to contest these violations and abuses, civil societies have expanded their counter-surveillance strategies and practices, strengthened their political agency with a nascent digital agency, and furthered demands for the rule of law and democratic oversight (Verde Garrido 2015, 164–5). This chapter focuses on the nature and particulars of democratic oversight of surveillance policies and practices, questioning the extent to which these require trust and transparency to be most effective. It is important to remember that "the towering institutions and processes of high technology and global government […] are not relentless and invincible" and that "ordinary people, often acting in concert" can contribute constructively to the "reimagination and shaping" of contemporary technological policies and practices (Lyon 2018, 147). Bearing

DOI: 10.4324/9781003120827-16

that in mind, the first section explores trust and transparency generally and in relation to surveillance, clarifying the nature of intelligent accountability. The second section explains the manner in which, counterintuitively, a lack of trust informs several democratic institutions as well as the governmental, legal, and juridical notion of militant democracy. The notion of militant democracy advances the idea that a liberal democracy can defend its constitutional order from the threat of authoritarian political movements and that it can do so through enacting political and legal measures that fulfill three criteria: legitimacy, legality, and necessity. This section proposes that a militantly democratic approach within civil society can further ensure that oversight of surveillance is effective, democratic, and upholds civil liberties and human rights. In order to illustrate this approach, the third section considers specific instances of surveillance in various countries: Germany, Poland, and the United States, which share the political encroachment of far-right populism, although to varying degrees. This section critically analyzes specific instances of surveillance policies and practices in these countries and notes how these are ideologized to varying extents and fail to fulfill the three criteria promoted by a militantly democratic oversight. This chapter ends by offering some conclusions and recommendations on ensuring a democratic oversight of surveillance policies and practices.

On the relation of trust and transparency to oversight of surveillance

The Snowden revelations provoked a global debate on the nature and implications of surveillance for state—as well as corporate—intelligence functions. There are questions about the levels of privacy intrusion, the "accountability" of intelligence and security functions, the "efficiency of bulk surveillance practices and their compatibility with fundamental rights," and the manner in which "surveillance-intensive methods" impact the social fabric of democratic societies (Ball et al. 2019, 3; Wetzling and Vieth 2018, 10). The ongoing debate has not changed that "all major democracies allow their national intelligence services to intercept communications data in enormous quantities" or that court rulings admonish them "for flaws or shortcomings" in an oversight regime that must become "more rigorous and effective" (Wetzling and Vieth 2018, 10). Understanding that democratic oversight acts as an effective bulwark against "the erosion of fundamental rights should a government be infested with the illiberal virus that is currently rampant" proves crucial (Wetzling and Vieth 2018, 6). Because "temptations to abuse privileges such as government secrecy are omnipresent," it is important to remember that "democratic intelligence governance cannot be taken for granted" and "the legitimacy of intelligence action must constantly be earned" (Wetzling and Vieth 2018, 11–12). Therefore, democratic oversight of state—as well as corporate—policies and practices of surveillance should

consider dynamics of trust and trustworthiness and learn from democratic institutions and measures built upon a constructive lack of trust.

Trust can be understood as the belief and confidence on the part of a person or party (trustor) that another person or party (trustee) will reliably do what they have stated. There is never a complete guarantee that people or parties will be trustworthy, so every interaction requires granting trust to a certain extent and involves a risk that others prove that the granted trust was misplaced. The "most systematic evidence" to determine whether contemporary society is experiencing a "crisis of trust" comes from public opinion polls and similar academic research, but these surveys fail to realize their own ambiguities (O'Neill 2002, 3–4). First, surveys do not recognize that people "seek to place trust in a differentiated way" and do not grant "every instance of a certain type of official or […] person" the same level of trust. Second, surveys seldom ask respondents about specifics. Questions about trust in this or that type of person should be followed by: "To do what?" (O'Neill 2013). Consequently, the status of trust in contemporary societies is better illustrated by the fact that "we still constantly place trust in many of the institutions and professions that we profess to not to trust" (O'Neill 2002, 4).

Prompted by worries about what states and corporations may do with their data, more and more citizens and consumers have "sought ways to avoid observation by specific people, organizations or the government." These concerns come from "a lack of confidence in the security of everyday communications channels and a lack of trust in all kinds of organizations to protect their data" (Lyon 2018, 67–8). The Snowden revelations showed the limitations of data protection legislation and the reduction of corporate sovereignty over data and "profoundly undermined the trust and confidence" that private lives, human rights, and civil liberties are respected (Bigo et al. 2013, 1–4). Consequently, citizens and consumers wonder whether they should "ever trust that their information is safe on the Web." While the "main byproduct" of digital technologies—data—has great value for "law enforcement, industry, advertising, science, and other fields," it is even more valuable for its owners, representing the "center of trust" of their "interaction with technology." Since individuals must trust their interlocutors to provide them with data, government or corporate mishandling of data implies to "completely mishandle the trust." Ultimately, "the lack of clarity and consensus on rules for government access to data," added to the "constant stream of data breaches, intrusions into government systems, and attacks on service providers," has led civil society to experience "fear and paranoia" and lose "trust in technology" (Jordan 2015). Solely corporate surveillance policies and practices have also impacted citizen and consumer trust significantly. Internet giants such as Facebook and Google, following a business model and logics of data extraction and accumulation termed "surveillance capitalism," undermine relationships of trust by eschewing "the mutual dependencies and reciprocities" that hold other kinds of corporations accountable. Thriving on

the "public's ignorance" of their imperatives and operations and offering minimal "meaningful options for privacy self-management," these corporations establish "unprecedented concentrations of information power," entrench new structural asymmetries of knowledge, power, and trust, and obfuscate themselves from transparency (Zuboff 2015, 83, 85–6).

Citizens and consumers have become aware that states and corporations deploy mass surveillance and that they employ mendacities and chicaneries in order to do so unnoticed. Lack of trust has grown worldwide as a "reasonable response to growing untrustworthiness" (O'Neill 2002, 12). Accordingly, states and corporations must provide citizens and consumers not only with information that claims they are trustworthy but also "the means to judge that information" independently as well (O'Neill 2002, 17). Transparency on its own does not allow others to fully determine trustworthiness or whether to grant trust and rarely means more than that certain information is being made publicly available. More effective is ensuring that the information in question is intelligible as well as assessable. Oversight of surveillance that not only demands information on specific practices but that also informs about the goals of the surveillance in question can be understood as establishing "intelligent accountability" (O'Neill 2017).

Complete openness and transparency have contributed very little to building or regaining public trust. Quite often, "trust seemingly has receded as transparency has advanced." This is not because transparency "destroys secrecy," but rather because restoring trust requires those who are untrustworthy to "reduce deception and lies rather than secrecy" (O'Neill 2002, 18). Most important for reducing asymmetries of power and knowledge resulting from asymmetric kinds of transparency are "legal measures to prohibit certain kinds of surveillance and to impose penalties on those whose watching transgresses acceptable transparency" (Lyon 2018, 162). There is no benefit in granting trust blindly: "well-directed trust and […] well-directed mistrust" are desirable because "we want mistrust in the untrustworthy […] and trust in the trustworthy" (O'Neill 2017). States and corporations who deceive citizens and consumers are untrustworthy and, hence, do not deserve trust. For these various reasons, addressing states and corporations with a lack of trust can, counterintuitively, prove to be a constructive approach.

A constructive lack of trust and a militantly democratic approach within civil society

The previous section explained that trust is granted without complete guarantees, relying on ostensible trustworthiness. Awareness of the nature and extent of surveillance has led citizens and consumers to lose much trust in states and corporations. This lack of trust comes not only from state and corporate failure to fulfill promises about how surveillance is deployed but also from their obscuring facts about why: namely, to establish new asymmetries

of power and knowledge. Ensuring transparency is neither sufficient for trust to be built or recovered nor is it desirable unless there is intelligent accountability: clearer explanations and more opportunities to contest and decide which goals are desirable in relation to surveillance policies and practices. This section will explain why a lack of trust informs certain democratic principles and institutions, how it can be embodied by a militantly democratic civil society, and why it can prove to be constructive for oversight of surveillance.

Liberal democracies have formal institutions built upon a constructive lack of trust. Examples include the separation of powers, secret ballots, and whistleblowing. The separation of powers implies a lack of trust because it recognizes that dividing government into branches, separate and independent, is crucial to avoiding an unchecked concentration of power. Secret ballots, which exist in a number of voting systems, also imply a lack of trust inasmuch as they acknowledge that mechanisms to avoid excessive influences are required. Institutional whistleblowing implies a lack of trust since it accepts that wrongdoings within states—as well as corporations—may be intentionally obscured to avoid consequences. Therefore, protections are established to shield whistleblowers from suffering retaliatory measures, and protocols are designed to investigate and right these wrongdoings. Civil societies can learn to constructively apply a lack of trust to oversight of security and intelligence functions, even if certain levels of secrecy are obligatory and limited transparency is the norm.

Contrary to arguments that security and privacy are incompatible, efforts to simultaneously ensure privacy and security can be valuable in terms of "public policy" since addressing the intrusiveness of certain instances of security and surveillance can maximize "security benefits and privacy protections" (Ball et al. 2019, 14). "Good oversight is good security" because it "pushes governments to be as effective as possible in allocating their resources and selecting their targets" (Wetzling and Vieth 2018, 87). Furthermore, because of the contemporary drift toward authoritarianism within liberal democracies (Zeid 2018; Human Rights Watch 2018; Amnesty International 2018; Freedom House 2018), a militantly democratic approach to oversight is crucial because it can help ensure better and more discerning transparency and technical literacy, hold states intelligently accountable for their relations with corporations and vice versa (Jordan 2015; Schneier 2015), and enact modernized legislation addressing the complexities of domestic as well as global surveillance.

Karl Loewenstein developed the notion of militant democracy (i.e., *streitbare* or *wehrhafte*, defensive, *Demokratie*) during the summer of 1937, shortly before the totalitarianisms of fascism and communism violently set off World War II. He addressed with grave concern why numerous states were experiencing authoritarian drifts, and several others had already fully devolved into authoritarianism (Loewenstein 1937a, 1937b). Loewenstein proposed that liberal democracies should "become militant" in defense of

their constitutional values: that is, these states needed to enact and implement constitutional political and legislative measures restricting the manners in which authoritarian political movements weaponized democratic freedoms, rights, and institutions in order to consolidate power and ultimately suspend them (Loewenstein 1937a, 422–3, 438–9). Militant democracy is a decisive response to the proven untrustworthiness of authoritarian politics.

Loewenstein differentiated constitutional governments from authoritarian ones, noting that the former signified the rule of law, rational and calculable administration, and the protection of private law and fundamental rights. The latter, in contrast, replaced the rule of law with "legalized opportunism," merged private law into public law, and collapsed fundamental rights and the rule of law, their interest being to achieve "unchallengeable command." Because "no government can rely only on force or violence," authoritarianism relied strongly on raw "emotionalism," especially nationalist fervor and a strategic combination of intimidation, "terrorization," and coercion (Loewenstein 1937a, 417–8). Constitutional governments can be understood as liberal democracies, upholding fundamental rights such as the freedom of speech and the press or the freedom to hold public office, which are not only liberties and freedoms but also civil and political rights (Altman 2017). While constitutional and authoritarian governments contrast starkly, there is also a certain kind of government considered mostly democratic, although a "new type of 'authoritarian' or 'disciplined' democracy" (Loewenstein 1937b, 644). Nowadays, such a "hybrid" regime, neither fully democratic nor fully autocratic, is termed an "anocracy." These regimes may uphold a number of freedoms while constraining others and may limit electoral competition as well as prevent political accountability in order to maintain power (Colomer et al. 2016, 19–20).

Authoritarianism adapted perfectly to democracy and its tolerance for other competing political ideologies. Employing novel "technical wonders" and democratic institutions, authoritarian regimes spread discourses that inflamed "emotionalism in its crudest and its most refined forms" among the masses, set different groups against each other, and discredited "the democratic order" as "unworkable." Liberal democracies responded slowly, concerned that restricting authoritarian "use of democratic institutions" weakened their legality. Loewenstein proposed that constitutional governments wishing to uphold their own values needed to act upon their lack of trust in the outward conformance to "the principles of legality and free play of public opinion" of authoritarian political movements and confront their dangerous political techniques. It is in this sense that "democracy must become militant" (Loewenstein 1937a, 423–4).

Liberal democracy cannot prove the superiority of its achievements and counter emotionalism by means of the same emotional techniques. Rather, it must employ "political and legislative" measures appealing to "reason" (Loewenstein 1937a, 428). Politically, the approach can be to establish "a

united and uniform action among the democratically-minded sections of the people"; legislatively, it can be to enact antiauthoritarian laws and regulations "without flagrant violation of democratic principles," enabled by means of "parliamentary vote and public opinion at large" (Loewenstein 1937a, 429–30, 438–9). Political and civil restrictions serve the purpose of "ultimately preserving these very fundamentals," and liberal democratic constitutions and governance anticipate "emergency powers." Loewenstein was convinced—and World War II validates his contention—that such measures were warranted because authoritarianism had "declared war on democracy." Liberal democracies had to "live up to the demands of the hour" and make "every possible effort" to survive, establishing political unity and counterintuitively enacting legislation to confront authoritarian political movements, even when it appeared to imply "the risk and cost of violating fundamental principles" (Loewenstein 1937a, 432).

