International Journal of Communication 12(2018), 3795–3813 1932–8036/20180005

Illiberal and Authoritarian Practices in the Digital Sphere

Prologue

MARLIES GLASIUS[1]
MARCUS MICHAELSEN
University of Amsterdam, Netherlands

Concern about how digital communication technologies contribute to a decline of democracy and the rise of authoritarian tendencies abounds in academic and public debate. In this conceptual contribution—which connects insights from new media studies, critical security studies, human rights law, and authoritarianism research—we argue that the threats citizens may be exposed to in a digitally networked world can be grouped into three categories: (1) arbitrary surveillance, (2) secrecy and disinformation, and (3) violation of freedom of expression. We introduce the twin concepts of digital illiberal and authoritarian practices to better identify and disaggregate how such threats can be produced and diffused in transnational and multi-actor configurations. Illiberal practices, we argue, infringe on the autonomy and dignity of the person, and they are a human rights problem. Authoritarian practices sabotage accountability and thereby threaten democratic processes. We use the example of the U.S. National Security Agency's massive secret data-gathering program to illustrate both what constitutes a practice and the distinctions as well as the connections between illiberal and authoritarian practices in the digital sphere.

Keywords: illiberalism, authoritarianism, digital technologies, human rights, practices, surveillance

---

Marlies Glasius: m.glasius@uva.nl
Marcus Michaelsen: m.michaelsen@uva.nl
Date submitted: 2018–07–11

[1] This research was supported by the Authoritarianism in a Global Age project at the University of Amsterdam and received funding from the *European Research Council (FP7/2007-2013)/ERC grant agreement number 323899.*

Introduction

After several decades in which waves of democratization went hand in hand with increased respect for human rights, at least at the discursive level, we now live in an age of democratic recession. Renewed concern about democratic processes and civil liberties, if not a rise of authoritarian tendencies, abounds even in established democracies (Bermeo, 2016; Burrows & Stephan, 2015). Digital communication technologies seem to be at the heart of what has been termed a "global turn to authoritarianism" (Murakami Wood, 2017).

At the same time, transcending spatial and political frontiers by design, the Internet has prompted a renegotiation of the boundaries of state power. As they seek to assert authority in the digital sphere, states increasingly depend on and cooperate with private companies that command online infrastructure and technical expertise. They also cooperate with and learn from one another, disseminating and legitimizing their ideas and tools for controlling the Internet in international and regional forums.

A burgeoning interdisciplinary literature in new media studies, critical security studies, human rights law, and increasingly also in authoritarianism research raises the alarm about digital threats to citizens: surveillance and mass data collection, information distortion and "fake news," trolling, and malware attacks, to name a few. There is indeed reason to be alarmed, but existing research suffers from conflations and blind spots when it comes to defining what is being threatened (freedom, rights, civil society, and democracy are among the candidates) and by whom. The paradoxical double shift in digital policies and practices, toward more Internet controls on citizens but at the same time away from autonomous state decision making, remains ill-understood. This is problematic from an analytical perspective but also from the point of view of advocacy; we need a better sense of what is in need of protection, from what and from whom, to fight good fights.

By connecting the different literatures, this article aims to better define and disaggregate what threats by what configurations of actors we should be worried about. Introducing the twin concepts of authoritarian and illiberal practices, we argue that threats to citizens in the digital sphere can be grouped into three categories: (1) arbitrary surveillance, (2) secrecy and disinformation, and (3) violation of freedom of expression.

The next section discusses the gaps and ambiguities in the existing literature on the topic. This is followed by a section that explains what we mean by the term *practices* and what we believe to be the advantages of a practice approach to digital threats. In this and subsequent sections, we use the example of the U.S. National Security Agency's (NSA's) massive data-gathering program, made public through the Snowden revelations and likely to be familiar to most readers, to illustrate both what constitutes a practice and our distinction between illiberal and authoritarian practices.[2]

---

[2] We are not, of course, suggesting that illiberal or authoritarian practices are primarily associated with U.S. government agencies. Rather, the notoriety of the NSA's practices through the Snowden revelations makes it a useful case for illustrative purposes.

Illiberal practices, we will argue, infringe on the autonomy and dignity of the person, and they are a human rights problem. Authoritarian practices sabotage accountability and thereby threaten democratic processes. The difference lies in the type of harm and its political consequences. Ultimately, sustained illiberal practices may also come to constitute threats to the democratic process, and conversely, subversion of the democratic process typically also comes to threaten the autonomy and dignity of the individual. Nonetheless, there is analytical utility in distinguishing between the two categories on the basis of the primary form of harm.

The article continues with an explanation and illustration of our characterization of arbitrary surveillance as an illiberal practice that infringes on the autonomy and dignity of the person by way of invasion of privacy. We then discuss sustained and organized patterns of secrecy and disinformation as an authoritarian practice. The final section is devoted to the third digital threat: violation of freedom of expression, which we characterize as both authoritarian and illiberal.

The idea of practices allows us to move away from structural regime type classifications to examine what political actors actually do in the digital realm that may be a threat to citizens. Prizing open, in each case, the actors involved in the practice and how authoritarian and illiberal impulses connect to each other brings clarity to current debates that struggle to go beyond indications of *here be dragons*. The distinction between illiberal and authoritarian practices allows us to analytically separate threats to the autonomy and dignity of the individual from threats to the democratic process.

State of the Art and Research Gaps

Digital threats to citizens have been discussed in at least four largely separate areas of research: legal, human rights–based writings; political science–based authoritarianism studies; technically and advocacy-oriented Internet literature; and critical security studies. We take inspiration from each of these approaches but also identify gaps and ambiguities that we seek to fill and overcome.

Rights-based approaches connect digital threats to a much older legal vocabulary of international declarations and treaties as adopted and ratified by the vast majority of states, which has clear advantages from an advocacy as well as an analytical point of view (see the annual *Freedom on the Net* reports by Freedom House [https://freedomhouse.org/report-types/freedom-net]; Mendel, Puddephatt, Wagner, Hawtin, & Torres, 2012). But these approaches also have drawbacks: rights—and violations of rights—put the spotlight on those who are affected by digital threats, not on the actors that produce them. Moreover, human rights thinking has never been able to overcome the notion, inherent in legal treaties, that states are the primary duty bearers, and hence also the potential violators, on the flip side of human rights. By using the term *practices*, we shift the focus from the victims to the political actors who are invading privacy, disabling access to information, or silencing online voices. The concept of practices also gets away from a state focus and allows us to examine transnational and public–private coalitions of political actors. It gets at the whodunit behind illiberal and authoritarian practices.

