UNIVERSITY OF AMSTERDAM

UvA-DARE (Digital Academic Repository)

Through a glass, darkly: Everyday acts of authoritarianism and surveillance cultures in the West

Hintz, A.; Milan, S.

Publication date
2018
Document Version
Final published version
Published in
International Journal of Communication : IJoC
License
CC BY-NC-ND

Link to publication

Citation for published version (APA):
Hintz, A., & Milan, S. (2018). Through a glass, darkly: Everyday acts of authoritarianism and surveillance cultures in the West. *International Journal of Communication : IJoC*, *12*, 3939–3959. https://ijoc.org/index.php/ijoc/article/view/8537/2466

General rights
It is not permitted to download or to forward/distribute the text or part of it without the consent of the author(s) and/or copyright holder(s), other than for strictly personal, individual use, unless the work is under an open content license (like Creative Commons).

Disclaimer/Complaints regulations
If you believe that digital publication of certain material infringes any of your rights or (privacy) interests, please let the Library know, stating your reasons. In case of a legitimate complaint, the Library will make the material inaccessible and/or remove it from the website. Please Ask the Library: https://uba.uva.nl/en/contact, or a letter to: Library of the University of Amsterdam, Secretariat, Singel 425, 1012 WP Amsterdam, The Netherlands. You will be contacted as soon as possible.

UvA-DARE is a service provided by the library of the University of Amsterdam (https://dare.uva.nl)

Download date:06 May 2021

International Journal of Communication 12(2018), 3939–3959 1932–8036/20180005

"Through a Glass, Darkly": Everyday Acts of Authoritarianism in the Liberal West[1]

ARNE HINTZ
Cardiff University, UK

STEFANIA MILAN
University of Amsterdam, The Netherlands

Institutional practices undermining citizen agency and infringing on individual freedoms are typically associated with authoritarian countries. However, they are also proliferating in Western democracies. This article redefines data-based surveillance as a "Western" authoritarian and illiberal practice in the digital realm, resulting from state–industry collaboration and alienated from accountability mechanisms. Straddling critical data studies and surveillance studies, the article explores these dynamics of surveillance in the West by focusing on two dimensions: the institutionalization of governmental practices in law and the societal normalization of surveillance in popular cultural practices. It thus investigates the renegotiation of the boundaries of state power along two axes—top down and bottom up. It connects the notions of "authoritarian and illiberal practices" and "surveillance cultures," asking how the former are produced, negotiated, and legitimized and reviewing their consequences for citizens and civil society. Based on empirical data from two projects exploring the interplay between citizenship and surveillance, the article argues that acts of authoritarianism in the West are institutionalized at the intersection of top-down governmental practices and bottom-up popular reactions.

Keywords: authoritarian practices, surveillance, surveillance cultures, liberal democracy, Internet freedoms

Some countries have erected electronic barriers that prevent their people from accessing portions of the world's networks. They've expunged words, names, and phrases from search engine results. They have violated the privacy of citizens who engage in non-violent

[1] "Through a glass, darkly" refers to a biblical passage from the New Testament (1 Corinthians 13:12) that can be translated as, "Now we see but a poor reflection as in a mirror." It is also the title of a 2006 novel by crime writer Donna Leon, where the hero investigates the entities literally "muddying the waters" of the Venice lagoon.

Arne Hintz: hintza@cardiff.ac.uk
Stefania Milan: S.Milan@uva.nl
Date submitted: 2017–12–07

Copyright © 2018 (Arne Hintz and Stefania Milan). Licensed under the Creative Commons Attribution Non-commercial No Derivatives (by-nc-nd). Available at http://ijoc.org.

> political speech. These actions contravene the Universal Declaration on Human Rights, which tells us that all people have the right "to seek, receive and impart information and ideas through any media and regardless of frontiers." With the spread of these restrictive practices, a new information curtain is descending across much of the world. (Clinton, 2010, p. 4)

As this quote by then–U.S. Secretary of State Hillary Clinton illustrates, institutional practices that undermine citizen agency and limit political pluralism are often associated with authoritarian countries. In literature, authoritarianism has been connected to centralized power structures, a lack of accountability of the state to its citizens, and repression of political dissidence (Linz, 1964). Authoritarian regimes are typically associated with political systems that differ from Western forms of democracy: In her famous speech on Internet freedoms, Clinton explicitly referred to government policies and regulatory acts in, among others, Iran, China, Vietnam, North Korea, and Egypt. However, "authoritarian practices" targeting citizens by "disabling their access to information and/or disabling their voice" (Glasius, 2018, p. 527) are increasingly observed in the professed democratic countries of the West. This is particularly visible in the area that Clinton focused on to draw new demarcation lines between a democratic and an authoritarian world: Internet freedoms, namely, the broad range of human rights as they apply to the digital, such as free expression, association, assembly, and privacy online (Freedom Online Coalition, n.d.). Although surveillance and censorship have long existed in democratic states, the inadequacy of distinguishing between a free and a nonfree world on the Internet became particularly apparent with the Snowden leaks, which demonstrated the pervasive monitoring of data traces by the U.S. and UK security agencies. The revelations uncovered not just the widespread interception of data traffic but also operations targeted against democratic institutions and civil society organizations that included hacking servers, reducing technological security, and spreading misinformation (Greenwald, 2014).

We follow Glasius (2018) in changing the perspective from "classic" authoritarian regimes to authoritarian practices as we analyze surveillance as both authoritarian and illiberal practice of and in the democratic West. We connect this notion to that of "surveillance culture" (Lyon, 2017), asking how the "active practice[s] of disrupting or sabotaging accountability" (Glasius, 2018, p. 521) emerging in the West are produced, negotiated, and legitimized. More specifically, the article advances the claim that the authoritarian dimension of surveillance is institutionalized at the intersection of two dynamics: (a) the top-down dynamic of policy reform that followed the Snowden revelations and enables wider data collection and analysis by state agencies, empowering the state at the expense of civic rights, and (b) the bottom-up dynamic of public responses to massive data collection that have facilitated the normalization of surveillance and the consolidation of a surveillance culture while harboring emerging resistance tactics. To this end, we bring the disciplines of surveillance studies and critical data studies into a dialogue with emerging work on authoritarian practices within international relations. This notion, we argue, allows us to interpret the turn to blanket surveillance in Western democracies, exploring the ongoing (re)negotiation of the boundaries of state power. Our goal is to offer both empirical grounding and conceptual development in the context of an emerging critique of simplistic distinctions between an allegedly free and democratic world and a sphere of authoritarian regimes. Our focus is on Internet freedoms as the thematic field where such distinctions have been promoted most prominently over the past decade.

The article is based on findings from two multiyear research projects that have addressed Internet surveillance and massive data collection in liberal democracies in the European Union and the Americas. It is organized as follows. First, we illustrate the historical trajectory of digital freedoms and restrictions, elucidate the conceptual tenets of the article, and describe our data sets. Next, we take the top-down perspective, exploring the making of surveillance policies in the West with a focus on the accountability of states toward their citizens. We then analyze authoritarian practices from a bottom-up perspective, surveying both the public resignation that followed the normalization of surveillance and emerging tactics of resistance. We conclude by bringing our findings to bear on the notion of authoritarian practices, reflecting on advantages and challenges of transposing this concept to liberal democracies.