Defending democracy through restricting fundamental institutions and rights can dangerously lead to the opposite: weakening it and making it more susceptible to authoritarianism (Invernizzi Accetti and Zuckerman 2017, 182, 183–4). Loewenstein recognized that several European states hollowed out their constitutionality and destroyed the rule of law to the extent of becoming anocracies and authoritarians (Loewenstein 1937b, 638–40). This is an important lesson in the context of securitization and the expansion of surveillance since history shows that authoritarianism often encroaches through claims and proposals that are seemingly those of embattled liberal democracies. Nowadays, the emergency powers of the "state of exception" have increasingly become a "dominant paradigm of government" even in constitutional governments (Agamben 2005, 1–2). Their normalization should be viewed with caution as these can radically alter constitutional forms and establish the state of exception as the "threshold of indeterminacy between democracy and absolutism" (Agamben 2005, 2–3). Accordingly, it is important to clarify the legal and juridical understanding that states and institutions have of a "democracy capable of defending itself" (O'Connell 2009, 84).

The Basic Law of Germany and international frameworks such as the Universal Declaration of Human Rights (UDHR) and European Convention of Human Rights note, respectively, the duty to prevent "enemies of democracy" from employing the "rights and freedoms of democracy to undermine it"; that human rights cannot be used or abused to "undermine the purposes of the United Nations"; and that parties to the Convention cannot destroy the "rights and freedoms" that it sets forth (O'Connell 2009, 84–5). General legal and juridical understanding is that restrictions to rights must satisfy three criteria: these should be "for a legitimate purpose, prescribed by law and necessary in a democratic society." (O'Connell 2009, 86). Accordingly, the language of militant democracy is used to confront political violence, to combat discriminatory and extremist movements, to secure the transition to democracy in an anocracy, and to ensure constitutional or human rights.

Even so, restrictions and preventative measures are only legitimate and justified when states or institutions prove their commitment to democratic means and goals. History also shows that "even established democracies fall short of the ideal" of liberal democracy (O'Connell 2009, 86–90). Altogether, a militantly democratic approach to the oversight of surveillance within civil society can constructively employ a lack of trust in order to determine whether state and corporate policies and practices satisfy the three criteria of legitimacy, legality, and necessity. Doing so further establishes intelligent accountability and ensures the defense of liberal democracy while upholding human rights, civil liberties, and privacy and data protections.

Oversight of surveillance policies and practices in times of authoritarian drift

The previous section explained that various established democratic institutions are built upon a constructive lack of trust so as to check abuses of power. Questioning whether surveillance policies and practices can further defend liberal democracy is especially relevant in contemporary politics, where authoritarian drift is rampant. Militant democracy ensures constitutional government, avoids liberal democracy devolving into anocracy, and checks authoritarianism and its divisive emotionalism. The three criteria that determine whether militantly democratic means are justified can also be applied to the oversight of surveillance. Considering the above, this section will explore instances of surveillance policies and practices in Germany, Poland, and the United States—countries experiencing the political encroachment of far-right populism to varying degrees. It will critically analyze the policies and practices in question so as to clarify the manner in which these are also ideologized to varying extents and fail to fulfill the three criteria required for a militantly democratic oversight of surveillance.

Germany: oversight of intelligence and law enforcement agencies

The historical experiences of having devolved into far-right as well as far-left authoritarianisms have taught Germany the importance of militantly democratic institutions. Once the National Socialist Third Reich was defeated, the Federal Republic of Germany (1949) established the Federal Office for the Protection of the Constitution (BfV) through its Basic Law. A domestic security and counterintelligence agency, the BfV defends the "free democratic basic order" of Germany, monitors anticonstitutional activities, mostly those of far-left and far-right groups, and formally embodies militant democratic principles. The agency reports to the Ministry of Interior, and its principal executive agent is its president. A critical analysis of the case of former BfV president Hans-Georg Maaßen serves to clarify that a militantly democratic approach is required even within the oversight of the surveillance deployed

by an ostensibly militantly democratic institution. Maaßen, president of the agency from August 2012 to November 2018, was fired when he publicly contradicted the federal government by downplaying antimigrant violence that occurred during protests against a murder in the town of Chemnitz. When several government officials, including Chancellor Angela Merkel, condemned the violence, Maaßen not only argued that journalistic reporting on far-right gangs hunting foreigners in the streets was "deliberate misinformation," but also—astonishingly—claimed that "arrest records, various videos, media reports and photos of protestors doing the Hitler salute" were not "reliable information" (Jordan 2018).

The year before, however, Maaßen showed no qualms about arguing without any kind of reliable information for the expansion of surveillance of the "wives and children of German 'IS' fighters" returning to the country, stating that the agency should "keep them in our sights" since they "could pose a risk" (Deutsche Welle 2017). The children, he warned, "could be living time bombs […] brainwashed with a mission to carry out attacks" (Shalal and Siebold 2018), and therefore were not an "insignificant potential threat" (Deutsche Welle 2018). The state had already lowered its age limit for surveillance from 16 to 14 in 2016, but Maaßen argued that it should be expanded to include children under the age of 14. A civil rights organization explained that it was "unreasonable to consider children a threat to the constitutional order" and that their surveillance represented "a massive violation of their fundamental rights" (Deutsche Welle 2018). Remarkably, earlier that year, a former leader of the youth wing of the right-wing Alternative for Germany (AfD) denounced Maaßen for allegedly advising party leaders on strategies to "avoid being placed under surveillance." As reporting on Maaßen's contradictory policies intensified, it was revealed that the BfV had "failed for months to act on […] concerns about local [AfD] youth chapters" (Reuters 2018).

The BfV denied the leaks and stated that suspicions of party sympathies were "entirely without foundation" (Koch and Neuerer 2018). Governmental as well as public outcry ensured the removal of Maaßen, but interior minister Horst Seehofer proposed he become "deputy interior minister"—which was "technically a promotion with a pay rise" (Associated Press 2018a). When this backfired, Seehofer proposed Maaßen become his "special advisor" (Associated Press 2018a). Even more political and public outcry followed, especially when BfV agents blew the whistle on a video where Maaßen told "European domestic spy chiefs" that the Social Democratic Party (SPD), Germany's ruling coalition partner, were "radical left-forces" conspiring against him. Only then did Seehofer send Maaßen into "early retirement" (Escritt 2018).

A militantly democratic approach to oversight of surveillance is crucial because the ideologization of policies and practices is a threat to ensuring security. Thomas Haldenwang, the new BfV president, announced a significant expansion of agents monitoring far-right groups, explaining that the

violence in Chemnitz illustrated "developments in right-wing extremism," as numbers were rising and more than half were "violence-oriented" (Associated Press 2018b). Questioned whether the AfD has contributed to this growth, he replied that "in any case, it doesn't seem to be detrimental." The BfV announced surveillance of the far-right party, AfD critics claiming "an increasing blurring of boundaries between the party and the extreme right neo-Nazi scene" (Associated Press 2018b). The monitoring included AfD member Björn Höcke—a "driving force" in moving the party to "the extreme right" and "a threat to the liberal democratic principles of Germany's constitution"—as well as the party's youth wing (JA) (Connolly 2019). When Walter Lübcke, a conservative pro-refugee politician, was murdered by a right-wing extremist, the debate illustrated a lack of trust whether the BfV had "underestimated the threat posed by the militant far right" (Oltermann 2019). The agency's annual report, mostly written while Maaßen was BfV president, had failed to mention Nordkreuz, a far-right extremist group shown to have "close links to the police and military," which accessed police records to create a "death list" including "almost 25,000 names and addresses of local politicians" who had contributed to "civil efforts during the refugee crisis in 2015" (Oltermann 2019). Investigations of Nordkreuz further revealed members to be in the military, law enforcement, and reservists and that it was stockpiling of weaponry, ammunitions, and even body bags and quicklime to dissolve the corpses of "political enemies" (Bennhold 2020).

News coverage and public outcry led the federal government to propose 300 additional positions within the BfV to better monitor right-wing extremism, focus on early detection of radicalization of law enforcement and military personnel, and strengthen international cooperation with similar state agencies (Wiedmann-Schmidt 2019). This militantly democratic approach to oversight remains necessary, especially considering leaked classified documents that reveal authorities arguing to allow state security and intelligence "to read encrypted chats" and reports that the BfV is considering "artificial intelligence to identify suspicious postings online and on social media" (Der Spiegel 2019). Such efforts to further automate surveillance practices risk undermining intelligent accountability in the absence of militantly democratic oversight.

Oversight of surveillance technologies outsourcing

Poland not only has a history of occupation by far-right and far-left authoritarianisms, but it also had a pivotal role in the former Soviet sphere's transition toward democracy. In recent years, however, the European Union launched an unprecedented procedure to monitor "threats to the rule of law in Poland" because of measures enacted by the Law and Justice (PiS) party, which presently rules the government (Jankovic 2016, 51). A critical analysis of state untransparency and prevention of intelligent accountability

over surveillance technology in Poland sheds light on why a militantly democratic approach is recommended not only within civil society but also within the political opposition when there is an institutional lack of oversight. Importantly, the measures enacted by the PiS include nonacceptance of elected judges, which effectively paralyzed the Constitutional Tribunal, and "new laws relating to the media, civil service, the police, and prosecution" that allowed security and intelligence services to "obtain information from internet providers without a court order" or informing those surveilled (Jankovic 2016, 55, 58). Considered altogether, "the line between democracy and dictatorship seems to be very thin" and also "fragile and profoundly susceptible to subversion" (Jankovic 2016, 64). Consequently in 2017, the European Commission activated Article 7 of the Treaty on European Union against the country for "persistently flouting democratic rules." Years later, the vice president of the European Commission warned that it "had not yet had any impact on Warsaw's behavior" (Reuters 2019).

To be clear, the expansion of surveillance in Poland started before the PiS came to power, but the party's willingness to threaten the rule of law and the independence of the judicial branch has allowed this trend to intensify. The state has exploited events such as the 2016 North Atlantic Treaty Organization (NATO) summit or the papal visit to further surveil foreigners without judicial warrants and extend the time that suspects can be detained without charges (Szary 2016). In anticipation of the 2018 Conference of the Parties (COP) to the United Nations Framework Convention on Climate Change (UNFCCC), agencies were authorized to "collect, obtain, gather, verify, process and use information, including personal data about persons posing a threat to public safety and order, including outside the borders of the Republic of Poland" with few restrictions (Aronoff 2018). Furthermore, information on foreigners attending the conference, including "police records and intelligence gathered by state surveillance," could be collected without their "knowledge or consent" and stored several months after the event ended. Various UN bodies and special rapporteurs sent concerned letters to Polish authorities, warning that the measures "may lead to human rights violations" as acts of reprisal against individuals "for their cooperation with the United Nations" (Aronoff 2018).

Surveillance policies and practices in Poland, as with many postcommunist states, were characterized by "swift commercialisation of […] the police state's security apparatus" during the political transition, blurring the "lines between the private security industry" and state security and intelligence agencies (Łoś 2018, 363–4). Consequently, members of this industry "became the primary providers of risk definitions and risk management technologies" (Łoś 2018, 364). Unsurprisingly, Poland has continued expanding its surveillance capabilities by outsourcing to national and international corporations. According to a technical and academic report, Poland has deployed "Pegasus" surveillance malware created by NSO Group, a surveillance technology corporation based

in Israel (Marczak et al. 2018). The report led journalists and political opposition to inquire whether the malware was purchased and deployed by security and intelligence agencies. It is noteworthy that NSO Group has a scandalous record of its technologies being deployed to violate human rights and civil liberties (Gera 2019; Bing and Satter 2019). For this reason, a lack of trust in state purchases and deployments of Pegasus is entirely advisable. A Polish NGO defending freedom and human rights from contemporary technological threats argues that institutional lack of oversight of surveillance is the reason for the lack of clarity on whether the Central Anti-Corruption Bureau (CBA) and/or the security and intelligence agencies purchased and deployed malware such as Pegasus (Panoptykon Foundation 2019). The Civic Platform (PO) opposition party has publicly supported the interpretation that the purchase and deployment of Pegasus would be illegal since there is "no place for such systems in democratic countries respecting rule of law" because the malware would presumably "be used by secret police under the radar of the courts" (Kość 2019).

A militantly democratic approach is evident within political opposition and civil society attempts at oversight of surveillance policies and practices—and is recommended. Organizations such as Panoptykon Foundation have scrutinized previous instances of state untransparency and have questioned whether it is defensible to purchase security and intelligence goods from corporations that enable the surveillance policies and practices of authoritarian regimes and obfuscate the availability of such surveillance capabilities (Panoptykon Foundation 2015). Furthermore, they argue, the deployment of such surveillance technologies is worrisome for at least four other reasons: first, deploying Pegasus, "even if a court order were obtained," would most likely "not [be] legal under Polish law"; second, "oversight over secret services" in Poland is lacking, and "there is no obligation to inform people" who are being surveilled; third, parliamentarians are concerned these surveillance technologies are being deployed "against independent journalists" and "opposition politicians"; and, fourth, Poland "does not follow human rights standards," a claim supported by the fact such malware is "used by authoritarian regimes to spy on citizens" (Gera 2019). Civil society and the political opposition should continue their attempts at oversight with a militantly democratic approach, especially considering that Prime Minister Mateusz Morawiecki merely responded that everything "will be explained in due time" (Kość 2019), and Deputy Prime Minister Jacek Sasin entirely dismissed any concerns, offering discursive platitudes as divisive as the claim that "honest citizens" do not to worry about such matters (Kość 2019).