The authoritarianism literature is considerably more focused on such whodunits, since one of its primary objects of inquiry is how authoritarian regimes survive challenges to their rule. But it suffers from its own biases: authoritarianism is about authoritarian *states*, and within those states, a set of power holders referred to as the *regime*. More often than not, the complexity behind this term is further obscured by referring to a single dictator as shorthand. Understanding authoritarianism is thereby reduced to second-guessing the calculations in the mind of a Putin, Erdogan, or Xi Jinping. This line of thinking is exemplified by the so-called digital dictator's dilemma: the "dictator" needs to find ways of profiting from the advantages of the Internet without being exposed to the challenges arising from a potential increase in possibilities for free speech (the term as relating to the Internet appears to originate with Kedzie, 1997; see also Boas, 2000; Göbel, 2013; Shirky, 2011). The potential implication of any actors other than the dictator in digital threats to citizens is absent in this literature. It also suffers from a kind of tautological reasoning: having once defined authoritarian regimes as those states that fail to organize free and fair elections, political actors beyond those states are by definition not part of the field of study. This tautological definition of the field blinds it to the possibility of authoritarian practices outside the purview of authoritarian regimes (see also Glasius, 2018). We do not mean to suggest that regime type–based literature has become altogether obsolete but rather that a practice lens enables the observation of manifestations of digital authoritarianism that cannot be captured within the confines of regime types.

Sociotechnical approaches to power and control on the Internet are typically more interested in what happens in practice—that is, who develops and applies what kinds of technologies in the digital sphere (Marquis-Boire, Marczak, Guarnieri, & Scott-Railton, 2013). However, these approaches regularly struggle to pinpoint the political implications of their findings. They can describe in detail, for instance, how firewalls or spyware work, but while they do so with a sense of unease and threat, it is not always entirely clear what or who is being threatened by the latest developments in digital control techniques. Does or should the difference between targeted and mass surveillance matter politically? Also, although grouping Internet controls into different generations (Deibert, 2015) has helped our understanding of state learning and the ever-evolving menu of choices, the differences between the generations in terms of their political effect are not always clear. Technical or generational approaches cannot, for instance, tell us whether human rights defenders should be more worried about disinformation campaigns, just-in-time disruptions of Internet traffic, or malware attacks.

What we undertake in this article is to develop a *political* vocabulary to understand digital threats. In this respect, our efforts are in line with the literature in critical security studies and, more specifically, surveillance studies. However, we find that this literature lacks precision. It uses the terms *practices* and *governmentality* but does not always define these terms. In castigating digital controls, and in particular surveillance, it makes little distinction between infringements on individual rights and erosion of transparency and often uses the terms *illiberal* and *authoritarian*, at times even *totalitarian*, interchangeably (Bauman et al., 2014; Fuchs & Trottier, 2015; Lyon, 2014; Murakami Wood, 2017). Moreover, while its point of departure is more promising than that of authoritarianism studies, this literature also fails to transcend the distinction between democratic and authoritarian regimes, because its empirical focus is overwhelmingly on liberal, formally democratic states. In this article, we draw on the legal, technical, and political science literature to examine the illiberal and authoritarian practices of configurations of authoritarian *and* democratic as well as state, interstate, *and* nonstate actors. The next section illuminates what we mean by practices.

A Practice Approach to Digital Threats

Practices are, simply put, "patterned actions that are embedded in particular organized contexts" (Adler & Pouliot, 2011, p 5). According to Theodore Schatzki (2001a), one of their prime theorists, "Practice approaches can . . . analyze (a) communities, societies, and cultures, (b) governments, corporations, and armies, and (c) domination and coercion as either features of, collections of, or phenomena instituted and instantiated in practices" (pp. 14–15). Practices are much more than the action or behavior of an individual but much less than a regime type.

In our use of the term *practices*, we take no position in debates between more Bourdieu-inspired versus Latour-inspired or other conceptions of practices. Indeed, we concur with Adler and Pouliot (2011), who "do not believe that using the concept necessarily entails an exclusive 'ism,'", but instead hold that a "practice-oriented theoretical approach comprises a fairly vast array of analytical frameworks that privilege practice as the key entry point to the study of social and political life" (pp. 3–4: see also Bueger & Gadinger, 2015, p. 458, as inspired by Reckwitz, for a "thin" approach to practices).

We approach practices primarily as a "unit of analysis" (Bueger & Gadinger, 2015, p. 449). Calling something a practice does not, for us, have explanatory power in and of itself. It identifies the object of inquiry. A focus on practices allows a shift away from exclusively looking at states, recognizing that in today's world, policy may be made or implemented by transnational or public–private coalitions, not solely by governments. Practice theory also gives particular emphasis to the organizational and social context in which practices arise. According to Schatzki (2001b), "a practice is a set of doings and sayings organized by a pool of understandings, a set of rules" (p. 61). Thus, as Bigo and Tsoukala (2008) recognized in their exploration of illiberal practices of liberal regimes, a practice approach avoids "focusing too much on the spectacular and ignoring the routine, the everyday practices of late modernity" (p. 3).

The NSA's global digital surveillance program nicely illustrates what constitutes a practice. For a number of years, the NSA gathered massive amounts of data primarily on non-U.S. citizens, but also from Americans, through various methods, including siphoning data from land and undersea cables, ordering companies to share metadata, using malware, and pressuring vendors to install backdoors into their products (Greenwald, 2014). The practice was not associated specifically with one administration: while various subprojects such as PRISM and XKeyscore appear to have been initiated under George W. Bush (Greenwald & MacAskill, 2013; Lee, 2013b), they continued under the Obama administration. The 2008 FISA Amendment Act that authorized the NSA, in principle, to monitor electronic communications of foreigners abroad was renewed in 2012 (FISA Amendments Act, 2012). The program was sustained for years, well documented, and quite transnational in its mode of operation, with the British Government Communications Headquarters and the Australia Signals Directorate being particularly close collaborators (Greenwald, 2014). Hundreds of people have been involved in its implementation. Private service providers and telecommunication companies have—sometimes voluntarily, sometimes under duress—collaborated in these data-gathering exercises (Bauman et al., 2014).