Exploring Authoritarian Practices in the Digital Realm

Digital Freedoms and Restrictions: A Rapidly Shifting Landscape

"Governments of the Industrial World, you weary giants of flesh and steel . . . leave us alone," cyberlibertarian activist John Perry Barlow (1996, para. 1) famously proclaimed in *A Declaration of the Independence of Cyberspace*. With many of its key protocols developed outside established institutions and with the goal to facilitate end-to-end communication, the decentralized design of the Internet promised enhanced interaction between individuals and challenged the influence of traditional forms of authority (cf. Abbate, 1999). Creating "a world where anyone, anywhere may express his or her beliefs, no matter how singular, without fear of being coerced into silence or conformity," the Internet was hoped to represent a "citizen-designed, citizen-controlled worldwide communications network" able to "revitalize the public sphere" (Rheingold, 1993, pp. 14–15). On and through this new infrastructure, "the people formerly known as the audience" (Rosen, 2006, para. 1) could create and share their own content, increasingly without expert mediation. As a space of interaction, the Internet generated new forms of networked, collaborative and participatory production (Benkler, 2006) and lowered the costs of association and organization (Shirky, 2008). It also helped advance new understandings of digital citizenship based on people's self-enactment of their role in society through digital acts (Isin & Ruppert, 2015; Mossberger, Tolbert, & McNeal, 2007).

However, the supposedly empowering features of the Internet have been progressively met by the expansion of the influence of both state and corporations, which have sought control over cyberspace (Deibert, 2013; Goldsmith & Wu, 2006). Internet regulation, censorship, and state cyberpolicing capacities have increased significantly (Nye, 2011). These restrictions have included the virtual separation of national networks from the transnational Internet and, thus, the demarcation of virtual national borders, as in the case of the Great Firewall of China (Deibert, Palfrey, Rohozinski, & Zittrain, 2008, 2011). During times of protests and uprisings, governments are now routinely closing down online services or interrupting connections to the outside world. The Shutdown Tracker Optimization Project has documented Internet shutdowns in 30 countries from January 2016 to September 2017 (Access Now, 2017; see also Freyburg & Garbe, 2018; Wagner, 2018). Often "the targets (victims) are active domestic civic society movements" (Howard, Agarwal, & Hussain, 2011, p. 220). Within national borders, filtering and blocking content that transcends moral, religious, or political limits set by governments or religious authorities have become common practice. Some of this was pioneered by governments in the Middle East and Asia, but Western countries have rapidly expanded their censorship and surveillance capacities (Deibert et al., 2008).

FinFisher, commercial software used to secretly access the machines of suspected criminals to steal passwords and record conversations, has been located in countries as diverse as Canada, the Netherlands, the United Kingdom, Germany, India, Bahrain, Vietnam, Turkmenistan, and the United States, among others (Marquis-Boire, Marczak, Guarnieri, & Scott-Railton, 2013). Meanwhile, the creation of an extensive censorship architecture for accepted forms of content restrictions (e.g., blocking child pornography) serves also the purpose of normalizing the practice of wider restrictions. But "once the tools of censorship are in place, the temptation for authorities to employ them for a wide range of purposes are large" (Deibert, 2009, p. 327).

As private entities are enlisted to implement content restrictions and surveillance and set their own rules on core issues of freedom of expression, we observe "a shift of the responsibility for monitoring and policing Internet conduct onto strategically positioned private sector intermediaries" (Mueller, 2010, p. 149). With social media platforms mediating people's access to the digital public sphere, such intermediaries become gatekeepers and take on the role of regulators. State policy is thus complemented by the privatization of policy, or private ordering (Hintz, 2016). This interaction is particularly prevalent in the area of surveillance, where states use the "data mine" (Andrejevic, 2012) of online platforms, as the Snowden leaks demonstrated, to develop detailed knowledge about their citizens, for example, by tracking the vast pool of data generated through social media platforms for "open source intelligence" operations (Trottier, 2015). As a consequence, chilling effects on online speech, whereby surveillance deters people from engaging in legal (or even desirable) online activities because they fear punishment or criminal sanction and do not trust the legal system to protect their innocence (Penney, 2016), have been observed. As we shall see, these chilling effects undermine critical debate and dissenting voices (Hampton et al., 2014).

Learning From Surveillance Studies and Critical Data Studies

Two interdisciplinary fields of inquiry, surveillance studies and critical data studies, help us to interpret these developments. Surveillance studies has documented how "all manner of everyday activities are recorded, checked, traced and monitored" (Lyon, 2007, p. 454). Theoretical approaches to surveillance have been heavily influenced by classic concepts such as Bentham's (1843) panopticon, emphasizing the role and position of the watchful eye of an authority, thus stressing the hierarchical relationship of power between the agents and objects of surveillance, whereas other (and often more recent) understandings of surveillance have incorporated the active role of those surveilled in complex processes of "veillance" (Bakir, 2015). As Bauman and Lyon (2012) noted:

> Much of the personal information vacuumed so vigorously by organizations is actually made available by people using their cell phones, shopping in malls, travelling on vacation, being entertained or surfing the internet. We swipe our cards, repeat our postcodes and show our ID routinely, automatically, willingly. (p. 12)

Meanwhile, the rise of what has been termed "surveillance capitalism" (Zuboff, 2015) has been accompanied by pervasive logics of data accumulation promoting the collapse of previously disassociated data contexts—with ever-newer threats to citizen privacy.

Lyon (2017) has conceptualized this notion as the rise of a *surveillance culture,* whereby surveillance "is no longer merely something external that impinges on our lives. It is something that everyday citizens comply with—willingly and wittingly, or not—negotiate, resist, engage with, and, in novel ways, even initiate and desire" (p. 825). Such culture manifests itself in corresponding social imaginaries, or shared understandings and normative commitments "constructed through everyday involvement with surveillance as well as from new reports and popular media" (p. 829). Surveillance technologies have not just proliferated; they have become fully embedded in everyday practices and "in the norms and institutions of society" (Murakami Wood & Webster, 2009, p. 264). The use of digital devices, and the mere physical existence in heavily digitized spaces such as smart cities, inevitably lead to the generation of data by citizens and thus to the—sometimes active and willing, sometimes passive and unaware—participation of people in surveillance regimes, what Albrechtslund (2008) has referred to as "participatory surveillance." The distributed and often opaque nature of contemporary "surveillance assemblages" (Haggerty & Ericson, 2000) makes it difficult to "pinpoint the locus of responsibility for surveillance processes" (Lyon, Haggerty, & Ball, 2012, p. 9).

Our understanding of the norms and implications of contemporary forms of surveillance have been further enhanced through the interdisciplinary field of critical data studies, engaging more specifically with the rise of big data and the associated algorithmic processes (cf. Dalton & Thatcher, 2014). Scholars have explored emerging "data assemblages" (Kitchin & Lauriault, 2015), developing a critical perspective on how the epistemological and ontological implications of data-driven processes may (re)constitute both knowledge and subjectivity and, in the process, democracy and the society at large (e.g., Baym, 2013; boyd & Crawford, 2012). Emphasis has been put on the role of private actors in promoting the monitoring of the citizenry, investigating the "politics of" algorithms and platforms (Gillespie, 2014) and the subtending logics prompting people to engage in predetermined actions such as sharing (van Dijck & Poell, 2013). The use of data for surveillance purposes, or "dataveillance," has been recognized as an intrinsic component of today's "culture of connectivity" (van Dijck, 2013). Corporate and government bodies alike turn citizens into data doubles that enable social sorting and alter access to resources and life chances (Lyon, 2014; van Dijck, 2014) and can produce inequality and discrimination (Gangadharan, 2012; Noble, 2018).