United States: oversight of governmental agencies and outsourcing of surveillance and intelligence technologies and services

The United States has not experienced devolution from liberal democracy to anocracy or authoritarianism. However, its global hegemony depends not

only on its economy and culture but also on the power of its military and intelligence. Moreover, no other liberal democracy has more state and corporate surveillance capabilities than the United States. A critical analysis of how these functions are increasingly outsourced clarifies why a militantly democratic approach to oversight is vital to limiting abuses of power and defending the political agency of civil society—especially those resulting from the ideologization of surveillance. It is clarifying to consider the ways in which immigration is being ideologized at the same time as securitized. Ongoing debate, domestically and globally, on this matter intensified after the revelation that thousands of immigrant children were separated from their families and detained in facilities without relatives (Aguilera 2019). This family separation practice was later disclosed as a "migration deterrent" within the wider scope of a "zero tolerance" antiimmigration policy (Miroff and Dawsey 2019). The extension of the state and corporate surveillance assemblage built in order to realize these and other immigration policies and practices is entirely unprecedented (Fox Cahn 2019).

This state–corporate nexus partners federal departments and agencies such as Homeland Security (DHS) and Immigration and Customs Enforcement (ICE) with corporations as recognizable as Amazon, Microsoft, and Hewlett-Packard (Corbett 2018) as well as other, more obscure, ones. Palantir Technologies, focused on big data mining and analytics, is such a corporation. The state has extensively outsourced matters concerning the military, intelligence, and law enforcement agencies to it. When public outrage against family separation began, Palantir insisted that it provided goods and services for "cross-border criminal investigations," not "interior civil immigration enforcement"—i.e., the deportation and detention of undocumented immigrants. However, an advocacy network obtained documents revealing that ICE employs "Investigative Case Management" (ICM), a Palantir software platform, to build "profiles of immigrant children and their family members" and facilitate their arrest and prosecution. The corporation's untrustworthiness was further exposed by the fact that ICM allows ICE agents to also access the intelligence platforms of various "other federal and private law enforcement entities" (Biddle and Devereaux 2019).

The function creep and drift of this surveillance assemblage is evidenced by the fact that fusion centers established for counterterrorism "not only monitor and target immigrants" but political activists as well. Diverse kinds of biometric information are collected in "cases of mass arrests at protests," stored, analyzed, and then shared with a multitude of federal agencies (Corbett 2018). Surveillance of those documenting, protesting against, or working with the consequences of present-day immigration policy goes further. A DHS whistleblower leaked documents revealing a secret database on people concerned with immigration to the United States as well as the migrant caravan approaching San Diego from Central America in late 2018. Alerts were placed on some of the passports of these concerned individuals—who

included political activists, lawyers, journalists, advocates, and social media influencers—to screen them at the border with Mexico and stop them from entering and working there as journalists or lawyers. Others were "arrested, interviewed, or had their visa or [expedited travel] pass revoked." These revelations confirmed previous reports from journalists, who denounced becoming "targets of intense inspections and scrutiny by border officials." Besides ICE, the database was made available to other federal law enforcement agencies, including Customs and Border Protection (CBP). The whistleblower warned that the creation of the dossiers constituted an abuse, since the DHS focuses on "criminal investigation" and not "intelligence." When local news media confronted the CBP with the leak, it confirmed neither the authenticity nor the legality of the dossiers. The agency only stated that assaults on law enforcement agents were made after the caravan arrived and the border wall was breached, which represented crimes and a "risk to public safety." As such, the event was being "routinely monitored and investigated" and evidence was collected "to determine if the event was orchestrated." Once the leak was reported, the CBP stated that those surveilled "were present during the violence" (Jones et al. 2019).

When dozens of civil society and nongovernmental organizations as well as senators sent letters of protests to the DHS acting secretary, the agency stated without evidence that those surveilled had "some level of participation in the violent incursion events." Only several months later did the DHS inspector general promise the senators to launch an investigation into "the creation of the secret dossiers" and "specific allegations of targeting and/or harassment" (Hussain and Cope 2019). Not only did the faltering CBP statements expose the agency as untrustworthy, but the instance of surveillance in question also failed to satisfy the three criteria of legitimacy, legality, and necessity. The American Civil Liberty Union (ACLU) qualified it as "outrageous," violating the constitutional freedoms of speech, of the press, and of assembly, and serving as "the latest example of abuse of power by the CBP," underscoring the "dire need for meaningful agency oversight and accountability" (Jones et al. 2019).

Although travel and immigration not only in the United States but worldwide, have greatly decreased as a result of the global COVID-19 pandemic (Connor 2020), it is worth remembering that shortly before the pandemic began, the administration of President Trump proposed collecting DNA samples from immigrants detained by law enforcement agencies, dubiously arguing that it could help "detect fraud and solve cold criminal cases"—even though multiple studies have shown immigrants commit less crimes than native-born citizens (Trotta 2019). It is reasonable to respond to the emotionalism underlying such a discourse with a lack of trust. The ACLU has warned that biometric surveillance can seriously impact privacy and civil liberties, with DNA collection employed in "criminal investigation" becoming used for "surveillance of the population" with "xenophobic goals"—i.e., establishing

immigrants as security "threats" (Trotta 2019). A militantly democratic oversight of surveillance can ensure that a liberal democracy does not devolve into an anocracy when ideologized policies and practices become commonplace, and that state accountability is not obfuscated behind the outsourcing of security and intelligence functions to corporate partners.

Some lessons for and from militant democracy

An examination of recent political dynamics in the United States, Poland, and Germany, provides evidence that contemporary liberal democracies are never exempt from experiencing authoritarian drift. Furthermore, while the exact circumstances and actors involved can vary widely, these diverse examples have in common the fact that surveillance policies and practices require strict oversight, lest they contribute to obscuring emotional appeals to ideology and make violations of civil liberties even more opaque. Surveillance, whether state or corporate or a synergy of both, trusted blindly and left unaccountable, can become a peril to liberal democracy. However, when guarded against by a militant commitment to values, institutional mechanisms, and political actions that are liberal and democratic in nature and realization, the potential of this threat can be kept from being actualized.

Conclusions and recommendations

This chapter began by addressing the dynamics of trust and transparency in relation to oversight of surveillance. It explained that granting trust to others, whether people or organizations, depends on their trustworthiness. Because the Snowden revelations proved a number of states and corporations to be untrustworthy in their surveillance policies and practices, the resulting lack of trust within civil society on the part of citizens and consumers requires constructively confronting the fact that these technologies can be deployed in manners that are obfuscated by untransparency, deceptions, and authoritarian emotionalism, oftentimes concealed within discourses of securitization and transparency that prevent intelligent accountability. Oversight of surveillance should not only demand clearer information in order to be transparent but also more instances to contest and resemantize—i.e., reinterpret and establish a new meaning for—surveillance policies and practices so as to ensure these are democratic, respecting and upholding human rights and civil liberties.

Accordingly, this chapter continued by arguing that democratic principles and institutions should be built on a constructive lack of trust, which only grants trust to the trustworthy. It was explained that the contemporary threat of authoritarian drift can exploit surveillance technologies to structure power and knowledge asymmetries that can threaten liberal democracy. Consequently, a militantly democratic approach within civil society is

recommended to oversee surveillance deployed by states, corporations, or the state–corporate nexus. Actors within civil society, governments, and corporate institutions can employ the three criteria of legitimacy, legality, and necessity to ensure that surveillance policies and practices establish security in a democratic manner, not only within their national contexts but within the global context as well.

This chapter addressed and critically analyzed contemporary experiences and lessons learned in Germany, Poland, and the United States concerning the oversight of surveillance, illustrating the manner in which a militantly democratic approach is practiced to check untransparency, emotionalism, and encroachment on civil liberties and human rights. Liberal democracy is not a state that is achieved and then maintained evermore, but a state that is accomplished by means of recurrent decisions to strive toward principles, establish institutions, and commit to courses of action that are liberal and democratic.

This chapter offered these explanations and recommendations in order to argue that a militantly democratic approach to surveillance oversight enables political agency within civil society to democratically reimagine and resemantize the direction and consequences that technologies have in structuring our societies, economies, and politics. Oversight of surveillance can be understood as a modality of resistance, contestation, and resemantization of policies and practices of surveillance so as to further enable a nascent digital agency, which can contribute to constructively structuring a "meaningful data politics" in which "human dignity and especially agency" decide the courses of action required to establish "alternative futures that embody holistic, reflexive and democratic imaginaries and practices" (Lyon 2019, 73). A constructive lack of trust and a militantly democratic approach to contemporary surveillance technologies and socioeconomic-political dynamics can loudly voice two crucial questions for reimagining and resemantizing our societies: "Do we really need this?" and "How does it contribute to the common good and human flourishing?" (Lyon 2019, 75).

References

Agamben, Giorgio. 2005. *State of Exception*. Chicago: University of Chicago Press.

Aguilera, Jasmine. 2019. "Trump Administration Has Separated 1,556 More Migrant Children than Previously Known." October 26, 2019, https://time.com/5710953/trump-administration-confirms-more-migrant-family-separation/.

Altman, Andrew. 2017. "Civil Rights." *Stanford Encyclopedia of Philosophy*, https://plato.stanford.edu/entries/civil-rights/.

Amnesty International. 2018. *Annual Report 2017/18*, www.amnesty.org/en/latest/research/2018/02/annual-report-201718/.

Aronoff, Kate. 2018. "Poland's New Surveillance Law Targets Personal Data of Environmental Advocates, Threatening UN Climate Talks." July 2, 2018, https://theintercept.com/2018/07/02/cop24-poland-surveillance-law/.

Associated Press. 2018a. "German Domestic Spy Chief Won't Get New Government Job." November 5, 2018, www.apnews.com/9b6e4f17f172402d8e69c2177312cf65.

Associated Press. 2018b. "Germany's Intel Chief to Step Up Efforts Against Far Right." December 21, 2018, www.apnews.com/64ac6f21d6be4e2e9e7d6611c5ce2084.

Ball, Kirstie, Sara Degli Esposti, Sally Dibb, Vincenzo Pavone, and Elvira Santiago-Gomez. 2019. "Institutional Trustworthiness and National Security Governance: Evidence from Six European Countries." *Governance* 32(1): 1–19, https://doi.org/10.1111/gove.12353.

Bennhold, Katrin. 2020. "Body Bags and Enemy Lists: How Far-Right Police Officers and Ex-Soldiers Planned for 'Day X.'" August 1, 2020, www.nytimes.com/2020/08/01/world/europe/germany-nazi-infiltration.html.

Biddle, Sam, and Ryan Devereaux. 2019. "Peter Thiel's Palantir Was Used to Bust Relatives of Migrant Children, New Documents Show." May 2, 2019, https://theintercept.com/2019/05/02/peter-thiels-palantir-was-used-to-bust-hundreds-of-relatives-of-migrant-children-new-documents-show/.

Bigo, Didier, Gertjan Boulet, Caspar Bowden, Sergio Carrera, Elspeth Guild, Nicholas Hernanz, Paul de Hert, Julien Jeandesboz, and Amandine Scherrer. 2013. "Open Season for Data Fishing on the Web: The Challenges of the US PRISM Programme for the EU." *Centre for European Policy Studies* (no. 293: June 18), www.dw.com/en/german-intel-chief-warns-of-potential-threat-posed-by-wives-children-of-german-jihadis/a-41630197.

Bing, Christopher, and Raphael Satter. 2019. "Exclusive: Government Officials Around the Globe Targeted for Hacking Through WhatsApp—Sources." October 31, 2019, www.reuters.com/article/us-facebook-cyber-whatsapp-nsogroup-excl/exclusive-government-officials-around-the-globe-targeted-for-hacking-through-whatsapp-sources-idUSKBN1XA27H.

Colomer, Josep M., David Banerjea, and Fernando Barros de Mello. 2016. "To Democracy Through Anocracy." *Democracy & Society* 13(1): 19–25.

Connolly, Kate. 2019. "Extreme-Right Wing of Germany's AfD Placed Under Surveillance." January 15, 2019, www.theguardian.com/world/2019/jan/15/extreme-right-wing-germany-afd-under-surveillance.

Connor, Phillip. 2020. "More Than Nine-in-Ten People Worldwide Live in Countries with Travel Restrictions Amid COVID-19." April 1, 2020, www.pewresearch.org/fact-tank/2020/04/01/more-than-nine-in-ten-people-worldwide-live-in-countries-with-travel-restrictions-amid-covid-19/.

Corbett, Erin. 2018. "Tech Companies Are Profiting Off Ice Deportations, Report Shows." October 23, 2018, https://fortune.com/2018/10/23/tech-companies-surveillance-ice-immigrants/.

Der Spiegel. 2019. "Deadly Attack Exposes Lapses in German Security Apparatus." October 11, 2019, www.spiegel.de/international/germany/far-right-terrorism-in-germany-shooting-exposes-lapses-in-security-apparatus-a-1291075.html.

Deutsche Welle. 2017. "German Intel Chief Warns of Potential Threat Posed by Wives, Children of German Jihadis." December 3, 2017, www.dw.com/en/german-intel-chief-warns-of-potential-threat-posed-by-wives-children-of-german-jihadis/a-41630197.

Deutsche Welle. 2018. "Islamist Children Pose Real 'Threat' to Germany, Spy Chief Warns." August 6, 2018, www.dw.com/en/islamist-children-pose-real-threat-to-germany-spy-chief-warns/a-44963227.