A traditional top-down and statist understanding of politics fails to fully explain why the NSA undertook its massive data-gathering efforts: Neither President Bush nor President Obama appear to have explicitly ordered it, and the U.S. Congress certainly did not. Instead, it was a shared understanding, within and beyond the intelligence community, about what constituted necessary and permissible data gathering for national security that made the NSA's surveillance practice possible (Harris, 2013). Using practices as our unit of analysis allows us to understand various aspects of what NSA surveillance was: a set of doings by a group of individuals, and enabled by technical capabilities, within one organization as well as implemented in a networked setting across different organizations and jurisdictions. It also helps us identify what NSA surveillance was not: a preconceived plan to spy on the world, wittingly mandated by the president or Congress (see also Bigo & Tsoukala, 2008, p. 4).

But why did the Snowden revelations uncovering these practices cause such furor? Why did they shock not only cyberactivists but ordinary citizens all over the world? We suggest that the NSA practices were politically problematic in three quite distinct ways, which are often conflated. We will elaborate each of them in the next three sections, with the aim of illuminating the three types of digital threats that this article seeks to distinguish: arbitrary surveillance as an illiberal practice, secrecy and disinformation as an authoritarian practice, and violation of freedom of expression/disabling of voice as both illiberal and authoritarian.

Arbitrary Surveillance as Illiberal Practice

The practice of mass surveillance by the NSA was widely held to constitute an infringement of the right to privacy. The enabling legislation had been quite explicit in authorizing surveillance of non-Americans abroad. In the United States, the political controversy revolved mainly around the extent to which Americans had also come under scrutiny (Nakashima, 2013). Citizens and governments of other states, especially in Germany and Brazil, by contrast, were incandescent over the lackadaisical approach U.S. authorities had taken to the privacy of non-Americans. The revelations swiftly triggered comparisons to the sniffing and spying that had occurred under the dictatorships in both countries, experienced in a not-so-distant past ("Europe Furious," 2013; Lee, 2013a; "The Snowden Case," 2013).

The discomfort and outcry caused by the breaking news of the NSA practices is appropriately captured by the single word *surveillance*. Lyon (2007) defines surveillance as "the focused, systematic and routine attention to personal details for purposes of influence, management, protection or direction" (p. 14). Drawing on this definition, Richards (2013) is insightful in terms of delineating when and why surveillance is harmful and under what conditions it should be considered an illegitimate invasion of privacy. He holds that surveillance can be harmful for two reasons: First, it may interfere with intellectual privacy—that is, freedom of thought, belief, and private speech[3]—and thus stifle diversity and individuality (see also Mokrosinska & Roessler, 2015, on the social dimensions of privacy). Second, he points out that surveillance, and particularly secret surveillance, changes the power relation between the watcher and the watched and may open the latter to blackmail, discrimination, and—more ambiguously—persuasion.

---

[3] Richards's account focuses on the tradition of practicing of freedom of thought in U.S. jurisprudence, but freedom of thought is also protected by Article 18 of the Universal Declaration of Human Rights and Article 18 of the International Covenant on Civil and Political Rights.

Clearly, not all forms of surveillance are illegitimate. Most of us would accept that our governments are entitled to know a good many of our personal details for various purposes. International human rights law actually gives good guidance as to where legitimate surveillance ends. Article 12 of the Universal Declaration of Human Rights (United Nations General Assembly, 1948) stipulates that "no one shall be subjected to arbitrary interference with his privacy"; see also Article 17 of the International Covenant on Civil and Political Rights (United Nations General Assembly, 1966). The meaning of the word arbitrary in this context is the same as it is in the phrase "arbitrary detention": not based on a precise, specific, and proportional prior legal procedure. The nature and specificity of such procedures should depend on the nature of the personal details collected, their purpose, and their potential for harm. There should be proportionality between the aim of surveillance and the degree of infringement. The level of specificity required for an entity to be entitled to hold someone's home address details without the person's prior permission, for instance, might be relatively low. The safeguards surrounding the tax office gathering data from third sources to verify one's income, on the other hand, should be considerably higher. Procedures for eavesdropping on electronic communications, where the potential for harm is highest, should also have the highest specificity: measures should relate to a named individual, authorized by a warrant based on a reasonable suspicion, signed by an authorized person, stipulating a particular purpose, the means of surveillance, and a limited time frame.

Obviously, determining where legitimate data gathering ends and arbitrary surveillance begins in the digital realm is a huge and largely unexplored territory in legal theory and practice, and there will be many hard cases. Mass surveillance of private communications, we argue, is arbitrary by nature; it is like fishing with a dragnet rather than a rod (see also Bauman et al., 2014, p. 132). Targeted surveillance can still be arbitrary depending on the circumstances. Yet we are not interested, as lawyers would be, in the exact circumstances under which a particular instance of targeted surveillance might still be legitimate; rather, we are interested in practices—sustained patterns of action in organizational contexts. Our focus is on the relatively easy cases of arbitrary and potentially harmful surveillance. The NSA practices constitute such a case, because the potential harm relating to intellectual privacy and power imbalance was great, the authorizing law was broad and vague, and the scope was massive.

Based on the types of harm caused, as described by Richards, we would characterize arbitrary surveillance as an illiberal, rather than authoritarian, practice. In a now classic article in *Foreign Affairs*, Fareed Zakaria (1997) draws an analytical distinction between democracy and liberalism. According to Zakaria, constitutional liberalism "refers to the tradition . . . that seeks to protect an individual's autonomy and dignity against coercion, whatever the source—state, church, or society" (p. 26).[4] The distinction is illustrated with historical examples of liberal regimes that were not democratic and with contemporary examples of states that hold free and fair elections but do not respect liberal rights. The latter Zakaria refers to as "illiberal." In line with this use of the term *illiberal*, we define an illiberal practice as "a pattern of actions, embedded in an organized context, that infringes on the protection of the autonomy and dignity of a person over whom a political actor exerts control" (Glasius, 2018, p. 530).