Scholars have explored how novel subjectivities and "data publics" (Ruppert, 2015) are co-constituted in interaction with algorithmic modes of control (Cheney-Lippold, 2011). Yet, although a "Big Data divide" (Andrejevic, 2014) exists between the "surveillance-industrial complex" (Ball & Snider, 2013) and citizens as the objects of surveillance, people have also reclaimed agency and carved out spaces to engage in resistance and creative subversion of massive data collection (Couldry & Powell, 2014; Milan, 2018). These vary from "reactive" tactics, such as the adoption of encryption and anonymization tools as technical solutions to widespread surveillance, to "proactive" approaches such as "sousveillance," or the turning of surveillance against the surveillant (Milan & van der Velden, 2016; cf. Mann, Nolan, & Wellman, 2003).

Citizen Monitoring and Dataveillance as Authoritarian Practices

The notions of authoritarian and illiberal practices offer a fruitful lens through which to reflect on the role of the state in today's dataveillance. Traditionally, authoritarianism has been attributed a systemic character, with the literature emphasizing the role of a central authority within defined geographic

boundaries (Linz, 1964), but focusing on practices allows for the necessary flexibility. Authoritarian practices are patterns of action oriented to incapacitate citizens' access to information, "through filtering, misinformation, and secrecy that is not exceptional and not bound by procedure," or to voice, "through censorship, intimidation or punishment" (Glasius & Michaelsen, 2018, this Special Section). They alter "the relationship between the actor and the forum" and are made possible by "public-private authoritarian partnerships" (Glasius, 2018, pp. 517–521) whereby state agencies obtain user data from telecommunication companies—with or without court warrant (see, e.g., Parsons, 2014). They are typically justified with reasons of national security, therefore kept hidden from the public scrutiny and alienated from traditional accountability mechanisms. Furthermore, Glasius and Michaelsen (2018) distinguish between "authoritarian practices," which are marked by secrecy and the sabotage of accountability, and "illiberal practices," which infringe on the protection of the autonomy and dignity of a person. As we will discuss, both aspects can be observed in the institutionalization of surveillance through top-down and bottom-up dynamics.

Using the notions of authoritarian and illiberal practices to interpret the diffused character of surveillance in Western democracies and its effects on the state–citizens relation is useful for at least three reasons. First, they allow us to "go beyond a single-state context and recognize such phenomena as transnational illiberalism or public-private authoritarian partnerships" (Glasius, 2018, p. 517). As exemplified by PRISM, the surveillance program revealed by Snowden and empowering the U.S. National Security Agency (NSA) to collect Internet traffic data from companies such as Google, these practices are often based on public–private cooperation. Second, the notion allows us to stress the "organizational and social context" (p. 524) in which these practices are embedded. Third, the concept evokes the severe consequences that disabling access to information or voice might have on citizens, as "authoritarian practices enable domination: they entail substantive and procedural rule-breaking, interfere with the preferences and inhibit the civic virtues of those to whom accountability is owed, and strictly control information flows" (p. 525).

The engagement with surveillance as authoritarian and illiberal practice is embedded, moreover, in a broader social science literature that has addressed the implications of surveillance and data analytics for national and transnational politics and for state–citizen relations. Scholars of international relations and security studies, for example, have explored the societal consequences of the transformation of Internet users into suspects in the context of big data surveillance (Bauman et al., 2014) and the paradigm of preemption that is advanced through the digital mode of prediction (Aradau & Blanke, 2017). Similarly, recent works on digital citizenship have investigated the implications of pervasive surveillance for citizen agency and state–citizen power shifts (Hintz, Dencik, & Wahl-Jorgensen, 2018; Isin & Ruppert, 2015).

The Data Sets

This article draws from empirical data gathered in the context of two interdisciplinary projects. The first, "Digital Citizenship and Surveillance Society: UK State-Media-Citizen Relations After the Snowden

Leaks" (Cardiff University, 2014–16),[2] analyzed the implications of the Snowden leaks across the four thematic areas of technology, policy, news media, and civil society. Focusing on the United Kingdom as one of the countries most implicated in the Snowden revelations, the researchers investigated the role of technical infrastructures and standards, reforms in the legal and regulatory framework of surveillance, the media coverage of the leaks, and public knowledge and attitudes about surveillance. The research involved a combination of qualitative and quantitative methods, including policy document analysis, focus groups with a cross-section of the British public, media content analysis, and more than 40 expert interviews with policy makers, industry representatives, digital rights activists, and other relevant stakeholders. Here, we draw particularly from 24 expert interviews and 10 focus groups that addressed the policy environment of and popular reactions to surveillance.[3] The second project, "Data Activism: The Politics of Big Data According to Civil Society" (DATACTIVE; University of Amsterdam, 2015–20), explores citizens' engagement with datafication and massive data collection, with a focus on the organized civil society.[4] To date, researchers have interviewed more than 120 digital rights activists, human rights defenders, and software developers from European countries and the Americas in view of understanding how users with varying degrees of tech expertise engage with datafication and how citizen participation is being reformatted as a consequence of blanket surveillance. This article draws from a subset of interviews conducted at digital rights events in Europe.

In what follows, we use findings from these projects to underpin a discussion of two dimensions of surveillance as authoritarian and illiberal practice: state policy and public responses. We do not suggest that surveillance today is fully captured by this dichotomy, but it uncovers processes and interactions that help us understand the particular configuration of authoritarian and illiberal practices in the West. Recognizing the multiple dynamics of data assemblages and dataveillance, we zoom in on these two perspectives to identify specific dimensions that entrench and institutionalize authoritarian and illiberal practices in the digital realm.

Authoritarian Practices, Top Down: State Surveillance and Policy

The Snowden revelations, leaking (from June 2013 onward) classified information about government surveillance programs, represented a significant historical juncture in many respects. They demonstrated the almost limitless capabilities of intelligence services to track, record, and analyze people's online interactions, thereby changing our understanding of the Internet and, arguably, digital citizenship (Hintz et al., 2018). They also contributed to altering an international discourse that had merely focused on restrictions to online communication by authoritarian states, mostly on the Asian continent, as seen in Clinton's milestone address, while the activities of institutions such as the NSA and the UK Government Communications Headquarters (GCHQ) had received less scrutiny, or at least faced less open criticism. Their

[2] See http://www.dcssproject.net/. Research results have been published in a Special Issue of the *International Journal of Communication* (Hintz, Dencik, & Wahl-Jorgensen, 2017).

[3] Findings have been summarized by Hintz and Brown (2017) and Dencik and Cable (2017).