Escritt, Thomas. 2018. "Outgoing German Spy Chief Sacked for Branding SPD as 'Radical Left.'" November 5, 2018, www.reuters.com/article/us-germany-politics/outgoing-german-spy-chief-sacked-for-branding-spd-as-radical-left-idUSKCN1NA105.

Federal Republic of Germany. 1949. *Basic Law for the Federal Republic of Germany*, www.bundesregierung.de/breg-en/chancellor/basic-law-470510.

Fox Cahn, Albert. 2019. "Surveillance by Sanctuary Cities Is Helping ICE Track Undocumented Immigrants." July 9, 2019, www.nbcnews.com/think/opinion/surveillance-sanctuary-cities-helping-ice-track-undocumented-immigrants-ncna1027981.

Freedom House. 2018. *Freedom in the World 2018: Democracy in Crisis*, https://freedomhouse.org/report/freedom-world/freedom-world-2018.

Gera, Vanessa. 2019. "Poland Pressured to Say if It Bought Israeli Phone Spyware." September 4, 2019, www.apnews.com/461df123f8d84db9965ee2a762e17414.

Human Rights Watch. 2018. *World Report 2018*, www.hrw.org/world-report/2018.

Hussain, Saira, and Sophie Cope. 2019. "DEEP DIVE: CBP's Social Media Surveillance Poses Risks to Free Speech and Privacy Rights." August 5, 2019, www.eff.org/deeplinks/2019/08/deep-dive-cbps-social-media-surveillance-poses-risks-free-speech-and-privacy.

Invernizzi Accetti, Carlo, and Ian Zuckerman. 2017. "What's Wrong with Militant Democracy?" *Political Studies* 65(1): 182–99.

Jankovic, Sava. 2016. "Polish Democracy Under Threat? An Issue of Mere Politics or a Real Danger?" *Baltic Journal of Law & Politics* 9(1): 49–68.

Jones, Tom, Mari Payton, and Bill Feather. 2019. "Source: Leaked Documents Show the U.S. Government Tracking Journalists and Immigration Advocates through a Secret Database." March 6, 2019, www.nbcsandiego.com/news/local/Source-Leaked-Documents-Show-the-US-Government-Tracking-Journalists-and-Advocates-Through-a-Secret-Database-506783231.html.

Jordan, Frank. 2018. "Top German Spy Ousted after Clash with Merkel over Migrants." September 18, 2018, www.apnews.com/02e154035b4b4422810aa48e36e8c873.

Jordan, Klara. 2015. "Opinion: Why Microsoft's Data Access Case Matters to Everyone on the Internet." September 30, 2015, www.csmonitor.com/World/Passcode/Passcode-Voices/2015/0930/Opinion-Why-Microsoft-s-data-access-case-matters-to-everyone-on-the-Internet.

Koch, Moritz, and Dietmar Neuerer. 2018. "German Domestic Spy Chief Maassen under Pressure to Resign." October 9, 2018, www.handelsblatt.com/today/politics/monitoring-the-monitors-german-domestic-spy-chief-maassen-under-pressure-to-resign/23583276.html.

Kość, Wojciech. 2019. "Poland's PiS Faces Questions over Israeli Spyware." September 7, 2019, www.politico.eu/article/poland-pis-israeli-spyware-questions/.

Loewenstein, Karl. 1937a. "Militant Democracy and Fundamental Rights, I." *The American Political Science Review* 31(3): 417–32.

Loewenstein, Karl. 1937b. "Militant Democracy and Fundamental Rights, II." *The American Political Science Review* 31(4): 638–58.

Łoś, Maria. 2018. "Postscript." *Surveillance & Society* 16(3): 362–69.

Lyon, David. 2018. *The Culture of Surveillance*. Cambridge: Polity Press.

Lyon, David. 2019. "Surveillance Capitalism, Surveillance Culture and Data Politics." In *Data Politics: Worlds, Subjects, Rights*, edited by Didier Bigo, Engin Isin, and Evelyn Ruppert, 64–77. London: Routledge.

Marczak, Bill, John Scott-Railton, Sarah McKune, Bahr A. Razzak, and Ron Deibert. 2018. "Hide and Seek: Tracking NSO Group's Pegasus Spyware to Operation in 45 Countries." Citizen Lab, September 18, 2018, https://citizenlab.ca/2018/09/hide-and-seek-tracking-nso-groups-pegasus-spyware-to-operations-in-45-countries/.

Miroff, Nick, and Josh Dawsey. 2019. "'All the Best People': The Ghostwriter: The Advisor Who Scripts Trump's Immigration Policy." August 17, 2019, www.washingtonpost.com/graphics/2019/politics/stephen-miller-trump-immigration/.

O'Connell, Rory. 2009. "Militant Democracy and Human Rights," *Constitutional Law Review* 1: 84–90, www.constcourt.ge/uploads/other/3/3824.pdf.

Oltermann, Philip. 2019. "German Far-Right Group 'Used Police Data to Compile Death List.'" June 28, 2019, www.theguardian.com/world/2019/jun/28/german-far-right-group-used-police-data-to-compile-death-list.

O'Neill, Onora. 2002. "Reith Lectures: A Question of Trust." BBC, www.immagic.com/eLibrary/ARCHIVES/GENERAL/BBC_UK/B020000O.pdf.

O'Neill, Onora. 2013. "What We Don't Understand about Trust." *TEDxHousesofParliament*, https://youtu.be/1PNX6M_dVsk.

O'Neill, Onora. 2017. "Trust vs Trustworthiness." *Huxley Summit of the British Science Association*, https://youtu.be/XWwTYy9k5nc.

Panoptykon Foundation. 2015. "Legalne, ale tajne? Analiza kontrowersji wokół RCS." July 14, 2015, https://panoptykon.org/wiadomosc/legalne-ale-tajne-analiza-kontrowersji-wokol-rcs.

Panoptykon Foundation. 2019. "Pegasus, czyli inwigilacyjne zabawki CBA poza kontrolą." September 5, 2019, https://panoptykon.org/wiadomosc/pegasus-czyli-inwigilacyjne-zabawki-cba-poza-kontrola.

Reuters. 2018. "German Domestic Security Agency Failed to Act on AfD Concerns: Media." September 15, 2018, www.reuters.com/article/us-germany-security/german-domestic-security-agency-failed-to-act-on-afd-concerns-media-idUSKCN1LV0C5.

Reuters. 2019. "EU's Katainen Says Article 7 Procedure Against Poland Has Had Little Impact." May 1, 2019, www.reuters.com/article/us-poland-katainen-eu-idUSKCN1S73C6.

Schneier, Bruce. 2015. *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World* (epub version). New York: W. W. Norton & Company.

Shalal, Andrea, and Sabine Siebold. 2018. "'Brainwashed' Children of Islamist Fighters Worry Germany: Spy Chief." January 31, 2018, www.reuters.com/article/us-germany-security-children/brainwashed-children-of-islamist-fighters-worry-germany-spy-chief-idUSKBN1FK1FJ.

Szary, Wiktor. 2016. "Poland Approves Closer Surveillance of Foreigners Ahead of NATO Summit, Pope Visit." June 10, 2016, www.reuters.com/article/us-poland-security-lawmaking-idUSKCN0YW1OT.

Trotta, Daniel. 2019. "U.S. Proposes Collecting DNA Samples from Detained Immigrants." October 21, 2019, www.reuters.com/article/us-usa-immigration-dna/us-proposes-collecting-dna-samples-from-detained-immigrants-idUSKBN1X0250.

Verde Garrido, Miguelángel. 2015. "Contesting a Biopolitics of Information and Communications: The Importance of Truth and Surveillance after Snowden." *Surveillance & Society* 13(2): 153–67.

Wetzling, Thorsten, and Kilian Vieth. 2018. "Upping the Ante on Bulk Surveillance: An International Compendium of Good Legal Safeguards and Oversight Innovations." *Publication Series on Democracy* 50. Berlin: Heinrich Böll Stiftung, www.stiftung-nv.de/sites/default/files/upping_the_ante_on_bulk_surveillance_v2.pdf.

Wiedmann-Schmidt, Wolf. 2019. "Bundesregierung will Verfassungsschutz Massiv Aufstocken." September 24, 2019, www.spiegel.de/politik/deutschland/horst-seehofer-will-verfassungsschutz-massiv-aufstocken-regierungsplaene-a-1288364.html.

Zeid, Ra'ad H. 2018. "'Human Rights No Longer Treated as a Priority, but as a Pariah,' Zeid Tells 25th Anniversary Gathering in Vienna." May 22, 2018, www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=2311.

Zuboff, Shoshana. 2015. "Big Other: Surveillance Capitalism and the Prospects of an Information Civilization." *Journal of Information Technology* 30(1): 75–89.

Outlook

Chapter 13

Surveillance, transparency, and trust

Critical challenges from the COVID-19 pandemic

David Lyon

Introduction

It is no exaggeration to say that the issues of surveillance, transparency, and trust have never been as important as in the early twenty-first century. This bold assertion rests on the observation that today's complex global condition is the product of a heady—some would say toxic—mix of technological, social, economic, political, and cultural change. We inhabit a global world of high technology—the digital—in which major corporations vie for supremacy, challenging conventional nation-states and their varying "democracies," which are themselves simultaneously buffeted by new authoritarian nationalisms and the negative consequences of globalization.

Surveillance has become an everyday feature of social, economic, and political life in the twenty-first century. At an infrastructural level, the systems for organizing daily life are data dependent and surveillant. This has occurred faster than the development of appropriate norms and legal instruments for ensuring that surveillance is practiced for the common good (Stoddart 2021), including data justice based on trust, especially between state and citizen and corporation and consumer.

The unwelcome insertion of the coronavirus pandemic has sharpened debates over precisely these issues (French and Monahan 2020). At every level, COVID-19 exacerbates the acute threats to both person and planet, across various dimensions. Responses are overwhelmingly reliant on digital systems and devices, in a multitude of ways. This is not surprising; the pandemic was the first to occur in a context of developed platform companies, and it inspired imaginative digital responses. However, the lack of common regulation, along with resistance to government restrictions on the part of some large corporations, makes for an ambiguous situation, the consequences of which will be debated for years to come (Lyon 2021).

On the one hand the pandemic prompted a wholesale shift to remote working for millions of people, where feasible, and the massive global reliance on many highly surveillant platforms for communication, education, entertainment, and business. On the other is the huge array of digital devices

DOI: 10.4324/9781003120827-18

and systems for combating the effects of the virus, from ubiquitous contact-tracing apps to enhanced health data platforms for tracking its spread and distribution. Surveillance capitalism—the monetization of personal data by platform companies—is implicated in each.

Throughout 2020, state and corporate surveillance capacities were rapidly enhanced in many countries around the world. There was unprecedented pandemic-propelled growth in data gathering, analysis, and use, which within a few months had affected literally billions of people. China and India—with their huge populations—were among the many nations that expanded their ability to probe details of citizens' lives and made participation in smartphone-based schemes to obtain such data mandatory. Countries with small populations, such as Israel/Palestine or Iceland, also joined the COVID-19 surveillance rush to rapidly establish strengthened health data systems and to seek innovative digital applications designed to warn everyday smartphone users if they had been near a possibly infected person.

The global pandemic also inspired much welcome innovation in medical treatment and hospital care as well as numerous attempts to learn about and check the spread of the virus. These include multiple surveillance responses to COVID-19 as a *public health condition.* Such initiatives included efforts to chart the spread of the virus, to learn which geographical areas and population groups were the most vulnerable, and to allow as many people as possible to contribute meaningfully to reducing the ravages of contagion. The collection and curation of data were, however, not always accompanied by adequate explanations of how, why, and with what implications those data were being used for profiling and predicting or what expectations citizens could have about issues such as data protection and privacy. Transparency was often lacking and trust was eroded. In the Indian state of Kerala, for instance, legal objections were raised about the threat to civil liberties of the mandatory phone app.

At the same time, the surveillance responses to COVID-19 as a *social condition* have also been enormous and at the time of writing are also ongoing. There is a worldwide plethora of new surveillance initiatives—responding to developments such as working, shopping, and learning from home—that have been appearing with great rapidity but have been less in the limelight than those relating directly to the pandemic. Remote monitoring and policing of employees, urban residents, and students, along with enhanced routine commercial surveillance of consumers, is booming. These systems and devices are touted as supposed "solutions" to the social condition of a health emergency but, despite being inherently surveillant, are under even less ethical and legal scrutiny than usual. Yet their production bodes ill for those who care about the long-term consequences of the pandemic. Accountability for such innovations is often minimal to nonexistent (Deibert 2020).

Back in 2001, a perceived crisis of national and international security was prompted by the attacks on Washington and New York, and these were met

by a similar explosion of concern to find digital means of predicting and preventing terrorism. Although much was clear about the massively increased scope of US national security at the time—it affected many others globally, not least through air transportation requirements—it was not until the much-publicized disclosures by Edward Snowden in 2013 that the enormous reliance on so-called open-source data—that is, largely from social media—became clear. These prompted major, international queries about transparency—who knew?—and trust in relation to security-surveillance data (Lyon and Murakami Wood 2020, Laidler this volume).