[4] Zakaria assumed that illiberalism was a non-Western phenomenon, explained in part by a lack of the right traditions—a view that is difficult to sustain today.

Stifling intellectual privacy, diversity, and individuality and risk of blackmail or discrimination are all harms at the individual level: they interfere with the autonomy and dignity of the person. Indirectly, there is also a connection between arbitrary surveillance and threats to democracy, if we believe that such surveillance in and of itself has "chilling effects" (Bernal, 2016; Penney, 2017; Stoycheff, 2016) on online political expression. Invasion of privacy through arbitrary surveillance, when patterned and organized, belongs to a broader class of illiberal practices, along with, for instance, infringement on legal equality, legal recourse or recognition before the law, fair trial rights, freedom of religion, physical integrity rights, and freedom of expression, which we will return to below. Most of these illiberal practices (violation of physical integrity rights may be an exception) know some form of online manifestation, but no other practice has been as pervasive in the digital sphere as arbitrary surveillance.

Secrecy and Disinformation as Authoritarian Practices

The uproar caused by the Snowden revelations points to the second political problem with the NSA practice: the secrecy and government disinformation campaign surrounding it. Astoundingly perhaps, it appears that U.S. legislation gives U.S. government agencies a broad remit for wiretapping or other forms of communications surveillance of non-Americans outside U.S. territory. We are apparently all potential spies, and thus fair game. Wiretaps that involve domestic communications between Americans are covered by the Foreign Intelligence Surveillance Act (FISA) and require a warrant from a court, a provision allegedly bypassed by the NSA on a massive scale during the Bush administration in the name of fighting Al Qaeda (Risen & Lichtblau, 2005). In early 2013, before the Snowden revelations, Director of National Intelligence James Clapper was asked in a congressional hearing for a "yes or no answer to the question: does the NSA collect any type of data at all on millions or hundreds of millions of Americans?" "No, sir, Clapper said. Not wittingly. There are cases where they could inadvertently, perhaps, collect, but not wittingly" (Ackerman, 2013, paras. 7–8). When subsequent revelations made this claim untenable, he claimed that it was the "least untruthful" answer he could have given to what he deemed to be an unfair question (Ackerman, 2013, para. 2). As late as June 2013, President Obama claimed, "What I can say unequivocally is that if you are a U.S. person, the NSA cannot listen to your telephone calls, and the NSA cannot target your emails . . . and have not" (Gabbett, 2013, para. 8). A fact sheet released by Clapper at the same time stated that "the United States Government does not unilaterally obtain information from the servers of U.S. electronic communication service providers" (O'Harrow, Nakashima, & Gellmann, 2013, para. 6). Two weeks later, this fact sheet was withdrawn (Miller & Nakashima, 2013, para. 2). By August 2013, the president had amended his line to stating, "We don't have a domestic spying program. . . . What we do have is some mechanisms that can track a phone number or an email address that is connected to a terrorist attack"; a few days later, he vowed to "be more transparent and to pursue reforms of our laws and practices" (Gabbett, 2013, para. 13).

In other words, various U.S. officials exhibited a pattern of secrecy and disinformation regarding the NSA's programs. A discussion of secrecy, similar to a discussion of surveillance, requires a disclaimer. Under certain circumstances, political secrecy can be legitimate, provided that the procedure for determining exceptions to publicity should itself be public. Confidential sharing of information with designated representatives of the public can sometimes be a legitimate alternative to full publicity

(Gutmann & Thompson, 1998, pp. 95–127). However, while members of Congress, particularly those on the intelligence committees, were briefed about the NSA's programs on a regular basis, it remains unclear to what extent these briefings were accurate and complete. Parliamentarians from other states whose citizens were subject to data gathering either directly or via their own security services were certainly insufficiently informed (Chase, 2017; "German Intelligence Under Fire," 2015; Van Tartwijk, 2014).

Our use of the term *disinformation* requires some explanation. Politicians spin, twist, deflect, and selectively invoke facts all the time (Mearsheimer, 2011). But a pattern of disinformation, as we use it here, is more than an occasional gloss on the facts. Disinformation refers to a deliberate distribution of false, misleading, or deceptive information (Jowett & O'Donnell, 2010, p. 24; see also Bennett & Livingston, 2018). It means knowingly putting forward false facts.

Again, there are undoubtedly hard cases. It is not always easy to establish what public officials could have or should have known and to what extent they followed legitimate procedures when sharing confidential information with limited audiences. But for our purposes, the focus is on the easy cases—a pattern of deliberately disabling or distorting information—not on exceptional incidents or on well-regulated secrecy bound by transparent procedures. What was special, and especially problematic, about the NSA scandal was the pattern of secrecy and disinformation: the scale of the program that had been kept secret from the public and the repeated flat-out lies spoken and written by multiple government officials in response to direct questions, both from members of Congress and from journalists.

Whereas the Obama administration's dealing with the NSA's surveillance practices was primarily secretive and occasionally untruthful, active practices of digital disinformation have taken a steep flight in the years since. The Oxford Internet Institute has investigated the recent phenomenon of computational propaganda: "the use of algorithms, automation, and human curation to purposefully distribute misleading information over social media networks" in both authoritarian and democratic countries. It found that in "authoritarian countries, social media platforms are a primary means of social control" but also that in democracies, computational propaganda can take the form of "broad efforts at opinion manipulation or targeted experiments on particular segments of the public" (Woolley & Howard, 2017, p. 3).

The NSA is used as an example here to make the point that the secrecy and disinformation surrounding the NSA programs is a problem that should be analytically separated from the surveillance. Secrecy and disinformation are, for the most part, not a human rights problem. There is no right, in international legislation, to being fully and accurately informed by one's own government. Instead, secrecy and disinformation are a democratic problem: without accurate information, there can be no democratic accountability. Indeed, the primary purpose of freedom of information procedures in some countries, allowing citizens to demand that particular government documents be made public, is to increase the accountability of governance, not to fulfill an individual's right.