[4] See https://data-activism.net/. The project has received funding from the European Research Council (ERC) under the European Union's Horizon 2020 research and innovation program (grant agreement No. 639379-DATACTIVE).

role was eventually put into question as leading global media organizations such as *The Guardian*, *Der Spiegel*, and *The New York Times* began to publish detailed accounts of the extensive surveillance programs affecting Western democracies. They showed how security agencies in democratic states harvest data from the Internet's backbone cables (through programs such as Tempora and Upstream), collect messages and user geolocations (through programs such as Dishfire and Co-traveller), analyze data troves (with tools such as Xkeyscore), break encryption, weaken the security of software products, and hack into telecommunications services (Greenwald, 2014). In the aftermath of the Snowden leaks, the organization Reporters Without Borders (2014) named the NSA and GCHQ among the main "enemies of the Internet" and GCHQ as the "world champions of surveillance," highlighting "the schizophrenic attitude towards online freedoms that prevails in some countries," singling out "democracies that have traditionally claimed to respect fundamental freedoms" (para. 1).

Beyond exposing state agencies, the Snowden leaks uncovered the role of the industry, and social media platforms in particular, in the surveillance machine, showing how the comprehensive state access to personal data has been facilitated through public–private partnerships often handled in secrecy. Security agencies have been shown to collect data from the servers of large Internet companies such as Google, Facebook, Apple, and Yahoo—with or without their consent (see programs such as Prism, Muscular, and Squeaky Dolphin)—which was made possible by the data-oriented business model of social media corporations and other platforms (Trottier & Lyon, 2012).

The Snowden leaks brought to the forefront of public debate the question of the accountability of state institutions toward their citizens—or the break thereof (cf. Glasius, 2018). Following Glasius and Michaelsen (2018), the dataveillance schemes described above can be understood as illiberal practice by state powers resulting in consistent "infringements on individual autonomy and dignity" (this Special Section). The secrecy surrounding them and the lack of public accountability, meanwhile, point to their authoritarian characteristics. An example here may be the U.S. Foreign Intelligence Surveillance Court, which operates in closed hearings, withholds its records from the public, and does not have the affected parties represented in court (Greenwald, 2013). Of particular relevance, then, is the legal and regulatory environment that might provide both safeguards against governmental overreach and transparency of surveillance powers and offer citizens the opportunity to affect policy reform. And indeed, the turmoil that followed the leaks triggered official review processes in several countries and generated pressure toward policy reform. Some countries implemented partial but promising policy changes. The Brazilian Marco Civil da Internet of 2014 provided stronger protection of citizens' privacy and anonymity online (Medeiros & Bygrave, 2015), and the EU General Data Protection Regulation of 2018 expanded the protection of citizens' personal data, for example, by limiting the use and sharing of personal data by companies and mandating data protection by design (Mayer-Schoenberger & Padova, 2016). However, most countries, rather than pushing back on state powers, have extended the legal use of surveillance capabilities by state agencies. New laws to strengthen surveillance powers were adopted in France (2015), Germany (2017), Denmark (2017), and the Netherlands (2018). The United Kingdom—the country that one of our empirical research projects has focused on—offers a paradigmatic case of how the development of new legislation points to ambiguous results regarding authoritarian and illiberal practices in Western countries. Following the Snowden leaks, the official independent reviewer of existing antiterrorism legislation criticized the surveillance laws of the country as "obscure," "undemocratic," and "intolerable," calling for a significant

review and redevelopment (Anderson, 2015). Other parties demanded a democratic license for the surveillance activities of intelligence agencies (Royal United Services Institute, 2015). In response to such reviews and to public critique and legal challenges against the existing regulatory framework, the UK government initiated substantial policy reform. The Investigatory Powers Act of 2016 combined the previously fragmented legislative framework of data collection and analysis into one comprehensive law. Addressing a wide range of surveillance practices—from bulk data collection to "computer network exploitation" (i.e., hacking)—it opened up many of the traditionally secret surveillance measures to public scrutiny and oversight. However, rather than limiting state surveillance powers in light of the Snowden leaks, it confirmed, legalized, and expanded existing practices. This includes, for example, the collection of Internet connection records (i.e., people's Web browsing habits), which are now available to a wide range of authorities upon request; the removal of encryption; and the legalization of hacking by the state into the devices of citizens (Hintz & Brown, 2017).

As research from the Digital Citizenship and Surveillance Society project shows, most stakeholders agreed that the new legislation increases transparency, with one surveillance critic even suggesting that the act may be "the most transparent bit of legislation that Britain's ever had" (interview with digital rights activist, February 2016). Moreover, the process of developing the legislation provided opportunity for nongovernmental actors to contribute to the policy debate. It strengthened, particularly, the role of digital rights organizations in debates on national security, where they were increasingly recognized as legitimate actors with relevant expertise (interview with digital rights activist, January 2016). This would suggest that policy reform in the United Kingdom, although advancing illiberal rules, has enhanced accountability and cannot, therefore, be interpreted as authoritarian. In effect, however, the impact of surveillance critics, civil society, and other stakeholders on policy development was very limited. Although a wide range of actors were invited to contribute through, for example, the submission of public comments, most of these were neglected during the development and revision process. Parliamentary control suffered from a lack of "the time and exposure to be able to get sufficient knowledge" (interview with UK parliamentarian, March 2016) to fully understand the issues and, in some cases, pressure by government "to defend the agencies" (interview with UK parliamentarian, February 2016). Accountability was thus maintained on the surface but disguised in the actual process of policy reform.

Instead, the security and intelligence community enjoyed prominent access to policy makers and consideration of their concerns. For example, the time frame for data retention was based on a suggestion by the National Crime Agency (interview with former security officer, February 2016) and was not amended despite heavy criticism from most other stakeholders. The key role attributed in the process to the Home Office—which is responsible for domestic security and, hence, has a strong interest in expanding surveillance—together with the close access for security agencies to decision makers shaped both the general direction and the details of policy reform. Key officers inside the Home Office acted, according to a UK parliamentarian (interview, February 2016), "not as a filter but as an advocate" for the expansion of surveillance powers. Although most of the publicly available consultations were critical of the draft law, its supporters thus had internal communication channels—a "hotline" to lawmakers (interview with UK parliamentarian, February 2016)—at their disposal to advance their interests. The limited debate that did take place was led by public relations efforts of intelligence and security agencies, and the institutional processes of balancing benefits and risks by incorporating multiple perspectives were underdeveloped. Both

chambers of Parliament adopted the governmental proposal despite a lack of substantial revisions that had been demanded even by parliamentary review committees (Hintz & Brown, 2017).

Our research shows how, according to stakeholders and observers, an extensive public discussion on the future of surveillance policy did not take place and that the policy reform process lacked both popular legitimation and wider public debate. Civil society activists and parliamentarians from oppositional parties regarded the main purpose of the new law as "justifying essentially previous secret practice" and aiming "to legitimize existing behavior rather than to enter into a debate about what should be done" (interview with digital rights activist, February 2016). The top-down dimension of governmental practice in one of the Western countries most implicated in the Snowden revelations was thus infused by both illiberal and authoritarian practices. In the following section, we investigate how these processes are reflected in citizen behavior.