But if that was true of 9/11 then how much more is the wholesale move to digital technologies evident in the global coronavirus pandemic that began in 2019? *The Economist* commented on the rapid growth of a "Coronopticon" as early as March 2020. While noting the need for urgent attention to be paid to the origins and spread of the disease, with a view to its containment, they did observe that many countries were using an array of apps and data systems to keep tabs on the pandemic—"and also, in the process, on their citizens" (The Economist 2020). While the emerging structure surpasses in multiple ways the unidirectional transparency of Bentham's 1791 "panopticon" prison diagram, certain similarities not mentioned in the *The Economist* briefing do bear mentioning.

First of all, it is clear that, as with so many apps and systems, those built or modified for the pandemic aspire to make the lives of ordinary citizens visible to the organizations that produce or use the technology, while little or no attention is paid to ensuring the transparency of the apps or systems to their subjects. Secondly, the reliance on digital technologies is often achieved through very close collaboration between government health departments and platforms along with private corporations. Public health tasks were often outsourced to private companies, with little oversight or accountability, either for completing tasks effectively or for safeguarding civil liberties or privacy. This also extends into other areas such as employment, commerce, and education. It is often unclear—think of the noteworthy case of the Google–Apple API offered for contact-tracing worldwide—exactly how government regulation applies or how these businesses are handling or storing data. This challenges notions of trust, in both business and government. Thirdly, the very framing of these emergency initiatives suggests a purely utilitarian spirit, much like that which energized Bentham in his quest for the greatest happiness of the greatest number. In the case of the pandemic, the emphasis is often on a calculus of how many deaths are acceptable in the effort to balance public health with economic dynamism.

In what follows, we shall examine these issues in more depth, with a view to considering the complex challenge of agency for human flourishing. This in turn depends on transparency and trust, each of which is threatened by many kinds of surveillance but which themselves require better definition and practical application. Why focus on flourishing? Because all too often the weight

of technological development and public policy pulls the questions down to the level of technocratic and deterministic criteria. To assert a need for considerations of human agency and flourishing is ambitious, of course, but as many contributions to these debates demonstrate, there is a crying need for ways to lift familiar constructions of the situation to a higher level.

Pandemic surveillance: transparency and trust

Since the late twentieth century, surveillance has grown exponentially—I choose these words carefully—in tandem with the development of digital technologies. Watching, monitoring, and tracking have shifted, in less than half a century, from being targeted and operated within specific siloes such as policing, workplace management, and government administration, to something experienced in everyday life as an unremarkable occurrence. Whereas machines such as video cameras were once placed where they might capture images as people pass by, we now see smartphones carried in personal pockets and bags that constantly record the time and place of communications and transactions between identifiable individuals, such that they may be mapped and traced. Of course, the surveillance cameras are still present, now enhanced by facial recognition technology, and are used by countries such as China, India, Russia, and South Korea to help enforce pandemic quarantines (Roussi 2020). These basic changes, orchestrated by both public and private organizations, now shape human life in unprecedentedly subtle yet serious ways.

The global pandemic that began in 2019 and spread in waves of contagion throughout the world was met with increased modes of surveillance that accentuated the vexing issues of data circulation. These were already the stuff of government commissions, academic research, company policy, and privacy and data protection regimes the world over. But now they presented themselves as even more troubling conundrums. While one might well be skeptical about the "security theater" and "terrorist threat" scares spawned by 9/11, COVID-19 was a palpable peril. Many thousands of ordinary people got horribly sick and died in many countries—and at the time of writing, are still being infected and, all too often, dying. The dismal toll does of course affect some population groups—predictably, the already disadvantaged and vulnerable—more than others, but it is nevertheless the case that millions more people around the world are at serious risk than were ever affected by terrorism.

At the same time, the situation also catalyzed the accelerated adoption of many new technologies. Consumer and business digital adoption skyrocketed (McKinsey 2020) with leaps of speed and scale. Online shopping and cashless transactions grew faster than anyone anticipated, while communication platforms such as Zoom grew from 10 million users in December 2019 to 300 million users by October 2020. In this context, Shoshana Zuboff's (2019)

analysis of surveillance capitalism becomes strikingly relevant. Platforms are driven by the impulse to collect, analyze, and act upon such everyday data, exponentially. Beyond the directly commercial context, schools and universities switched, when "necessary," to remote learning, complete with apps for everything from checking attendance to policing exams, and many employees still lucky enough to have jobs remained at home to work—all the while monitored by newly installed software. And of course, in obvious areas such as health, doctors switched rapidly in many countries to online consultations. The public health innovations were just another aspect of this generalized digital shift. However, while Zuboff's (2019) primary concern is how behavioral manipulation constrains what she sees as "autonomy," this hardly touches upon the urgent questions of how surveillance capitalism also magnifies socioeconomic inequalities, compounding systemic injustice.

The most immediate effects of the pandemic are those relating to healthcare and the imperative to reduce the risk of infection and its spread. A central conundrum is that those at risk wish to feel safe, but the proffered "solutions" are often ones that themselves carry risks. Contact-tracing, for instance, which in many cases offers to alert the users of an app when they have been close to an infected person, is replete with such contradictions. Systems may be either centralized, as the initial program in the UK, or related ones in China and Israel–Palestine, or decentralized, the latter often taking advantage of the Google–Apple API, offered so that health departments may create their own apps. Decentralized systems also include the European Decentralized Privacy-Preserving Proximity-Tracing protocol used in several countries. More data may be acquired through centralized systems, deemed useful for risk modeling and analysis, but critics object that without clear limits, once in government hands, those data could easily be used for other purposes. Beyond privacy and security concerns are important ethical and justice issues (Kitchin 2020; Muller 2020; Scassa et al. 2020).

Such issues, beyond what might be covered by privacy or data protection law, include simple failure to do the right thing, such as warning citizens about the limitations of digital tracking for contact-tracing. They can easily produce false positives—for instance if carried down a grocery store aisle. Again, the Bluetooth versions may have insufficient uptake, thus reducing their reliability. On a wider level, the use of contact-tracing apps may be used by employers to prevent workers from returning to work or, if used as "COVID passports," could undermine their "non-mandatory" status. The lack of access to such apps by those without cellphones could exacerbate other forms of inequality.

These kinds of complications, common to surveillance in the twenty-first century, have been widely accentuated during the global pandemic. Extensive public–private cooperation, for example, is visible in just about every jurisdiction, whether authoritarian or democratic. Chinese COVID-19-inhibiting initiatives, for instance, feature major corporations such as Alipay, which runs

the major contact-tracing app with its three-color "Health Code" scheme but is also answerable to the State Council. Indeed, the initiative with Alipay is also seen as a test-run for China's "Social Credit" schemes, set up, paradoxically, with precisely the aim of *ensuring* trust in a society that lacks Western-style credit cards. Critical discussion of these issues was sparked on Weibo (roughly the Chinese equivalent of Twitter), suggesting that much *mis*trust exists regarding the responses to the pandemic (Lin 2020).

The politics of trust and transparency are also observable. For example, South Korea was frequently cited in contrast to the Chinese case with respect to trust in government COVID-19 schemes. Much was made—by UNESCO for example—of the "openness and transparency" of South Korea's response to the rapid spread of the virus in that country (UNESCO 2020). It is interesting that the government's greater "transparency" was in response to complaints about damaging government secrecy during the MERS pandemic of 2015, when little was reported about virus hotspots. In 2020, after an explosive early outbreak, testing and tracing were implemented much more rapidly, plus public mapping in which citizens could check the movements of patients identified only by gender and age, and even see whether their homes were disinfected or if they were wearing masks (Thompson 2020).

Public trust in government is crucial to the effective working of digital systems established to counteract the pandemic (Ball et al. 2018), and such trust is based on the perceived *trustworthiness* of the government departments concerned. Furthermore, such trustworthiness must depend on the keeping of commitments, a feature of trust that applies in both interpersonal and institutional contexts (Hawley 2012). Some governments lost citizen trust, at least for a time, as was the case in Mexico in November 2020, when a program using QR swiping for contact-tracing was announced—including the fact that participation would be mandatory. This lacked democratic process, to which Mexico is officially committed. The former Data Protection Commissioner tweeted her disapproval, asking citizens to resist, and just before the rollout the government back-pedaled, stating that the initiative was voluntary (Martínez 2020). But of course, such episodes are not merely products of the pandemic. They relate to much longer-term shifts in patterns of governing and especially to the democratic deficits seen in contemporary populism and neoliberal practices and policies.

Many issues have arisen also concerning transparency. Transparency may be demanded by citizens and pressure groups but may also be imposed by the powerful. As Shaul Duke (this volume) notes, the tensions between "imposed" and "voluntary" transparency are profound and are worked out in a range of moves and counter-moves in the case he discusses—Israel/Palestine. During the pandemic, Israel required Shin Bet—the security agency normally involved in checking on Palestinian "terrorism"—to manage the country's contact-tracing system. Though critical questions

about civil liberties were raised about this in Israel and internationally, Shin Bet continued to run the contact-tracing system until March 2021 (Amit et al. 2020). This is hardly reassuring for those who see Shin Bet as a key means of minimizing Palestinian self-determination through its debilitating suspicion of both Israeli Arabs and Palestinian communities in the West Bank and Gaza. Transparency was in fact missing from the start, as the Shin Bet contact-tracing system was set up after an overnight cabinet meeting, thus bypassing parliamentary approval.

Both transparency and trust also have to be placed in a larger context, however—that of the rapidly expanding world of reliance on digital infrastructures. While the decades following World War II saw the application of computing and communication technologies to bolster and support surveillance activities, both commercial and governmental, the present stage of digital development means that the infrastructures *themselves* are deeply surveillant. The platform companies and surveillance capitalism represent this shift, in which value is located in the metadata generated by the everyday use of social media in particular and the internet in general. Transparency is seriously lacking among the platform companies; even when Facebook's Mark Zuckerberg faces high-level public questioning he refuses to acknowledge what Facebook routinely does with its users' data. And as Twitter's Jack Dorsey admitted at the October Congressional hearings, "We realize we need to earn trust more, we realize that more accountability is needed, to show our intentions and show our outcomes" (Romm et al. 2020).

Understanding trust and transparency sociologically

The concept of transparency has been debated in relation to the digital realm for several decades. It is unlikely to subside any time soon. Over time, it has taken wildly different forms, from the bright optimism of David Brin's (1998) *The Transparent Society* to Byung Chul Han's (2015) gloomy pessimism in *The Transparency Society*. Each of these books deals mainly with *social* transparency in the context of the putative loss of privacy in contemporary society. Brin argued that the quest for government-protected privacy is ultimately futile and that worries about growing surveillance could be assuaged by giving everyone the means of surveillance. This is an old argument, also sometimes used by those who optimistically engage in *sousveillance* or "watching from below."

But as technology critic Bruce Schneier (2008) observes, Brin discounts the already existing power differences between the parties involved, which place strong limits on hopes for transparency understood in this way. This relates closely with the arguments often made about inequalities associated with surveillance as "social sorting," especially in a big data context (Lyon 2003, 2007; Eubanks 2018). The power differentials are clear in a world where surveillors increasingly score and rank the populations on whom they have data, using

complex and inaccessible data analytics, without revealing how that process occurs or that its effects are consequential on those groups (Lyon 2014).

Byung Chul Han, on the other hand, while also acknowledging what he views as the diminution of private life, maintains that easily obtainable information means that transparency—that is, primarily, of those targeted by surveillance—creates a society of control, not of trust. Politics becomes increasingly short-term, with little sense of responsibility for the future. He sees this worsening with the COVID-19 pandemic, arguing that the state of exception engendered by the pandemic will be made permanent through the expanded use of digital tools against the coronavirus. Thus, the isolating tendencies of pandemic controls will strengthen the capitalist state (Han 2020).

Beyond such debates, in which participants often seem to talk past each other, it makes sense to consider some more specific problems with transparency as a goal among those who wish to increase democratic participation in digital times. One astute critic is David Pozen, who shows how easily the word transparency can be—and is—subverted in contemporary political discourse. While many still cling to the concept as a critically important aspect of good governance, or of data protection and policy, "it is increasingly suspected of facilitating antiregulatory or neoliberal agendas and of undermining the very values it is meant to promote" (Pozen 2019: 326; see also Viola this volume). Pozen very sensibly notes that as a concept, transparency is *not* coherent and thus that different and opposing views of its usefulness are bound to proliferate (see also Bjorkland, this volume). And he argues that a "sociological turn" is required to examine the historical, legal, cultural, and other contexts in which transparency concepts are developed and used.

Pozen quotes Darin Barney, who insists that transparency is never a "thing" but a social process, a means, not an end (Pozen 2019: 327). This is why sociological clarity is required. Human flourishing, or the flourishing of the earth itself, are *ends*, within which we may locate, in the present context, derived goals such as data justice. Transparency, on the other hand, is merely a means to such ends and has to be evaluated in each context for its contribution to human and social benefit. If, for instance, the opacity of the terms of service advertised by platform companies could be reduced, then the transparency of the provider to the user would be enhanced. But for this to serve genuine goals, other requirements, such as that users know how to respond to the information to which they now have access (see e.g. Raab 2012a), would have to be met. But greater platform transparency is only one limited step toward proper accountability. The latter has been developed more fully during the present century and has been given teeth within some data protection and human rights contexts (Raab 2012b). But neither transparency nor accountability in themselves could bring anything like a satisfactory condition of *data justice* into being. Why? Because if data justice means ensuring how people are made visible, represented, and treated, using data, is appropriate and fair,

then merely to see more clearly how users are unfairly dealt with will not contribute much to desirable outcomes.