Accountability, according to a parsimonious and widely cited definition, "is a relationship between an actor and a forum, in which the actor has an obligation to explain and justify his or her conduct, the forum can pose questions and pass judgment, and the actor may face consequences" (Bovens, 2007, p. 450). Deliberate and sustained secrecy and disinformation by political actors disrupts this relationship of accountability, and thereby the democratic process. Hence, we refer to such secrecy and disinformation as an authoritarian practice: "a pattern of actions, embedded in an organized context, sabotaging accountability to people over whom a political actor exerts control, by disabling their access to information" (Glasius, 2018, p. 527). We return later to the second aspect of accountability sabotage, the disabling of questions and judgment from the forum, in the form of violations of freedom of expression.

The sustained secrecy and disinformation surrounding the NSA surveillance program, up to the point that the scale, depth, and detail of the Snowden revelations made further dissembling impossible, would fall within our definition of an authoritarian practice. We may expect such practices to be more widespread and sustained in states under authoritarian rule than in democracies, but the idea of practices allows us to discern that they exist in democracies too, despite legal provisions to the contrary. Moreover, in the digital sphere, authoritarian and democratic states may jointly be engaged in practices of sustained and deliberate secrecy and disinformation, or it may be states and corporations that engage in such joint practices.

Disabling Voice: Illiberal and Authoritarian

Our discussion of arbitrary surveillance has characterized it as an illiberal practice, infringing on the autonomy and dignity of the individual, and the discussion of secrecy and disinformation has characterized it as an authoritarian practice, sabotaging accountability. But we have not yet characterized violation of the most classic of digital rights, the right to freedom of expression, in terms of illiberal or authoritarian practices. As visualized in Figure 1, violations of freedom of expression, we argue, are simultaneously illiberal and authoritarian: at the individual level, such violations infringe on the autonomy and dignity of the person, but at the collective level, disabling voice simultaneously also threatens the democratic process, just as secrecy and disinformation do.

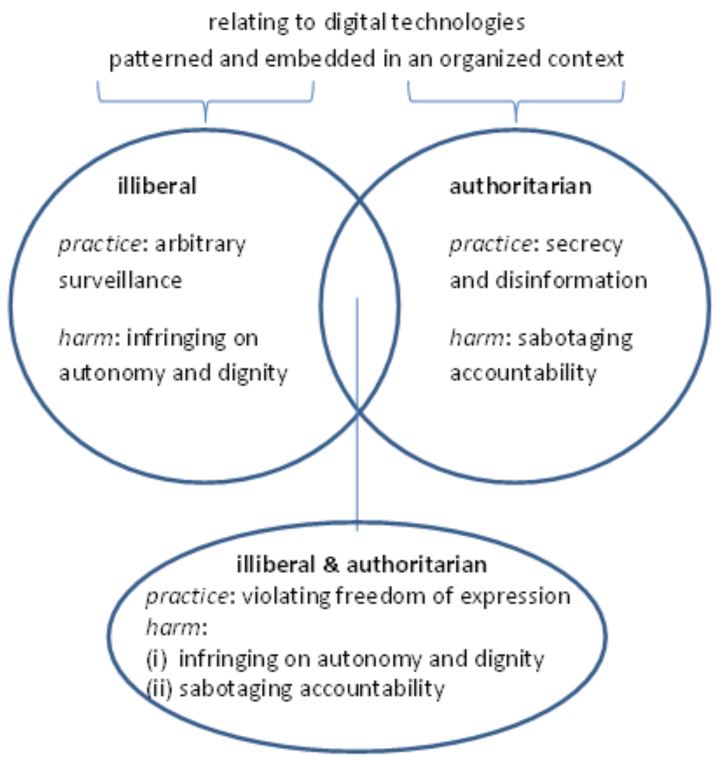

Figure 1. Digital illiberal and authoritarian practices.

For our example, we once again consider the Snowden revelations about NSA surveillance practices, but this time with a focus on what happened to Edward Snowden and to the journalists he collaborated with. It is well known that Snowden has been charged with espionage and theft of government property and that he continues to live in temporary asylum in Russia to evade arrest.

Less well known are the threats and prosecutions against the journalists and newspapers with whom Snowden collaborated. Filmmaker Laura Poitras was motivated to make a documentary about surveillance and subsequently became involved with Snowden, precisely because previous films had caused her to be placed on a watch list and she was routinely arrested and questioned about her journalistic activities at airports (Maass, 2013). Subsequent to the first revelations, the life partner of *Guardian* reporter Glenn Greenwald, the second journalist who initially met with Snowden and led the publication of the files, was detained without access to a lawyer at Heathrow Airport for nine hours. His mobile phone, laptop, and other materials were seized under the antiterrorism act ("Glenn Greenwald's Partner Detained," 2013).[5]

A simultaneous threat of legal action by the British government against *The Guardian* forced its editors, in a now notorious episode, to destroy hard drives containing copies of the Snowden files in the basement of the newspaper office, under the watchful eye of government agents (Borger, 2013). In October 2013, British prime minister David Cameron suggested he might "have to use injunctions or D notices or the other tougher measures" (Watt, 2013) against the media, and specifically *The Guardian* if they did not act responsibly (Elliott, 2013; Watt, 2013).

Snowden's status as a martyr for free speech remains contested, and the threats and harassment against his journalist associates were not especially egregious compared with some of the infringements on freedom of speech documented in other contributions to this Special Section. Nonetheless, we discuss their treatment in the context of our typology of digital threats because it allows us to prize apart practices that often coincide and may emanate from the same political actors but that constitute different types of harms. Existing analyses, by failing to make these distinctions, often "shed more heat than light"[6] on the political consequences of arbitrary surveillance, secrecy and disinformation, and violation of freedom of expression.