Authoritarian Practices, Bottom Up: Surveillance Culture, Resignation, and . . . Resistance

The top-down processes of establishing, practicing, and legitimizing surveillance are mirrored in bottom-up dynamics that include active engagement with, or passive acceptance of, the pervasive collection and analysis of personal data by the state-industry complex. As noted before, scholars have suggested that users partake in systems and processes that render personal lives increasingly transparent to a range of organizations whose activities are not necessarily transparent to them (Lyon, 2015). The internalization of surveillance as "part of a whole way of life" and "of everyday reflections on how things are" (Lyon, 2017, p. 825) transforms also our understandings of key practices in digital society, for example, by reinterpreting "sharing" as exposure of personal data to anyone, including state and corporate actors (van Dijck, 2013). Citizen participation is, not least, advanced through the attraction of the platforms and devices that generate and collect data (Harcourt, 2015). The prevailing consent model requires that users agree to comprehensive data collection if they wish to partake in digital life through most platforms, turning individuals into "unwitting data subjects" forced to carry the burden of privacy protection (Edwards & Veale, 2017).

However, this does not necessarily mean that the public actively consents to data collection practices or that citizens are apathetic bystanders to the technologies that envelop their daily activities. An increasing number of studies in the aftermath of the Snowden leaks has found that there are significant levels of unease, confusion, and concern in relation to how data is generated and collected, what it is used for and by whom, and how users can address these challenges. Respondents conveyed a general sense of lack of control over how data travels and a wish for more information about the data practices of organizations, revealing that average citizens tend to feel disempowered by the choices they can make in a digital environment (Eurobarometer, 2015; Information Commissioner's Office, 2015). Similarly, survey data from the Washington-based Pew Research Center showed how, amid the Cambridge Analytica case exposing Facebook's questionable data reuse practices, people struggle to understand the scope of the data collected about them by social media companies (Rainie, 2018). The empirical results of our research projects provide further evidence for these trends. In focus groups with members of the British public, people expressed concern about surveillance and data collection but, at the same time, assumed the inevitability of data-driven privacy violations in digital environments and saw little possibility to challenge,

circumvent, or mediate the data collected on them. Focus group participants noted being "uncomfortable" and "uneasy" not just about surveillance but also about their lack of knowledge of their own privacy (Dencik & Cable, 2017). A lack of understanding, combined with concerns about surveillance but a feeling of disempowerment, points to what Draper and Turow (2017) have posited as a "sociology of digital resignation" and Dencik and Cable (2017) have called as "surveillance realism," in which people resign to ubiquitous data collection in more and more aspects of social life. Rather than actively consenting or passively accepting surveillance, they feel unable to properly negotiate the reality of data collection.

The popular confusion about surveillance practices has been underpinned by shortcomings in mediated public debate and the predominant narrative of security that defines it. Research as part of the Digital Citizenship and Surveillance Society project demonstrated how media coverage has, by and large, justified surveillance and downplayed implications for citizen rights and civil liberties. Whereas blogs and new types of online news media have often provided a more differentiated perspective on the subject, classic mainstream media have—apart from a few exceptions—been unable to enhance public knowledge and, instead, have normalized surveillance (Wahl-Jorgensen, Bennet, & Taylor, 2017). A lack of sufficient information, public understanding, and debate and, as a consequence, the disempowerment of citizens thus mirror authoritarian governmental practices. The secrecy and lack of accountability that typically characterize such practices are evidenced by the intersection of both dimensions.

Snowden showed how politically active citizens can be particularly implicated when carrying out activities and expressing dissent in digital environments. Some of the leaked documents proved that government agencies in both the United States and the United Kingdom actively monitored political groups, including international organizations such as Medecins du Monde (Doctors of the World), Amnesty International, and Human Rights Watch, with a "watch-list" (Privacy International & Amnesty International, 2015). Germany's Federal Intelligence Service was spying for years on international journalists of, among others, *The New York Times*, *Reuters*, and the *BBC* (Baumgärtner, Knobbe, & Schindler, 2017). State surveillance practices have also extended to the monitoring of politically interested citizens, for example, with GCHQ tracking any visitor to the WikiLeaks site in the aftermath of WikiLeaks' Cablegate publications in 2010 (Greenwald & Gallagher, 2014).

The chilling effect of surveillance has particularly worrying consequences for these individuals and organizations. A survey of writers in the immediate aftermath of the Snowden leaks suggested that the revelations caused self-censorship (PEN, 2013). Further studies revealed a reluctance among citizens to engage in politically sensitive topics online, showing a decline in "privacy-sensitive" search terms on Google (Marthews & Tucker, 2017) and in page views of Wikipedia articles relating to terrorism (Penney, 2016). A "spiral of silence" in surveillance debates has been observed on social media (Hampton et al., 2014) and has affected also the expression of minority political views (Stoycheff, 2016). "Networked chilling effects" have been found as a consequence of merely being made aware of online regulatory actions, as people are scared of even hypothetical surveillance scenarios (Penney, 2017). As Greenwald (2014) argued, "mass surveillance kills dissent in a deeper and more important place as well, in the mind, where the individual trains him- or herself to think only in line with what is expected and demanded" (pp. 177–178). Findings from our research projects confirm this concern. Interviews with social justice activists have shown how the argument "nothing to hide, nothing to fear" has been internalized and how, therefore, distinctions are made

between different forms of dissent that may expect different levels of surveillance. Interviewees from several British civil society organizations noted that "we've got nothing to hide" and therefore felt less urgency to address the issue. Asked about the use of encryption technologies, several interviewees noted that it would be relevant mainly for the more radical groups, whereas their own organization should be safe because of its public and mainstream-oriented approach. In this way, surveillance can keep the mainstream in check while identifying more determined dissidents (Dencik & Cable, 2017).

Although these effects can be observed in a significant portion of social justice activists that work on issues such as housing, racism, or the environment, those who are more directly engaged with the development of, or advocacy about, digital infrastructure are actively carving out spaces of resistance. For example, politically motivated software developers create technical solutions (e.g., privacy-aware operating systems such as Qubes and anonymity networks such as Tor) to empower ordinary users to use end-to-end encryption. In their own words, "we want people to feel that they have something to hide" (interview with privacy advocate, August 2017), and "we need to teach people how to protect themselves online" (interview with security developer, July 2017). The main challenges to this approach include the scalability of technical solutions; the scarce and intermittent funding supporting development and maintenance; translation to adapt the tools to local needs; "behavior change" at both the individual and the organizational level; and "building a community" of developers, users, and trainers "able to take things on their own" (interview with digital rights advocate, August 2017). In addition, the ongoing criminalization of privacy-related activities (see the 2016 Apple–FBI encryption dispute or the 2015 pronouncements by the United Kingdom and Australia about banning encrypted communication) results in a chilling effect even among tech-savvy people who are increasingly concerned about the risks of being associated with encryption. In particular, human rights defenders interviewed for DATACTIVE expressed their fear that in the near future the development and use of privacy- and anonymity-enhancing technology might be imperiled by actors who find such tools threatening or problematic.