So, can transparency contribute to more trust in government, as was frequently suggested in the later twentieth century? Again, it depends. As Matthew Hall (this volume) eloquently argues, the act of publicizing power can itself have chilling effects. As he observes, the very fact that one *could* be harmed by surveillance may damage our freedom as citizens; such domination is a present threat. Theoretically, at least, Pozen is correct to say that the transparency–trust relationship is not self-evident (see also Bjorkland, this volume). But he also pleads for careful empirical analysis of the social situations in which transparency is sought, analysis that is highly attentive to context. The kinds of research that are required for a proper understanding of transparency in relation to rapidly expanding surveillance capitalism would do well to heed the suggestions made by Pozen. They are highly germane to the goals of any study of transparency, especially as it affects trust. As he concludes, "sociological inquiry, broadly conceived, gives our best hope for developing a deep understanding of transparency policies and their many and varied impacts" (Pozen 2019: 330).

What conditions are required for human flourishing?

As noted earlier, all too often, the weight of technological development and public policy pulls questions about surveillance down to the level of technocratic and deterministic criteria. There are many examples of how this happens. One is that the increasing range of public–private partnerships has made it more difficult to demand full accountability from corporations, which are sometimes seen as extensions of government activity rather than as entities subject to rules, regulations, and laws. Beyond this, of course, is the massive power of today's giant tech companies—the platforms in particular—that seems to lend them a sense of invincibility and immunity from criticism. Then, as they are tech companies, they depend on computing scientists and software engineers, who—despite some shining contrary examples—often dissociate themselves from the social contexts and consequences of their work and disengage from the politics of their endeavors (Möllers forthcoming).

Intellectual and practical work is needed to reverse the apparent guiding principle of much technological innovation, which is that human beings should constantly adapt themselves to the new. This chapter urges, rather, consideration of ways in which technologies could be shaped to truly human ends. Thus, in our present context, for example, the development of surveillance systems, devices, and apps should be guided by criteria whose shorthand here is "human flourishing." And if that sounds like a rather vague term, substantive content follows. It is deliberately broad, denoting a cluster of virtues and goals.

Of course, human flourishing is seen in diverse ways around the world, but many—perhaps classically, Aristotle—have seen such flourishing as dependent on living life with others, with people helping one another to develop virtues—good habits—which, as they continue to be practiced, contribute to love and justice. Such ideas are common to the world's religions, especially the Abrahamic: Judaism, Christianity, and Islam. As Miroslav Volf (2017) argues, such religions are inherently globalizing, and in an intensively globalized world, they continue to offer themes to guide contemporary societies. Love and justice are two pursuits related to flourishing, and in the context of surveillance they can be given specific aims—to an ethics of care with data on the one hand and to data justice on the other. One way of seeking these would be to ensure specific forms of transparency from those who surveil, such that they could demonstrate their willingness to be *accountable* to others, particularly when the plight of vulnerable population groups is obscured by the data (Taylor 2020). It would also contribute to trust if they were thus shown to be open to assessment. But this is only a first step to the goal, not the destination.

What social, technological, and political conditions might help promote human flourishing? Flourishing is more than health or security; it comprises a complex amalgam of varying features (Volf 2017). Nor is it appropriate to reduce flourishing to autonomy. There is a need to go beyond Zuboff's excellent work on surveillance capitalism here. Her target—not inappropriately—is the manipulation and behavior modification sought by Google and other platforms that emulate Google (Zuboff 2019). But, firstly, claims about autonomy can easily be reduced to an individualistic level and thus to a denial of the intrinsic sociality of humanness. And, secondly, the shaping of personal behaviors is not the only product of surveillance capitalism, which also systematically reproduces and reinforces social difference and disadvantage. Thus, a key aim of any desire to recalibrate the current mode of prediction to quite different ends would be rather to promote and struggle for "data justice" (Taylor 2017).

For Taylor, data justice goes beyond current data practices, which tend to be driven by technical, governmental, and commercial goals rather than social ones. Data-driven discrimination is widespread and relatively unimpeded by law or regulation. The root of the problem is that algorithms are constructed that make people visible in particular ways and that visibility is highly consequential for life chances and choices. To seek data justice is to demand fairness in the ways that people are made visible, represented, and treated as they continuously produce data. Doing this leads to the discovery of ethical paths through a datafying world. For Taylor, international data justice involves (in) visibility, (dis)engagement with technology, and antidiscrimination (Taylor 2020). Transparency and accountability are crucial here, especially in relation to the public–private interface, which today is a central issue in surveillance.

Governments employ few data scientists and generally rely on corporate bodies to provide such assistance.

Taking this further, many grassroots concerns and activities are evidence of social involvement and the search for local and global person-and-planet practices and orientations. In terms of technological involvement, movements to reinscribe social responsibility in technical education, reengaging computing and software professionals with the wider purposes of their expertise, is a vital contribution. Sara Degli-Esposti and David Arroyo (this volume) make an excellent case for trust-as-care, as opposed to mere control, which also speaks strongly to the matter of computing and software education. This can be reinforced, in the pandemic context, with Taylor's (2020) call for an ethics of care over and against the dominant utilitarian calculations, especially in countries where neoliberalism has taken root. This places emphasis on the collective rather than the population. People, with their unequal positions, are the focus.

Such social awareness may be complemented with more properly political activities in the quest for data justice—which also questions utilitarian calculation—and in the search, for instance, for ways of giving citizens the opportunity to help decide the rules of transparency (Hall, this volume). In addition, Verde Garrido (this volume) also insists that surveillance overreach, as exposed by Edward Snowden, requires citizens *not* to trust certain government agencies. These general orientations also have to be considered in the context of local historical cultural conditions. These include not only the massive and now long-term influence of tech giants based in California's Silicon Valley, but also, today, the huge influence of China and, increasingly, India. While the US platforms still affect millions in many parts of the globe, the influence of the newer digital economies of China and India have far-reaching impacts in emerging countries of the Global South in particular (Chakrovorti 2018).

Mobilizing publics, from grassroots to global

How can human agency and human flourishing be asserted in an age of surveillance? This appears as an unattainably high-level question at the best of times, but especially during a global pandemic. Yet a moment's reflection on the alternatives may place this aim in a better, and more realistic, light. Platform and related companies in many countries are frequently monopolistic, hugely powerful in their control of resources, markets, and employees, and arrogantly confident that they can do a better job of governing than democratically elected officials. Although much surveillance is carried out by government departments, security agencies, and the police, their activities are very often dependent on systems, software, and data originating in those corporations. The surveillance systems that have evolved under tech

company guidance exude utilitarian, technocratic, and "tech-solutionist" approaches.

There currently seems to be little enthusiasm for transparency among the leading players of the platform world. Their multibillionaire CEOs, such as Jeff Bezos, formerly at Amazon, and Mark Zuckerberg, at Facebook, show no signs of opening their corporate activities to scrutiny, any more than Sundar Pichai at Google—the company credited with creating surveillance capitalism—does. In the United States, Facebook's reputation has slipped significantly, mainly due to a lack of user trust in its handling of personal information, while Microsoft holds a high place and Amazon likewise—no doubt credited with keeping people supplied with the goods no longer available in brick-and-mortar stores at the start of the pandemic (*Verge* 2020). At the same time, the *Verge* (2020) survey supported earlier findings by Pew researchers that around half the US population believes that the big platforms do indeed require more government regulation (Smith 2018). But will governments step up and actually challenge the platforms? Former UK Information Commissioner Elizabeth Denham stands out for her challenge to Facebook after the Cambridge Analytica scandal in 2018. But the maximum fine she could levy was GBP500,000—a drop in a bucket for Facebook. This is a critical question that will have to be faced head-on in the coming years, if trust is to be restored.

How can the public be mobilized to reflect and deliberate on these issues? Post-Snowden, many have been retreating even further from public debate. And in some countries, of course, meaningful public debate has been muted by rising populist authoritarianism and nationalism. In Europe and the United States, some public debate has been growing, mostly in relation to the apparent unreliability of platforms and their unwillingness to listen to criticism—think Facebook, Amazon, Google, but also Airbnb and Uber. However, some security surveillance activities are still under scrutiny (e.g. Lyon and Murakami Wood 2020).

Of course, it may well also be possible to add surveillance trust-and-transparency concerns to other public issues. The Black Lives Matter movement is an obvious case in point in the northern hemisphere, as that cannot but be associated with police surveillance technologies, particularly body cameras and facial recognition technologies, in which data justice is manifestly lacking. Specific data-justice-promoting proposals relating to COVID-19 systems include data trusts (Dawson 2020) and distributed ledger technology (Demos Helsinki 2020). In addition, environmental and green concerns have to be considered in relation to the increasingly heavy energy requirements for server farms to service the internet, and these can be tied in with surveillance and data justice concerns (cf. Deibert's (2020) Massey Lectures emphasizing civil society).

A final, crucially important argument is prompted by the currently dominant feature of the internet, in its platform and social media aspects. The

culture of surveillance manifests a multiplicity of modes of online involvement, in which data politics (Bigo et al. 2019; Lyon 2019) is increasingly important and within which data justice becomes increasingly paramount (Taylor 2017). If agency is to be recovered in this area, it will come from those actively engaged with the internet, whose involvement is constructively political. The attitude of the platform companies, as Zuboff (2019) often observes, is that their activities are inevitable and their consequences unavoidable, and behaving as if such doctrines are true will indeed undermine agency. But the evidence of much online activism (cf. Verde Garrido, this volume) gives that doctrine the lie. Indeed, within the internet and social media itself many work to demonstrate that care and justice should govern both our considerations of transparency and the pressure to create new grounds for trust in the world of the digital.

References

Amit, Moran, Heli Kimhi, Tarif Bader, Jacob Chen, Elon Glassberg, and Avi Benov. 2020. "Mass Surveillance Technologies to Fight Coronavirus Spread: The Cases of Israel." *Nature Medicine*. 26(August): 1160–1169, www.nature.com/articles/s41591-020-0927-z.pdf?origin=ppub.

Ball, Kirstie, Sara Degli Esposti, Sally Dibb, Vincenzo Pavone, and Elivira Santiago-Gomez. 2018. "Institutional Trustworthiness and National Security Governance: Evidence from Six European Countries." *Governance*. 32(1): 103–121.

Bigo, Didier, Engin Isin, and Evelyn Ruppert. 2019. *Data Politics: Worlds, Subjects, Rights*. London: Routledge.

Brin, David. 1998. *The Transparent Society*. New York: Perseus.

Chakravorti, Bhaskar. 2018. "Competing in the Huge Digital Economies of China and India." *Harvard Business Review*. November 6, 2018, https://hbr.org/2018/11/competing-in-the-huge-digital-economies-of-china-and-india/.

Dawson, Philip. 2020. "COVID-19 Tracking Data Should Be Managed the Way Data Trusts Are." *Policy Options*, April 20, 2020, https://policyoptions.irpp.org/magazines/april-2020/covid-19-tracking-data-should-be-managed-the-way-data-trusts-are/.

Deibert, Ron. 2020. *ReSet: Reclaiming the Internet for Civil Society.* Toronto: Anansi.

Demos, Helsinki. 2020. "Tech vs COVID-19: Transparency and Trust Go to the Heart of Public Power." June 1, 2020, www.demoshelsinki.fi/en/2020/06/01/letter-tech-vs-covid-19-transparency-and-trust-to-the-heart-of-public-power/.

The Economist, 2020. "Countries Are Using Apps and Data Networks to Keep Tabs on the Pandemic … and also, in the Process, Their Citizens." March 28, 2020, www.economist.com/briefing/2020/03/26/countries-are-using-apps-and-data-networks-to-keep-tabs-on-the-pandemic/.

Eubanks, Virginia. 2018. *Automating Inequality: How High-Tech Tools Profile, Police and Punish the Poor*. New York: St Martin's Press.

French, Martin, and Torin Monahan. 2020. "Dis-ease Surveillance: How Might Surveillance Studies Address COVID-19?" *Surveillance & Society* 18(1): 1–11.

Han, Byung Chul. 2015. *The Transparency Society*. Stanford: Stanford University Press.

Han, Byung Chul. 2020. "Los países asiáticos están gestionando mejor esta crisis que Occidente." *El Pais*, https://elpais.com/ideas/2020-03-21/la-emergencia-viral-y-el-mundo-de-manana-byung-chul-han-el-filosofo-surcoreano-que-piensa-desde-berlin.html. English translation available at https://www.readingthechinadream.com/byung-chul-han-coronavirus.html.

Hawley, Katherine. 2012. *Trust: A Very Short Introduction*. Oxford: Oxford University Press.

Kelley, Jason. 2020. "Governments Must Commit to Transparency During the COVID-19 Crisis." March 20, 2020, www.eff.org/deeplinks/2020/03/governments-must-commit-transparency-during-covid-19-crisis.

Kitchin, Rob. 2020. "Using Digital Technologies to Tackle the Spread of Coronavirus: Panacea or Folly?" Maynooth University, https://progcity.maynoothuniversity.ie/wp-content/uploads/2020/04/Digital-tech-spread-of-coronavirus-Rob-Kitchin-PC-WP44.pdf.

Lin, Liza. 2020. "China's Plan to Make Permanent Health-Tracking on Smartphones Stirs Concern." *The Wall Street Journal*, May 25, 2020, www.wsj.com/articles/chinas-plan-to-make-permanent-health-tracking-on-smartphones-stirs-concern-11590422497.