Conclusion

This contribution defines and disaggregates what threats by what configurations of actors citizens may be exposed to in a world that is increasingly interconnected and interlaced by digital communication technologies. The border-blurring nature of the Internet defies common notions of a sovereign and autonomous state as the classic locus of power. At the same time, paradoxically, citizens face a greater risk of intrusions into their individual and political rights. We have noted a growing uneasiness about the disruptive potential of these technologies in the academic and public debate. Surveillance, disinformation, communication, and even behavioral controls through digital networks, it is feared, contribute to a rise of authoritarian politics.

We have pointed out that, although there may be reason for concern, the common ways of understanding digital threats suffer from conflations and blind spots. First of all, investigations into the interrelation between digital technologies and authoritarian power are often too state-centered and/or too technology-focused to provide a full picture. They zoom in on authoritarian regimes, or on the failings of formal democracies, or on the capabilities and applications of digital technologies alone. Thus, they may fail to pinpoint how threats to privacy, accountability, and freedom of expression emerge and diffuse in a digitally networked world. Second, while the literature abounds with warnings of unfolding dystopias,

[5] The case eventually led to a ruling by the highest British court that the power to stop and detain under the antiterrorism act, in particular in relation to journalists and their sources, was in contravention of the European Convention on Human Rights.

[6] We borrow this phrase, with ironic intent, from President Obama's response to the Snowden revelations. "Obama: Snowden's leaks 'shed more heat than light'" (*CBS News*, January 17, 2014).

the analytical distinction as well as the empirical connections between threats to individual rights and threats to democratic processes emanating from the digital sphere have been ill-understood.

To identify and analyze political threats in the digital sphere, we have introduced the twin concepts of digital illiberal and authoritarian practices. The focus on practices as recurring patterns of action or behavior in organized settings allows us to overcome the focus on state policies alone and to analyze transnational and multiactor settings involving authoritarian and democratic states as well as nonstate and private sector actors. Illiberal practices, we have argued, infringe on the autonomy and dignity of the person, and they are a human rights problem. Authoritarian practices sabotage accountability and thereby threaten democratic processes. We contend that, although a vast array of technical possibilities and political constellations exists, most threats that digitally connected individuals face from power holders boil down to three basic types:

1. Patterned and organized invasion of privacy through arbitrary surveillance—an illiberal practice

2. Patterned and organized secrecy and disinformation—an authoritarian practice

3. Patterned and organized violation of freedom of expression—a practice both illiberal and authoritarian.

To put it in information and communication terms: In the first case, information is extracted from citizens and hoarded; in the second case, the communication flow from power holders to citizens is blocked or perverted; and in the third case, the voice of citizens and their ability to communicate is disabled. As illustrated with the NSA case, the three types of practices often intersect. But the ways the practices relate to one another, coinciding with or following from each other, will be different in different situations, as becomes clear from other contributions to this Special Section.

In traditional authoritarian regimes, patterns of arbitrary surveillance, secrecy and disinformation, and violation of freedom of expression have usually gone hand in hand, and this is no different in the digital era. Spying on the citizenry is easier than ever through digital affordances (and with a little help from commercial experts), secrecy and disinformation about government behavior remains the default setting, with the latter now also possible via the Internet; and although citizens may not be as information-poor as they once were, digital censorship in manifold technical manifestations remains a defining feature of authoritarian rule. Hence, it is not our intention to replace the established regime type literature, classifying political regimes according to their authoritarian or democratic nature and distinguishing subtypes, with practice-based approaches. On the contrary, we believe authoritarian and illiberal practices are endemic to such regimes.

In these settings our concepts will be useful to trace how digital practices disabling voice and sabotaging accountability are produced and transferred from one actor or context to another. We argue that authoritarian power is no longer confined to a specific territory, to a regime within geographic borders, but that it is constructed and reconstructed in globalized settings. Authoritarian power holders rely on international technology companies to purchase software solutions for Internet surveillance and filtering, they take inspiration from democratic states when it comes to social media regulation, and they use digital infrastructures to spy on transnational advocacy networks. Investigating the emergence and diffusion of digital practices will enable a widening of the analytical scope beyond the established focus on state–citizen relations.

In formally democratic settings, pervasive surveillance has, since Snowden, been increasingly normalized and legitimated through new legislation. Moreover, in formally autocratic and democratic political settings alike, corporate surveillance, aiming to know and hence manipulate digitized individuals as consumers, has taken flight. While the privacy of individuals is invaded, the methods and motives of the actors watching them often remain shrouded in secrecy.

The distinction between practices of surveillance (illiberal, harming rights), secrecy and disinformation (authoritarian, sabotaging accountability), and patterns of violation of freedom of expression (both) can provide analytical clarity to debates about the influence of big digital technology corporations whose business models rely on the gathering of massive amounts of user data. The recent Cambridge Analytica scandal confirmed the increasing apprehension over these companies' lack of transparency in their handling of such data, their potential for profiling, targeting political information and distortion of the public debate, and their cooperation with intelligence agencies demanding backdoors to applications and access to user information. We may already be able to discern that companies such as Facebook and Google are involved, or at least complicit, in illiberal practices of surveillance. Further empirical work could determine whether their business practices based on secret algorithms withhold or distort information in patterned and organized ways, such that they should be considered authoritarian.

While frequent bouts of secrecy and occasional lying about so-called matters of national security have been a long-standing feature of democracies, new technologies have made it possible for political parties, governments, and other actors to flood citizens with well-targeted, often automated, disinformation. Partly in response to such computational propaganda and fake news, governments and commercial actors alike are beginning to adopt regulations intended to limit utterances in the public sphere that are either deemed inappropriate or factually inaccurate. Such initiatives, however well intentioned, in turn may come dangerously close to violations of freedom of expression. By considering under what conditions particular forms of fake news and information distortion could be considered accountability sabotage (an authoritarian practice) and under what conditions removing information from digital platforms falls foul of well-developed understandings of freedom of expression (both authoritarian and illiberal), we can develop a clearer political analysis of what is at stake in each of these cases.

Our twin concepts of illiberal and authoritarian practices make it possible to go beyond merely ringing the alarm over technological and especially political developments in the digital sphere and disentangle their implications for our autonomy and dignity as individuals and for democratic politics. As such, they serve as not only an analytical but also a political tool, advocating effectively against actual or potential harm.