Further, a strong disconnect has been observed between technology activism and wider civil society concerns, with social justice activists outsourcing responses to surveillance concerns to digital rights and tech activists, and the latter tending toward solutions for individualized protection rather than societal transformation (Dencik, Hintz, & Cable, 2016). The Snowden leaks represented one of those "sneaky moments in which the ongoing divide between those engaged in struggles of social justice and those struggling for just technologies have been reshaped" (Aouragh, Gürses, Rocha, & Snelting, 2015, p. 208), but the delegation of technological concerns and solutions to the "progressive techies" (Aouragh et al., 2015) remains firmly in place. Furthermore, the framing of privacy as a predominantly individual responsibility (Kazansky, 2015) jeopardizes a perspective on the societal process of datafication and the interests driving surveillance. If the dominant technological solutionism testifies to the prevalence of the "happy story about how technology will fix everything" (interview with digital rights advocate, July 2017), this approach risks excluding the large majority, turning user empowerment into "something that [only] the most privileged and sophisticated users are interested in, and those who are seeking . . . a vehicle to avoid regulation" (interview with digital rights advocate, September 2017). Complementing this overemphasis on technology, digital rights organizations address a somewhat broader societal dimension through advocacy campaigns, strategic litigation, and capacity building to empower individuals "so that people can use the technology to exercise their rights" (interview with digital rights advocate, March 2017). As part of this,

some have attempted to reframe privacy advocacy as "a movement of people who care about rights" (interview with privacy advocate, March 2017), thereby expanding its collective relevance beyond individual cyberhygiene. Similarly, RightsCon (https://www.rightscon.org/) rebranded itself as a conference series about "human rights in the digital age," explicitly moving beyond the digital rights frame. However, strategies of resisting, circumventing, and changing the authoritarian practices discussed here are facing significant challenges. In particular, they have limitations in addressing popular reactions of digital resignation and surveillance realism outside a digitally literate minority, and therefore in resolving the uncertainty resulting from governmental secrecy and lack of accountability. They have been successful in exposing the illiberal nature of surveillance practices and, to some extent, the authoritarian tendencies of their implementation and in pointing to alternatives. On the other hand, the individualized and niche character of much of today's digital activism has not hindered the emergence of widespread popular disempowerment, which is at the heart of the bottom-up dimension of authoritarian practices.

Conclusion

For a long time, digital authoritarian practices have been associated with nondemocratic regimes, which, as Clinton (2010) noted, "violate" and "violated the privacy of citizens" (p. 4). According to this perspective, "internet freedoms" and the "liberation technology" (Diamond, 2010) advanced by nonauthoritarian countries would provide a remedy against such practices, working as a vehicle of democratization in those parts of the world under authoritarian rule. However, as the Snowden leaks demonstrated, challenges to civic rights are now occurring across the world and throughout both authoritarian and democratic regimes. By conceptualizing surveillance as an authoritarian practice in the democratic West, we (a) presented an analysis that undermines political narrative seeking to divide the world into one with a free Internet and one where digital freedoms do not exist, (b) contextualized surveillance in the study of authoritarian practices, and (c) examined two dimensions that intersect in the emergence of authoritarian digital practices in the West. Reviewing qualitative data from two projects and placing it in the context of a broader range of studies, we argued that digital authoritarian practices are manifested through the interplay of two broad dynamics: the top-down dimension of governmental practices and policy and the bottom-up dimension of popular engagement with, and knowledge of, digital infrastructure. We showed how surveillance policies and policy making both affect civic rights and undermine the accountability of state power to citizens. By reviewing policy development and citizen engagement in the United Kingdom, one of the countries at the center of the post-Snowden surveillance debate, we exposed a lack of democratic process and public debate in the development of the recent surveillance law, the Investigatory Powers Act. By examining citizens' reaction to and engagement with surveillance, we pointed to the emergence of digital resignation and a surveillance realism whereby a system without surveillance becomes ever harder to imagine, with its corollary of chilling effects on the democratic discourse and (technical) attempts at resistance emerging at the fringes of the system. Together, both dimensions revealed an ongoing process of undermining the accountability of the state toward its citizens and the persistence (and expansion) of challenges to the informed exercise of civic rights.

We argue that an integrated perspective on both the top-down and the bottom-up dimensions can provide us with a mechanism for understanding the ways in which authoritarian practices are entrenched in democratic countries. The actions of state agencies and governmental policy development and their

reflection in citizen behavior offer a multifaceted understanding of the pervasiveness of authoritarian practices and of their societal institutionalization. This perspective, particularly, emphasizes the role of those who are often attributed a merely passive role: the citizens. If we are to adapt the notion of authoritarian practices to countries in which citizens enjoy many constitutional rights, we need to conceptualize a nuanced, layered role for those subjected to said practices. This article provides evidence for the need of a more differentiated perspective on authoritarianism that takes note of the wider diversity of practices and norms that are advanced across countries and political systems, including the democratic West. In times in which citizens view privacy merely "through a glass, darkly," we believe it is particularly fruitful—and necessary—to advance our understanding of authoritarian practices in this part of the world and to develop conceptual tools apt for the task.

References

Abbate, J. (1999). *Inventing the Internet. Inside technology*. Cambridge, MA: MIT Press.

Access Now. (2017, September 11). Shutdown tracker optimization project [#KeepItOn]. Retrieved from https://www.accessnow.org/keepiton/#problem

Albrechtslund, A. (2008). Online social networking as participatory surveillance. *First Monday*, *13*(3). Retrieved from http://firstmonday.org/article/view/2142/1949

Anderson, D. Q. C. (2015). *A question of trust: Report of the investigatory powers review (June 2015).* Independent Reviewer of Terrorism Legislation. Retrieved from https://terrorismlegislationreviewer.independent.gov.uk/a-question-of-trust-report-of-the-investigatory-powers-review/

Andrejevic, M. (2012). Exploitation in the data mine. In C. Fuchs, K. Boersma, A. Albrechtslund, & M. Sandoval (Eds.), *Internet and surveillance: The challenges of Web 2.0 and social media* (pp. 71–88). Abingdon, UK: Routledge.

Andrejevic, M. (2014). Big data, big questions: The big data divide. *International Journal of Communication, 8*, 1673–1689.

Aouragh, M., Gürses, S., Rocha, J., & Snelting, F. (2015). Let's first get things done! On division of labour and techno-political practices of delegation in times of crisis. *Fiberculture, 2015*(26), 208–235.

Aradau, C., & Blanke, T. (2017). Politics of prediction: Security and the time/space of governmentality in the age of big data. *European Journal of Social Theory, 20*(3), 373–391.

Bakir, V. (2015). Veillant panoptic assemblage: Mutual watching and resistance to mass surveillance after Snowden. *Media and Communication, 3*(3), 12–25.

Ball, K., & Snider, L. (Eds.). (2013). *The surveillance-industrial complex: A political economy of surveillance*. Abingdon, UK: Routledge.

Barlow, J. P. (1996). *A declaration of the independence of cyberspace*. San Francisco, CA: Electronic Frontier Foundation. Retrieved from https://www.eff.org/cyberspace-independence

Bauman, Z., Bigo, D., Esteves, P., Guild, E., Jabri, V., Lyon, D., & Walker, R. B. J. (2014). After Snowden: Rethinking the impact of surveillance. *International Political Sociology, 8*, 121–144.

Bauman, Z., & Lyon, D. (2012). *Liquid surveillance: A conversation*. Cambridge, UK: Polity Press.

Baumgärtner, M., Knobbe, M., & Schindler, J. (2017, February 24). Documents indicate Germany spied on foreign journalists. *Der Spiegel*. Retrieved from http://www.spiegel.de/international/germany/german-intelligence-spied-on-foreign-journalists-for-years-a-1136188.html

Baym, N. K. (2013). Data not seen: The uses and shortcomings of social media metrics. *First Monday, 18*(10). Retrieved from http://firstmonday.org/article/view/4873/3752

Benkler, Y. (2006). *The wealth of networks: How social production transforms markets and freedom*. New Haven, CT: Yale University Press.