Lyon, David. 2003. *Surveillance as Social Sorting: Privacy, Risk and Digital Discrimination.* London: Routledge.

Lyon, David. 2007. *Surveillance Studies: An Overview*. Cambridge: Polity Press.

Lyon, David. 2014. "Surveillance, Snowden and Big Data: Capacities, Consequences, Critique." *Big Data & Society*. July–December: 1–14. https://journals.sagepub.com/doi/pdf/10.1177/2053951714541861.

Lyon, David. 2019. "Surveillance Capitalism, Surveillance Culture and Data Politics." In *Data Politics: Worlds, Subjects, Rights*, edited by Didier Bigo, Engin Isin, and Evelyn Ruppert, 64–78. London: Routledge.

Lyon, David. 2021. *Pandemic Surveillance*. Cambridge: Polity Press.

Lyon, David, and Murakami Wood, David. 2020. *Security Intelligence and Surveillance in the Big Data Age: The Canadian Case*. Vancouver: University of British Columbia Press.

Martínez, Laura. 2020. "Contact-Tracing and Personal Data Protection Face-Off in Mexico City." *Slate*, https://slate.com/technology/2020/11/mexico-city-qr-code-contact-tracing-program-coronavirus.html.

McKinsey. 2020. "How COVID-19 Has Pushed Companies over the Tipping Point and Transformed Business Forever." (Report), www.mckinsey.com/business-functions/strategy-and-corporate-finance/our-insights/how-covid-19-has-pushed-companies-over-the-technology-tipping-point-and-transformed-business-forever/.

Möllers, Norma. Forthcoming. *A Culture of Disengagement: Computer Science and the Question of Justice in Algorithms*. Cambridge: MIT Press.

Muller, Bertie. 2020. "Tracking COVID-19 Effectively Rests on Transparency." *Techerati*, www.techerati.com/features-hub/opinions/tracking-covid-19-effectively-rests-on-transparency/.

Pozen, David. 2019. "Seeing Transparency More Clearly." *Public Administration Review*. 80(2): 326–331.

Raab, Charles. 2012a. "The Meaning of 'Accountability' in the Information Privacy Context." In Daniel Guagnin et al., eds. *Managing Privacy Through Accountability*. London: Palgrave-Macmillan.

Raab, Charles. 2012b. "Regulating Surveillance: The Importance of Principles." In Kirstie Ball, Kevin Haggerty, and David Lyon, eds. *The Routledge Handbook of Surveillance Studies*. London: Routledge.

Romm, Tony, Rachel Lerman, Cat Zakrzewski, Heather Kelly, and Elizabeth Dwoskin. 2020. "Facebook, Google, Twitter CEOs Clash with Congress in Pre-Election Showdown." *The Washington Post*, www.washingtonpost.com/technology/2020/10/28/twitter-facebook-google-senate-hearing-live-updates/.

Roussi, Antoaneta. 2020. "Resisting the Rise of Facial Recognition." *Nature*. November 18, www.nature.com/articles/d41586-020-03188-2.

Scassa, Teresa, Jason Millar, and Kelly Bronson. 2020. "Privacy, Ethics and Contact-Tracing Apps." In Colleen M. Flood, Vanesssa MacDonnell, Jane Philpott, Sophie Thériault, and Sridhar Venkatapuram, eds. *Vulnerable: The Law and Politics of COVID-19*, Chapter C-2. Ottawa: University of Ottawa Press.

Schneier, Bruce. 2008. "The Myth of the Transparent Society." *Wired*, March 6, 2008, www.schneier.com/essays/archives/2008/03/the_myth_of_the_tran.html/.

Smith, Aaron. 2018. "Public Attitudes Toward Technology Companies." Pew Research, www.pewresearch.org/internet/2018/06/28/public-attitudes-toward-technology-companies/.

Stoddart, Eric. 2021. *The Common Gaze: Surveillance for the Common Good*. London: SCM Press.

Taylor, Linnet. 2017. "What is Data Justice? The Case for Connecting Digital Rights and Freedoms Globally." *Big Data & Society*. July–December: 1–14, https://journals.sagepub.com/doi/pdf/10.1177/2053951717736335/.

Taylor, Linnet. 2020. "The Price of Certainty: How the Politics of Pandemic Demand an Ethics of Care." *Big Data & Society*. July–December: 1–7, https://journals.sagepub.com/doi/pdf/10.1177/2053951720942539/.

Thompson, Derek. 2020. "What's Behind South Korea's COVID-19 Exceptionalism?" *The Atlantic*, www.theatlantic.com/ideas/archive/2020/05/whats-south-koreas-secret/611215/.

UNESCO. 2020. "How the Republic of Korea Flattened the COVID-19 Curve: Openness, Transparency and Democracy." https://en.unesco.org/news/how-republic-korea-flattened-covid-19-curve-openness-transparency-and-democracy.

Verge. 2020. "Tech Survey." www.theverge.com/2020/3/2/21144680/verge-tech-survey-2020-trust-privacy-security-facebook-amazon-google-apple.

Volf, Miroslav. 2017. *Flourishing: Why We Need Religion in a Globalized World*. New Haven: Yale University Press.

Zuboff, Shoshana. 2019. *The Age of Surveillance Capitalism*. New York: Public Affairs.

Index

Note: Page numbers with an 'n' denote notes.

9/11 attacks 3, 4; national security surveillance after 108, 112–14, 121, 186; and security threats 244–5; *see also* terrorism

accountability 4, 109, 111, 132, 133, 244, 250, 252; democratic accountability 12, 26, 109; of foreign intelligence gathering 148; of intelligence and security functions 222; intelligent accountability 222, 224, 225, 228, 230–1, 235; mutual accountability among trustees 211, 212; and transparency 7, 23, 28, 40, 192, 252; and warrants 149, 150
Alipay 247–8
Altmeier, Peter 39
Amazon (company) 233, 254
American Civil Liberties Union (ACLU) 115–16, 234
Anderson, David 35
anocracy 226, 227, 228, 232, 235
antivaccination movement 50
Artificial Intelligence (AI) 159, 211, 212–13
authentication 209–11
authoritarianism 226, 227
authorization bodies, of bulk surveillance 151–2; G10 Commission 151; independent committee 151; independent judicial Commissioners 151; judicial oversight body 152; ministerial authorization 151; political leaders 152
automated internal compliance systems 159

Bentham, Jeremy 24, 79, 97, 245
Bezos, Jeff 254
Big Data processes 52
Binninger, Clemens 38
biometric surveillance 234–5
Black Lives Matter movement 254
Board for Special Services (KSS), Poland 135
Brennan, John 32
bulk surveillance 145–7, 161, 222; good practice compendium (*see* good practice, on bulk surveillance); methods 147–8; reforms of 161; reporting 160–1
bulk warrants 150; advantages of 150; application criteria 150–1; definition of 149–51
Bundesnachrichtendienst (BND) 21; expansion of power of 38–9; foreign embassies surveillance 37; and NSA 37; reform legislation 38, 39; surveillance activity 37–8; surveillance of officials at international organizations 37
Bush, George W. 31, 112, 115, 119
Buzek, Jerzy 135

Cambridge Analytica data scandal 4, 165, 174, 175, 254
camera surveillance 196, 246; police body cameras (bodycams) 58, 254; in Polish ambulances 195
capitalism 88–9; accumulation 85, 86–7, 92, 100; labor 86–7, 89, 90, 91–2, 93, 94, 96, 99; as an institutionalized

social order 90–1, *see also* surveillance capitalism
Central Anti-Corruption Bureau (CBA), Poland 137, 139
Central Intelligence Agency (CIA) 107, 110, 111, 116
checkpoints 65, 70–71, 73–75; monitoring, by human rights NGOs 71–73
chilling effects, of surveillance 26, 29, 49, 52, 54, 59, 61–2; amplification of 55; and arbitrariness 53; and publicization 55; of transparency 25, 26, 29, 55, 59, 251
China: COVID-19 surveillance in 244; public-private cooperation during COVID-19 pandemic 247–8; Social Credit schemes 248
Church Committee 111, 120
civil liberties 4, 145, 228, 232, 235, 236, 244, 249; abuse of 10; and biometric surveillance 234; and distrust 122; internal monitoring 122–3; organizations, and NSA 35, 115; protection of 10, 31–2, 116, 245
civil rights movement 35, 98, 100, 112, 119
Clinton, Bill 99
Coats, Dan 33, 40n6
Cold War era, national security surveillance during 110–12
colonialism 85, 89; and capitalism 89; exploitation and expropriation of labor during 93, 96; and primitive accumulation 88, 93; and racism 96; and settler colonialism 92; *see also* neocolonialism; settler colonialism
Constant, Benjamin 50
contact tracing 245, 247–9
Cooper, Yvette 49
corporate surveillance 4, 6, 14, 223, 233, 244
Council of Europe 160
counterterrorism surveillance policies 29, 30, 32, 33, 35, 186–187; of Poland 130–1; of United Kingdom 33–35, 187; of United States 30–33, 112–14, 233
Court of Justice of the European Union 148
Court of Justice of the European Union (CJEU) 129, 133
COVID-19 pandemic surveillance 4, 243; and adoption of technologies 246–7; contact-tracing 247; ethical and justice issues 247; politics of trust and transparency 246–9; as public health condition 244; public–private cooperation 247–8; remote learning 247; social transparency during 250; surveillance systems 254
cryptography 201, 209, 214

data: breach notification 209; collection 52; deletion 157–8; data doubles 169; data-driven discrimination 252; justice 250–1, 252, 254; maintenance 156; minimization 155; mishandling of 223; oversight practices in 158; processing, bulk surveillance 155–8; reciprocity 174; records of 158; sharing 157; storage 155–6; storage/retention periods 157–8
deep learning 212, 215n2
democracy: democratic accountability 12, 26; democratically authorized surveillance 59; democratic decision-making 24–5; deliberative democracy 25; democratic oversight acts 222; liberal democracies 225–7, 235, 236
Denham, Elizabeth 254
Digital Blind Trust (DBT) 212
disclosure, and transparency 32, 40; of information 22–3, 24, 25, 27; ratcheting effect 28; strategic disclosure 29
Distributed Ledger Technologies (DLTs,) 201
distrust 5, 10, 11, 12, 27, 50–51, 122, 183, 187, 191, 195, 196, 201–203; *see also* mistrust
domination: and camera surveillance 58–9; of labor 87, 90, 93; and liberty 48, 51–6, 62
Dorsey, Jack 249

eIDAS regulation 210
Ethereum 210
European Convention of Human Rights 148–9, 227
European Counter Terrorism Group (CTG) 156
European Court of Human Rights (ECHR) 129, 131, 133, 148, 161

European Decentralized Privacy-Preserving Proximity-Tracing protocol 247
European Union 58; Agency for Fundamental Rights (FRA) 129; Charter of Fundamental Rights 149; Data Retention Directive 186–7; General Data Protection Regulation (GDPR) 209

Facebook, Inc. 167–8, 170, 223, 249; advertising clients, strategy towards 175–7; Beacon 172, 173; and Cambridge Analytica (*see* Cambridge Analytica data scandal); data reciprocity 174; developers, strategy towards 173–5; end users, strategy toward 172–3; News Feed 172–3; patent on methods 168–9; reputation in US 254; users' call history data gathering 176–7
facial recognition technology 246
Federal Bureau of Investigation (FBI) 107, 110, 111, 112, 113, 116
Foreign Intelligence Agency (AW), Poland 139
Foreign Intelligence Surveillance Act (FISA) 31, 111–114, 116, 162n
Foreign Intelligence Surveillance Court (FISC) 31, 111, 113, 114–15, 119, 120
Foucault, Michel 69, 79
freedom 56–57; compared with negative liberty 51, 56; limits of 57; as nondomination 47, 48, 51–2, 55, 56, 61; republican 61–2; *see also* liberty
Fulford, Adrian 35

G10 Commission 151
Germany: Alternative for Germany (AfD) 229, 230; Basic Law 227, 228; BND (*see* Bundesnachrichtendienst (BND)); Federal Office for the Protection of the Constitution (BfV) 228, 230; foreign intelligence agency 166; Independent Control Council 39; Nordkreuz 230; oversight of intelligence and law enforcement agencies 228–30; Social Democratic Party (SPD) 229; surveillance law reform 29, 36–39; and United States 29, 36–7
good practice, on bulk surveillance 148–61; analysis 158–9; application process 149–51; authorization/approval 151–3; collection 153–4; data processing 155–8; filtering 154–5; of foreign communications 147; reporting 160–1; review and evaluation 159–60; strategic planning 148–9
Google 223, 252, 254
Google–Apple API, for contact tracing 247
Government Communications Headquarters (GCHQ) 21, 33, 47, 155, 158

herding behavior 25, 212
High-Level Expert Group on Artificial Intelligence (AI-HLEG) 212–13
human flourishing 245–6, 250, 251–3
human rights 9, 65, 69–79, 127, 129, 136, 138, 221, 222, 223, 227–8, 232, 235, 236
Husband, Charles 187

imposed transparency 65, 80; COVID-19 pandemic surveillance 248–9; cycles of 68; dynamics of 68–69; meaning and significance of 66–67; in Occupied Palestinian Territories (OPT) 69–70, 75–79; *see also* West Bank
India, COVID-19 surveillance in 244
Information and Communication Technologies (ICT) 201, 207
internet 254–5; illegal internet activity 54; limits of free inquiry on 52; online activities 254–6
Internet of Things (IoT) 207
Investigative Case Management (ICM) platform 233
Investigatory Powers Act (IPA) 33–6, 48, 150
Israeli NGOs 69, 71–72, 75, 76, 77, 79