References

Ackerman, S. (2013, June 12). Clapper: Obama stands by intelligence chief as criticism mounts. *The Guardian*. Retrieved from https://www.theguardian.com/world/2013/jun/12/james-clapper-intelligence-chief-criticism

Adler, E., & Pouliot, V. (2011). International practices. *International Theory*, *3*(1), 1–36. doi:10.1017/S175297191000031X

Bauman, Z., Bigo, D., Esteves, P., Guild, E., Jabri, V., Lyon, D., & Walker, R. B. (2014). After Snowden: Rethinking the impact of surveillance. *International Political Sociology*, *8*(2), 121–144. doi:10.1111/ips.12048

Bennett, W. L., & Livingston, S. (2018). The disinformation order: Disruptive communication and the decline of democratic institutions. *European Journal of Communication*, *33*(2), 122–139. doi:10.1177/0267323118760317

Bermeo, N. (2016). On democratic backsliding. *Journal of Democracy*, *27*(1), 5–19.

Bernal, P. (2016). Data gathering, surveillance and human rights: Recasting the debate. *Journal of Cyber Policy*, *1*(2), 243–264.

Bigo, D., & Tsoukala, A. (2008). Understanding insecurity. In D. Bigo & A. Tsoukala (Eds.), *Terror, insecurity and liberty: Illiberal practices of liberal regimes after 9/11* (pp. 1–9). Oxford, UK: Routledge.

Boas, T. (2000). The dictator's dilemma? The Internet and U.S. policy toward Cuba. *Washington Quarterly*, *23*(3), 57–67.

Borger, J. (2013, August 20). NSA files: Why the Guardian in London destroyed hard drives of leaked files. *The Guardian*. Retrieved from https://www.theguardian.com/world/2013/aug/20/nsa-snowden-files-drives-destroyed-london

Bovens, M. (2007). Analysing and assessing accountability: A conceptual framework. *European Law Journal*, *13*(4), 447–468. doi:10.1111/j.1468-0386.2007.00378.x

Bueger, C., & Gadinger, F. (2015). The play of international practice. *International Studies Quarterly*, *59*(3), 449–460. doi:10.1111/isqu.12202

Burrows, M., & Stephan, M. J. (Eds.). (2015). *Is authoritarianism staging a comeback?* Washington, DC: Atlantic Council.

Chase, J. (2017, February 13). Bundestag grills Merkel subordinates on NSA spying. *Deutsche Welle*. Retrieved from http://p.dw.com/p/2XUgj

Deibert, R. (2015). Cyberspace under siege. *Journal of Democracy*, *26*(3), 64–78. doi:10.1353/jod.2015.0051

Elliott, F. (2013, October 28). Cameron hints at action to stop security leaks. *The Times*. Retrieved from https://www.thetimes.co.uk/article/cameron-hints-at-action-to-stop-security-leaks-krg6tl9w80c

Europe furious over US spying allegations. (2013, October 24). *Der Spiegel*. Retrieved from http://www.spiegel.de/international/world/angry-european-and-german-reactions-to-merkel-us-phone-spying-scandal-a-929725.html

FISA Amendments Act Reauthorization Act of 2012, Pub. L. No. 112-238. Retrieved from https://www.govtrack.us/congress/bills/112/hr5949

Fuchs, C., & Trottier, D. (2015). Towards a theoretical model of social media surveillance in contemporary society. *Communications*, *40*(1), 113–135. doi:10.1515/commun-2014-0029

Gabbett, A. (2013, August 9). Nobody is listening to your calls: Obama's evolution on NSA surveillance. *The Guardian*. Retrieved from https://www.theguardian.com/world/2013/aug/09/obama-evolution-nsa-reforms

German intelligence under fire for NSA cooperation. (2015, April 24). *Der Spiegel.* Retrieved from http://www.spiegel.de/international/germany/german-intelligence-agency-bnd-under-fire-for-nsa-cooperation-a-1030593.html

Glasius, M. (2018). What authoritarianism is . . . and is not: A practice perspective. *International Affairs*, *94*(3), 515–533. doi:10.1093/ia/iiy060

Glenn Greenwald's partner detained at Heathrow airport for nine hours. (2013, August 18). *The Guardian*. Retrieved from https://www.theguardian.com/world/2013/aug/18/glenn-greenwald-guardian-partner-detained-heathrow

Göbel, C. (2013). The information dilemma: How ICT strengthen or weaken authoritarian rule. *Statsvetenskaplig Tidskrift*, *115*(4), 385–402. Retrieved from http://journals.lub.lu.se/index.php/st/article/view/9744

Greenwald, G. (2014). *No place to hide: Edward Snowden, the NSA, and the U.S. surveillance state*. New York, NY: Picador.

Greenwald, G., & MacAskill, E. (2013, June 7). NSA Prism program taps in to user data of Apple, Google and others. *The Guardian*. Retrieved from https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data

Gutmann, A., & Thompson, D. (1998). *Democracy and disagreement*. Cambridge, MA: Harvard University Press.

Harris, S. (2013, September 9). The cowboy of the NSA. *Foreign Policy*. Retrieved from http://www.foreignpolicy.com/articles/2013/09/08/the_cowboy_of_the_nsa/

Jowett, G. S., & O'Donnell, V. (2010). *Propaganda and persuasion*. London, UK: SAGE Publications.

Kedzie, C. (1997). *Communication and democracy: Coincident revolutions and the emergent dictator's dilemma* (RAND dissertation). Santa Monica, CA: RAND Corporation. Retrieved from http://www.rand.org/publications/RGSD/RGSD127/sec2.html

Lee, T. B. (2013a, August 22). Glenn Greenwald lives in Brazil. Here's how Brazilians feel about his reporting. *The Washington Post*. Retrieved from https://www.washingtonpost.com/news/the-switch/wp/2013/08/22/glenn-greenwald-lives-in-brazil-heres-how-brazilians-feel-about-his-reporting

Lee, T. B. (2013b, June 6). How Congress unknowingly legalized PRISM in 2007. *Wonkblog—The Washington Post*. Retrieved from https://www.washingtonpost.com/news/wonk/wp/2013/06/06/how-congress-unknowingly-legalized-prism-in-2007/?utm_term=.be2bec29ce98

Lyon, D. (2007). *Surveillance studies: An overview*. Cambridge, UK: Polity Press.