Bentham, J. (1843). *The works of Jeremy Bentham: Vol. 4. Panopticon, Constitution, Colonies, Codification*. Edinburg, UK: W. Tait.

boyd, d., & Crawford, K. (2012). Critical questions for big data. Provocations for a cultural, technological, and scholarly phenomenon. *Information, Communication & Society, 15*(5), 662–679.

Cheney-Lippold, J. (2011). A new algorithmic identity. Soft biopolitics and the modulation of control. *Theory, Culture & Society, 28*(6), 164–181.

Clinton, H. R. (2010, January 21). *Remarks on Internet freedom.* Washington, DC: U.S. Department of State. Retrieved from http://immagic.com/eLibrary/ARCHIVES/GENERAL/US_DOS/S100121C.pdf

Couldry, N., & Powell, A. (2014). Big data from the bottom up. *Big Data & Society, 1*(2), 1–5.

Dalton, C. M., & Thatcher, J. (2014, May 12). What does a critical data studies look like and why do we care? *Society & Space.* Retrieved from http://societyandspace.org/2014/05/12/what-does-a-critical-data-studies-look-like-and-why-do-we-care-craig-dalton-and-jim-thatcher/

Deibert, R. J. (2009). The geopolitics of Internet control: Censorship, sovereignty, and cyberspace. In A. Chadwick & P. N. Howard (Eds.), *The Routledge handbook of Internet politics* (pp. 323–336). London, UK: Routledge.

Deibert, R. J. (2013). *Black code: Inside the battle for cyberspace*. Toronto, Canada: McClelland & Stewart.

Deibert, R. J., Palfrey, J. G., Rohozinski, R., & Zittrain, J. (2008). *Access denied: The practice and policy of global Internet filtering*. Cambridge, MA: MIT Press.

Deibert, R. J., Palfrey, J. G., Rohozinski, R., & Zittrain, J. (Eds.). (2011). *Access contested: Security, identity, and resistance in Asian cyberspace*. Cambridge, MA: MIT Press.

Dencik, L., & Cable, J. (2017). The advent of surveillance realism: Public opinion and activist responses to the Snowden leaks. *International Journal of Communication, 11*, 763–781.

Dencik, L., Hintz, A., & Cable, J. (2016). Towards data justice? The ambiguity of anti-surveillance resistance in political activism. *Big Data & Society, 3*(2), 1–12.

Diamond, L. (2010). Liberation technology. *Journal of Democracy, 3*, 69–83.

Dijck, J. van. (2013). *The culture of connectivity: A critical history of social media*. Oxford, UK: Oxford University Press.

Dijck, J. van. (2014). Datafication, dataism and dataveillance: Big data between scientific paradigm and ideology. *Surveillance and Society, 12*(3), 197–208.

Dijck, J. van, & Poell, T. (2013). Understanding social media logic. *Media and Communication, 1*(1), 2–14.

Draper, N., & Turow, J. (2017). Toward a sociology of digital resignation. Paper presented at the Data Power 2017 conference, June 22–23, Ottawa, Canada.

Edwards, L., & Veale, M. (2017). Slave to the algorithm? Why a "right to an explanation" is probably not the remedy you are looking for. *Duke Law & Technology Review, 18.* Retrieved from https://ssrn.com/abstract=2972855

Eurobarometer. (2015). *Data protection* (Special Eurobarometer Report 431). Retrieved from http://ec.europa.eu/public_opinion/archives/eb_special_439_420_en.htm

Freedom Online Coalition. (n.d.). *Aims and priorities*. Retrieved from https://freedomonlinecoalition.com/about-us/about/

Freyburg, T., & Garbe, L. (2018). Blocking the bottleneck: Internet shutdowns and ownership at election times in sub-Saharan Africa. *International Journal of Communication*, this Special Section.

Gangadharan, S. (2012). Digital inclusion and data profiling. *First Monday, 17*(5). Retrieved from http://journals.uic.edu/ojs/index.php/fm/article/view/3821/3199

Gillespie, T. (2014). The relevance of algorithms. In T. Gillespie, P. Boczkowski, & K. Foot (Eds.), *Media technologies: Essays on communication, materiality, and society* (pp. 167–194). Cambridge, MA: MIT Press.

Glasius, M. (2018). What authoritarianism is . . . and is not: A practice perspective. *International Studies, 94*(3), 515–533.

Glasius, M., & Michaelsen, M. (2018). Illiberal and authoritarian practices in the digital sphere. *International Journal of Communication*, this Special Section.

Goldsmith, J., & Wu, T. (2006). *Who controls the Internet? Illusions of a borderless world*. Oxford, UK: Oxford University Press.

Greenwald, G. (2013, June 20). The top secret rules that allow NSA to use US data without a warrant. *The Guardian*. Retrieved from https://www.theguardian.com/world/2013/jun/20/fisa-court-nsa-without-warrant

Greenwald, G. (2014). *No place to hide: Edward Snowden, the NSA, and the U.S. surveillance state*. London, UK: Hamish Hamilton.

Greenwald, G., & Gallagher, R. (2014, February 18). Snowden documents reveal covert surveillance and pressure tactics aimed at WikiLeaks and its supporters. *The Intercept*. Retrieved from https://theintercept.com/2014/02/18/snowden-docs-reveal-covert-surveillance-and-pressure-tactics-aimed-at-wikileaks-and-its-supporters/

Haggerty, K. D., & Ericson, R. V. (2000). The surveillance assemblage. *British Journal of Sociology*, *51*(4), 605–622.

Hampton, K. N., Rainie, L., Lu, W., Dwyer, M., Shin, I., & Purcell, K. (2014). *Social media and the "spiral of silence."* Washington, DC: Pew Research Center. Retrieved from http://www.pewinternet.org/files/2014/08/PI_Social-networks-and-debate_082614.pdf

Harcourt, B. E. (2015). *Exposed: Desire and disobedience in the digital age*. Cambridge, MA: Harvard University Press.

Hintz, A. (2016). Restricting digital sites of dissent: Commercial social media and free expression. *Critical Discourse Studies, 13*(3), 325–340.

Hintz, A., & Brown, I. (2017). Enabling digital citizenship? The reshaping of surveillance policy after Snowden. *International Journal of Communication, 11*, 782–801.

Hintz, A., Dencik, L., & Wahl-Jorgensen, K. (2017). Digital citizenship and surveillance society: Introduction. *International Journal of Communication, 11*, 731–739.

Hintz, A., Dencik, L., & Wahl-Jorgensen, K. (2018). *Digital citizenship in a datafied society*. Cambridge, UK: Polity Press.

Howard, P. N., Agarwal, S. D., & Hussain, M. M. (2011). When do states disconnect their digital networks? Regime responses to the political use of social media. *The Communication Review, 14*(3), 216–232.

Information Commissioner's Office. (2015). *Data protection rights: What the public want and what the public want from data protection authorities.* Paper presented at the European Conference of Data Protection Authorities, Manchester, UK. Retrieved from https://ico.org.uk/media/about-the-ico/documents/1431717/data-protection-rights-what-the-public-want-and-what-the-public-want-from-data-protection-authorities.pdf

Isin, E., & Ruppert, E. (2015). *Becoming digital citizens*. Lanham, MD: Rowman & Littlefield.