Javid, Sajid 35
Jim Crow laws 95–6

key signing 210

liberty: and distrust 50–1; reduction of 26, 51–2; under surveillance 62–3; negative liberty 55; compared with

freedom as nondomination 51, 56; *see also* freedom
Liberty (civil rights organization) 35–6
Lübcke, Walter 230

Maaßen, Hans-Georg 228–9
machines: machine learning 52, 212; trustworthiness of 207–8
Marx, Karl 86, 87, 90, 92
Massive Volume Reduction (MVR) systems 155
mass surveillance, *see* surveillance
McConnell, Mitch 32
Merkel, Angela 36, 229
MERS pandemic 248
metadata collection: in Poland 131, 132; in United States 31, 114–16
Mexico, trustworthiness of government in 248
MI5 35
Microsoft 254
militant democracies 222, 224–8, 235–6; in Germany 228–30; lessons for and from 235; in Poland 230–2; in United States 232–5
mistrust 59–60, 146, 224, 248; *see also* distrust
Morawiecki, Mateusz 232
multifactor authentication 210
multi-sided markets 165, 167, 171, 173, 175, 177

Nakamoto, Satoshi 201
National Institute of Standards and Technology 210
National Security Agency (NSA), US 21, 30, 36, 107, 110–16, 120; and BND 37; call detail record program 32–3; and GCHQ 33; phone tapping accusation 36–7; PRISM surveillance program 31; surveillance programs 165; warrantless wiretapping 31; XKeyscore system 158
national security surveillance, 4, 7, 12, 13; United States 30–33, 107–9; UK 34–36; Cold War era 110–12; constitutionality of 107, 109, 114, 115, 118, 119, 120; and executive branch 107–8, 110, 111–12, 113, 115, 117–18, 119, 122; and judicial branch 108, 115, 116, 119, 120, 121; and legislative branch 117, 120–1; legislative reform 114–15, 116–17; secrecy of 108, 109, 110, 111–13, 117–19, 121; state of emergency 110, 112, 118, 119, 122; transparency of 109, 110, 111, 113–14, 115, 116, 118, 119, 120–3
neocolonialism 85, 89, 96, 100; *see also* colonialism; settler colonialism
neo-republicanism 47–63
network effects 167, 170, 172, 173, 175, 178n4
non-governmental organizations (NGOs) 136, 137; NGO Monitor project 77, 78; and transparency 69
NSO Group 231–2

Obama, Barack 30, 31, 113–14, 115
Occupied Palestinian Territories (OPT): imposed transparency in 69–70; and NGOs 75
oversight surveillance policies and practices 224; in Germany 38, 228–30; in Poland 230–2; and republican nondomination 60; in United States 31–32, 120, 232–5

Palantir Technologies 233
Palestinian human rights 71, 75–77, 77–79
panoptic gaze 69, 79
Panoptykon Foundation x, 137, 232
Patriot Act 30, 31, 112, 113, 114, 116, 119
Pegasus surveillance malware 231–2
PGP encryption system 210, 215n6
Pichai, Sundar 254
Pike Committee 111, 120
Poland 127–8; Anti-terrorism Law 130–1; Central Anti-Corruption Bureau (CBA) Act 136, 139; Civic Platform (PO) 129, 232; Code of Criminal Proceedings, amendment of 130; Commissioner for Human Rights (RPO) 129, 138; Constitutional Tribunal 128, 129–30, 138–40; and European Commission 231; Government Protection Bureau (BOR) 131; Internal Oversight Inspector (BNW) 131–2, 134; Internal Security Agency (ABW) 130–1, 137, 139, 140; Law and Justice party (PiS) 129, 134, 230, 231; Law on the Prosecutor's Office 130, 134;

legal framework after 2013 128–33; Minister of Internal Affairs 131–2; National Revenue Administration (KAS) 131; National Security Services (SOP) 131; Pegasus surveillance malware 231–2; Sejm Committee for Special Services (SKSS) 135–6; Surveillance Act of 2016 129–30, 137, 140; surveillance of healthcare system 187; and transparency 129; and UN 231
Polanyi, Karl 87, 89–90
police body cameras (bodycams) 58, 254, *see also* camera surveillance
Polish People's Party (PSL) 129
predictive oversight 154
PRISMS survey 185
privacy 4, 6, 14n, 21; policies 208–9; protections 154–159; and security 225; in social media 168, 173; versus surveillance 30, 31, 34, 36, 52, 54, 133, 137, 145, 149, 183–4; and US national security surveillance 107, 115, 116, 118
Privacy International 149
Public Key Infrastructure (PKI) 210, 215n6, 215n7

quantum computing 211

racializing surveillance 96, 100–1; definition of 85; in United States 92–6
Rawls, John 25
risk: and transparency 50; and trust 50

Sasin, Jacek 232
Schindler, Gerhard 39
secrecy: and surveillance 4, 21, 23–25, 127, 128–134; and transparency 7, 107, 108, 111, 136, 137; of US national security surveillance 108, 109, 110, 111–13, 117–19, 121
security: and privacy 225; as a public good 212; security engineering 208; *see also* national security surveillance
Seehofer, Horst 229
self-censorship 29, 51, 55, 59
Sensburg, Patrick 39
settler colonialism 85, 100; and colonialism, distinction between 92–3; and racializing surveillance 92–6; *see also* colonialism; neocolonialism
Shin Bet 248–9
signals intelligence (SIGINT): bulk warrants 153; nontargeted 147–8
slavery 93–5; Roman slave 51
Snapchat 168
Snowden revelations 4, 22, 54–55, 107, 221, 235, 254; and bulk surveillance reform 145, 146, 161; and democratic mistrust 60; and global surveillance 221, 222, 223, 235; impact in Germany 21, 29–30, 36–9, 166; impact in Poland 127–8, 132, 133, 139; impact in UK 21, 29–30, 33–6; impact in US 21, 29–33, 32, 114–17, 118, 120, 122–3; impact on intelligence functions 222; legitimization and normalization of surveillance after 21; transparency proposals and public trust after 48–51
social media/social media platforms 165, 177–8, 249, 255; advertising clients, strategy towards 175–7; concentration in markets for 168–71; developers, strategy towards 173–5; digital platforms 208, 253–4; economic aspects 167–8; end users, strategy towards 172–3; multisided market strategy 171–7; network effects 172; supply side 169–70, 172
social sorting, surveillance as 58, 62, 85, 100, 101, 249
South Africa, apartheid-era 54
South Korea, trust and transparency during COVID-19 pandemic 248
Stellar Wind program 112
Supreme Audit Office (NIK), Poland 129, 138
surveillance 3–5, 127, 243; as authorized interference 57; by Bundesnachrichtendienst (BND) 36–8; and conforming behaviors production 59; and criminal proceedings 130, 131; dangers and risks of 4; definition of 108, 221; and democracy 50, 121; enabling versus regulating 21–2; and freedom as nondomination 51–2; global culture of 221; and inequality 59–60, 62, 249–50; legitimization of 28, 33–4; mass surveillance 51, 224; normalization of 28; NSA's PRISM program 31; overreach 253; positive attitudes to 185–6; publicization of 47; public responsiveness to concerns

of 40; racializing surveillance (*see* racializing surveillance); secrecy of (*see* secrecy); and social media 168–171; as social sorting 85, 100, 101, 249; and transparency 11–13, 26, 47–50, 108–110, 166–7, 222–4; and trust (*see* trust); United States government 107–23; welfare surveillance 97–100
surveillance capitalism 3, 167, 177, 223, 244, 247, 249, 252, 255

telecommunications companies: bulk data collection by 153; collection of data from 114–15
Temporary Assistance for Needy Families (TANF), US 98, 99, 100
terrorism: 9/11 attacks 112–14, 244–5; Anti-terrorism Law (Poland) 130–1; counterterrorism surveillance policies 186; and US national security surveillance 112–14, 119, 121; *see also* counterterrorism surveillance policies
Terrorist Surveillance Program (TSP) 112
transparency 5, 6–8; 22-30, 38-40, 66–68, 108, 127, 128, 224; aesthetics of 8; as an inherent normative good 23–4; beneficial effects 22; chilling effects 25, 26, 29; as a condition for trust 26–7; as disclosure 40; effects on deliberation 25; forced 69; and Framers 122; hierarchical structure of 48, 55–7; horizontal structure of 59–62; imposed and voluntary 248–9; an information 24–25; logics of 23–7; and legislation 77–79; and legitimacy 24–25; as monitoring 26; and platforms 250; policies 122–3; procedural transparency 53–4, 56; and public trust 26–7; regulations 47, 57; and relations of power 27–8; and risk 50; and secrecy 107, 108, 111, 121, 127, 132–4, 136, 137; sociological understanding of 249–51; and surveillance 11–13, 26, 47–50, 108–110, 166–7, 222–4; transparency trap 22, 29–30; and trust (*see* trust); types of 66–68; of US national security surveillance 31–33, 109, 110, 111, 113–16, 118, 119, 120–3
Truman, Harry 110
Trump, Donald 33, 116, 234
trust 5, 8–11, 47–51, 183–4; as care 203–6, 211, 214, 253; constructive lack of 59–60, 224–8; as control 202–3, 206, 213, 253; crisis of 223; definitions 203, 204; as dependability 213–14; emergence of 188–91; generalized trust 187–8, 189; and governance 5, 9, 26, 248; institutionalist theories of 183, 185, 189–93, 196; and norms 190, 193–4, 203; particular trust 186–8, 189, 190–1, 193, 194–5; performance-based approach to 192, 193; and the public 145, 160; rationalist paradigm of trust 202–3, 205; and risk 50; social trust 49–50, 185; sociological understanding of 249–50; sociocultural theory on 190–1, 193–5, 196; and surveillance 9, 183, 185–8, 195–6, 235; surveys on 223; and transparency 5, 6–10, 26–7, 47, 48–51, 192–3, 222–4; trustee–trustor relationship 202, 203–6, 211, 214; *see also* distrust, mistrust
trusted computing base (TCB) 207–8
trustworthiness: and dependability, difference between 206–8; of government 248; of trustees 211, 213–14
Twitter 249

United Kingdom: bulk equipment interference warrants 34–5; civil liberty organizations challenges to IPA 35–6; counterterrorism policies 187; equipment interference 34; Government Communications Headquarters (GCHQ) 21, 33, 35, 155; intelligence agencies 34–5; Intelligence and Security Committee of Parliament 48–9; Investigatory Powers Act (IPA) 33–6, 48, 150; legitimization of surveillance powers 33–4; MI5 35; Poor Law Amendment Act 1834 97
United States: Black Codes 95; bulk warrants in 150; call detail record program 32–3; colonialism 85, 93; Congress 108–14, 116–21; counterterrorism policies 31–32, 112–14, 233; Customs and Border Protection (CBP) 234; Department

of Homeland Security Fusion Centers 187; DHS whistleblowing 233–4; executive branch of 107–8, 110, 111–12, 113, 115, 117–18, 119, 122; FISA Amendments Act (2008) 31–2, 113, 114; Foreign Intelligence Surveillance Act (FISA) 31, 111, 114, 116; Fourth Amendment 116; Framers 122; Freedmen's Bureau 95; Freedom Act (2015) 114–15, 116; Fugitive Slave Act of 1850 95; and Germany 29, 36–7; Great Society programs 98; intelligence agencies, and Yahoo 153; intelligence community 32–3; judicial branch of 108, 115, 116, 119, 120, 121; legislative branch of 117, 120–1; migration policies 233; National Security Act 110; National Security Agency (NSA) (*see* National Security Agency (NSA), US); National Security Letters (NSL) 112, 114; national security surveillance 107–23; welfare surveillance 96–100; Office of Legal Counsel (OLC) 112; oversight of governmental agencies and outsourcing 232–5; Patriot Act 30, 31, 112, 113, 114, 116, 119; Personal Responsibility and Work Opportunity Act (PRWOA) 99; police monitoring of Muslim communities post-9/11 187; President's Review Groupon Intelligence and Communications Technologies 30; PRISM program 113, 114; Privacy and Civil Liberties Oversight Board (PCLOB) 30, 114, 115, 120; Protect America Act (2007) 113; racializing surveillance in 92–6; Review Group on Intelligence and Communications Technology 114; separation of powers doctrine 108, 109, 110, 111, 117, 119, 122, 123; settler colonial expropriation of land 92; Supreme Court 112, 115, 119, 121; telephone metadata collection program 31; Temporary Assistance for Needy Families (TANF) 98, 99, 100; USA Freedom Act (2015) 30–3; Vesting Clause 117–18
Universal Declaration of Human Rights (UDHR) 227
USA Freedom Act 30–32, 114–116

veillance 221
Venice Commission 129, 133
voluntary transparency: COVID-19 pandemic surveillance 248–9; universal application of 67
Voßhoff, Andrea 37–8

war on terror 3; *see also* counterterrorism surveillance policies
Weibo 248
West Bank: checkpoints deployment at 70–71; checkpoints monitoring by human rights NGOs at 71–73; indoor checkpoints at 73–75
whistleblowing/whistleblowers 4, 31–2, 38, 225

XKeyscore system (NSA) 158

Yahoo, and US intelligence agencies 153

zero-day attacks 215n2
Zuckerberg, Mark 173–4, 249, 254