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

Maass, P. (2013, August 13). How Laura Poitras helped Snowden spill his secrets. *The New York Times*. Retrieved from http://www.nytimes.com/2013/08/18/magazine/laura-poitras-snowden.html

Marquis-Boire, M., Marczak, B., Guarnieri, C., & Scott-Railton, J. (2013, May 1). *For their eyes only: The commercialization of digital spying.* Toronto, Canada: Citizen Lab and Canada Centre for Global Security Studies. Retrieved from https://citizenlab.ca/storage/finfisher/final/fortheireyesonly.pdf

Mearsheimer, J. J. (2011). *Why leaders lie: The truth about lying in international politics.* Oxford, UK: Oxford University Press.

Mendel, T., Puddephatt, A., Wagner, B., Hawtin, D., & Torres, N. (2012). *Global survey on Internet privacy and freedom of expression* (UNESCO Series on Internet Freedom). Paris, France: United

Nations Educational, Scientific and Cultural Organization. Retrieved from http://unesdoc.unesco.org/images/0021/002182/218273e.pdf

Miller, G., & Nakashima, E. (2013, June 25). NSA fact sheet on surveillance program pulled from Web after senators' criticism. *The Washington Post*. Retrieved from https://www.washingtonpost.com/world/national-security/nsa-fact-sheet-on-surveillance-program-pulled-from-web-after-senators-criticism/2013/06/25/afe95d9e-ddda-11e2-b797-cbd4cb13f9c6_story.html?utm_term=.1b00cf9c687a

Mokrosinska, D., & Roessler B. (2015). Introduction. In B. Roessler & D. Mokrosinska (Eds.), *Social dimensions of privacy: Interdisciplinary perspectives* (pp. 1–8). Cambridge, UK: Cambridge University Press.

Murakami Wood, D. (2017). The global turn to authoritarianism and after. In D. Murakami Wood (Ed.), Surveillance and the global turn to authoritarianism [Special issue]. *Surveillance and Society*, *15*(3/4). Retrieved from https://ojs.library.queensu.ca/index.php/surveillance-and-society/article/view/6835/6505

Nakashima, E. (2013, June 6). Verizon providing all call records to U.S. under court order. *The Washington Post*. Retrieved from https://www.washingtonpost.com/world/national-security/verizon-providing-all-call-records-to-us-under-court-order/2013/06/05/98656606-ce47-11e2-8845-d970ccb04497_story.html?utm_term=.0085d265debe

O'Harrow, R., Nakashima, E., & Gellmann, B. (2013, June 8). U.S., company officials: Internet surveillance does not indiscriminately mine data. *The Washington Post*. Retrieved from https://www.washingtonpost.com/world/national-security/us-company-officials-internet-surveillance-does-not-indiscriminately-mine-data/2013/06/08/5b3bb234-d07d-11e2-9f1a-1a7cdee20287_story.html?utm_term=.0fe0295df3a2

Penney, J. W. (2017). Internet surveillance, regulation, and chilling effects online: A comparative case study. *Internet Policy Review*, *6*(2). doi:10.14763/2017.2.692

Richards, N. M. (2013). The dangers of surveillance. *Harvard Law Review*, *126*(7), 1934–1965. Retrieved from http://www.jstor.org/stable/23415062

Risen, J., & Lichtblau, E. (2005, December 16). Bush lets U.S. spy on callers without courts. *The New York Times*. Retrieved from http://www.nytimes.com/2005/12/16/politics/bush-lets-us-spy-on-callers-without-courts.html

Schatzki, T. R. (2001a). Introduction. In K. Knorr Cetina, T. R. Schatzki, & E. Von Savigny (Eds.), *The practice turn in contemporary theory* (pp. 10–23). London, UK: Routledge.

Schatzki, T. R. (2001b). Practice mind-ed orders. In K. Knorr Cetina, T. R. Schatzki, & E. Von Savigny (Eds.), *The practice turn in contemporary theory* (pp. 50–63). London, UK: Routledge.

Shirky, C. (2011). The political power of social media. Technology, the public sphere, and political change. *Foreign Affairs*, *90*(1). Retrieved from https://www.foreignaffairs.com/articles/2010-12-20/political-power-social-media

The Snowden case and the Brazilian reaction. (2013, September 19). *Digital Rights: Latin America and the Caribbean*, no. 30. Retrieved from https://www.digitalrightslac.net/en/el-caso-snowden-y-la-reaccion-brasilena

Stoycheff, E. (2016). Under surveillance: Examining Facebook's spiral of silence effects in the wake of NSA Internet monitoring. *Journalism and Mass Communication Quarterly*, *93*(2), 296–311. doi:10.1177/1077699016630255

United Nations General Assembly. (1948). *The universal declaration of human rights.* Retrieved from http://www.un.org/en/universal-declaration-human-rights/

United Nations General Assembly. (1966). *International covenant on civil and political rights.* Retrieved from https://treaties.un.org/doc/publication/unts/volume%20999/volume-999-i-14668-english.pdf

Van Tartwijk, M. (2014, February 11). Dutch minister of interior fights for his political life; faces possible no-confidence vote he misled public. *The Wall Street Journal*. Retrieved from https://www.wsj.com/articles/dutch-minister-of-interior-fights-for-his-political-life-1392132084?tesla=y

Watt, N. (2013, October 28). David Cameron makes veiled threat to media over NSA and GHCQ leaks. *The Guardian*. Retrieved from https://www.theguardian.com/world/2013/oct/28/david-cameron-nsa-threat-newspapers-guardian-snowden

Woolley, S., & Howard, N. P. (2017). *Computational propaganda worldwide: Executive summary* (Working Paper 2017.11). Oxford, UK: Project on Computational Propaganda. Retrieved from http://comprop.oii.ox.ac.uk/wp-content/uploads/sites/89/2017/06/Casestudies-ExecutiveSummary.pdf

Zakaria, F. (1997). The rise of illiberal democracy. *Foreign Affairs*, *76*(6), 22–43.