Kazansky, B. (2015). Privacy, responsibility, and human rights activism. *Fibreculture, 2015*(26). doi:10.15307/fcj.26.195.2015

Kitchin, R., & Lauriault, T. (2015). *Towards critical data studies: Charting and unpacking data assemblages and their work.* (The Programmable City Working Paper 2). Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2474112

Linz, J. J. (1964). An authoritarian regime: The case of Spain. In K. Allardt & Y. Littunen (Eds.), *Cleavages, ideologies and party systems*. Helsinki, Finland: Transactions of the Westermarck Society.

Lyon, D. (2007). Surveillance, power, and everyday Life. In R. Mansell, C. Anthi Avgerou, D. Quah & R. Silverstone (Eds.), *The Oxford handbook of information and communication technologies* (p. 449–472). Oxford/New York: Oxford University Press.

Lyon, D. (2014). Surveillance, Snowden, and big data: Capacities, consequences, critique. *Big Data & Society, 1*(2). doi:10.1177/2053951714541861

Lyon, D. (2015). *Surveillance after Snowden*. Cambridge, UK: Polity Press.

Lyon, D. (2017). Surveillance culture: Engagement, exposure, and ethics in digital modernity. *International Journal of Communication, 11*, 824–842.

Lyon, D., Haggerty, K. D., & Ball, K. (2012). Introducing surveillance studies. In D. Lyon, K. D. Haggerty, & K. S. Ball (Eds.), *Routledge handbook of surveillance studies* (pp. 1–11). London, UK: Routledge.

Mann, S., Nolan, J., & Wellman, B. (2003). Sousveillance: Inventing and using wearable computing devices for data collection in surveillance environments. *Surveillance & Society, 1*(3), 331–355.

Marquis-Boire, M., Marczak, B., Guarnieri, C., & Scott-Railton, J. (2013, April 30). For their eyes only: The commercialization of digital spying. *The Citizen Lab*. Retrieved from https://citizenlab.ca/2013/04/for-their-eyes-only-2/

Marthews, A., & Tucker, C. (2017). *Government surveillance and Internet search behaviour*. Retrieved from https://ssrn.com/abstract=2412564

Mayer-Schoenberger, V., & Padova, Y. (2016). Regime change? Enabling big data through Europe's new data protection regulation. *The Columbia Science & Technology Law Review, 17*, 315–332.

Medeiros, F. A., & Bygrave, L. A. (2015). Brazil's Marco Civil da Internet: Does it live up to the hype? *Computer Law & Security Review, 31*(2), 120–130.

Milan, S. (2018). Political agency, digital traces and bottom-up data practices. *International Journal of Communication, 12*, 507–527.

Milan, S., & van der Velden, L. (2016). The alternative epistemologies of data activism. *Digital Culture & Society, 2*(2), 57–74.

Mossberger, K., Tolbert, C., & McNeal, R. S. (2007). *Digital citizenship: The Internet, society, and participation*. Cambridge, MA: MIT Press.

Mueller, M. L. (2010). *Networks and states: The global politics of Internet governance*. Cambridge, MA: MIT Press.

Murakami Wood, D., & Webster, C. W. R. (2009). Living in surveillance societies: The normalisation of surveillance in Europe and the threat of Britain's bad example. *Journal of Contemporary European Research, 5*(2), 259–273.

Noble, S. U. (2018). *Algorithms of oppression: How search engines reinforce racism*. New York, NY: New York University Press.

Nye, J. S., Jr. (2011). *The future of power*. New York, NY: PublicAffairs.

Parsons, C. (2014, March 6). The murky state of Canadian telecommunication surveillance. *The Citizen Lab.* Retrieved from https://citizenlab.ca/2014/03/murky-state-canadian-telecommunications-surveillance/

PEN. (2013). *Chilling effects: NSA surveillance drives U.S. writers to self-censor*. New York, NY: PEN American Center. Retrieved from http://www.pen.org/sites/default/files/Chilling%20Effects_PEN%20American.pdf

Penney, J. W. (2016). Chilling effects: Online surveillance and Wikipedia use. *Berkeley Technology Law Journal, 31*(1), 117–182.

Penney, J. W. (2017). Internet surveillance, regulation, and chilling effects online: A comparative case study. *Internet Policy Review, 6*(2), 1–38.

Privacy International & Amnesty International. (2015). *Two years after Snowden: Protecting human rights in an age of mass surveillance*. Retrieved from https://www.privacyinternational.org/sites/default/files/Two%20Years%20After%20Snowden_Final%20Report_EN_0.pdf

Rainie, L. (2018, March 27). *Americans' complicated feelings about social media in an era of privacy*. Washington, DC: Pew Research Center. Retrieved from http://www.pewresearch.org/fact-tank/2018/03/27/americans-complicated-feelings-about-social-media-in-an-era-of-privacy-concerns/

Reporters Without Borders. (2014). *Enemies of the Internet 2014: Entities at the heart of censorship and surveillance*. Retrieved from https://rsf.org/en/news/enemies-internet-2014-entities-heart-censorship-and-surveillance

Rheingold, H. (1993). *The virtual community: Homesteading on the electronic frontier*. Reading, MA: Addison-Wesley.

Rosen, J. (2006). *The people formerly known as the audience*. Retrieved from http://journalism.nyu.edu/pubzone/weblogs/pressthink/2006/06/27/ppl_frmr.html

Royal United Services Institute. (2015). *A democratic licence to operate: Report of the Independent Surveillance Review*. Retrieved from https://rusi.org/publication/whitehall-reports/democratic-licence-operate-report-independent-surveillance-review

Ruppert, E. (2015). Doing the transparent state: Open government data as performance indicators. In R. Rottenburg, S. E. Merry, S.-J. Park, & J. Mugler (Eds.), *A world of indicators: The making of governmental knowledge through quantification* (pp. 127–150). Cambridge, UK: Cambridge University Press.

Shirky, C. (2008). *Here comes everybody: The power of organizing without organizations*. New York, NY: Penguin.

Stoycheff, E. (2016). Under surveillance: Examining Facebook's spiral of silence effects in the wake of NSA Internet monitoring. *Journalism & Mass Communication Quarterly, 93*(2), 296–311.

Trottier, D. (2015). Open source intelligence, social media and law enforcement: Visions, constraints and critiques. *European Journal of Cultural Studies, 18*(4–5), 530–547.

Trottier, D., & Lyon, D. (2012). Key features of social media surveillance. In C. Fuchs, K. Boersma, A. Albrechtslund, & M. Sandoval (Eds.), *Internet and surveillance: The challenges of Web 2.0 and social media* (pp. 89–105). New York, NY: Routledge.

Wagner, B. (2018). Understanding Internet shutdowns: A case study from Pakistan. *International Journal of Communication*, this Special Section.

Wahl-Jorgensen, K., Bennet, L., & Taylor, G. (2017). The normalisation of surveillance: The invisibility of citizens and their rights in media coverage of the Snowden revelations. *International Journal of Communication, 11*, 740–762.

Zuboff, S. (2015). Big other: Surveillance capitalism and the prospects of an information civilization. *Journal of Information Technology, 30*, 75–89.