The limits of transparency as a tool for regulating surveillance

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

Lora Anne Viola

Introduction

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

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

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

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

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

The logics of transparency: a critical reconsideration

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

Transparency as an inherent normative good

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

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

Transparency as information: a condition for democratic decision-making

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

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

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

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

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

Transparency as monitoring: a condition for democratic accountability

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

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

Transparency as a condition for trust

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

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

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

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

Three distorting effects of transparency

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

power, in turn, condition the kinds of effects transparency can have on socio-political relations.

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

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

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

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

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

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

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

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

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

The US case: the USA Freedom Act (2015)

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

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

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

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

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

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

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

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

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

The UK case: the Investigatory Powers Act (2016)

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

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

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

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

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

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

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

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

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

The German case: the BND Reform Bill (2016)

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

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

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

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

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

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

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

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

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

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

The BNDG reform has since been subject to legal contestation, particularly from civil society organizations and journalists claiming that the law violates the German Basic Law with respect to the collection of personal data and freedom of the press. On May 19, 2020, in response to a suit brought by *Reporters sans frontières*, the German Constitutional Court ruled that the law regarding the telecommunications surveillance of foreign nationals abroad does violate fundamental rights and ordered the law to be amended in conformity with constitutional rights.¹⁵ The judgment was significant because it affirmed for the first time that German authorities are bound to respect fundamental rights not only at home but also when acting abroad vis-à-vis foreigners. At the same time, it declared telecommunications surveillance of foreigners abroad to be fundamentally permissible on the grounds of the overriding public interest. In response to the judgment, the Bundestag passed a new BNDG reform law on April 19, 2021.¹⁶ The central goals of the reform are to provide a stronger legal basis for the collection of telecommunications of foreigners abroad and to introduce new control mechanisms. A newly created Independent Control Council is to be introduced to monitor the legality of BND investigations. In the view of the government, the overall aim of both of these measures is to legitimize the collection of foreign information abroad and to make the surveillance powers of the BND more precise.¹⁷

Conclusions

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

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

Notes

- 1 In my particular case, I am assuming that surveillance is an activity that the public wants checked; but it would be perfectly consistent with my argument to claim that, for example, the condoning effect can lead to normatively desirable outcomes. This might be the case, for example, when the condoning effect leads to the breakdown of a taboo or norm that was restrictive of rights (e.g., undermining norms against homosexuality).
- 2 www.intelligence.gov/index.php/ic-on-the-record-database/results/787-fact-sheet-implementation-of-the-usa-freedom-act-of-2015. See also Snowden (2019).
- 3 www.intelligence.gov/index.php/ic-on-the-record-database/results/787-fact-sheet-implementation-of-the-usa-freedom-act-of-2015.
- 4 This is also true of other legal instruments that sanction government surveillance, such as the 1981 Executive Order 12333, which authorized expansive data collection and provided the basis for subsequent surveillance-related Executive Orders (see, e.g., Tye 2014).
- 5 Provisions of the Freedom Act were set to expire in December 2019 pending reauthorization.
- 6 Coates' argument is particularly unconvincing, since one reason for the ineffectiveness of the program is its outdatedness, given the shift to internet-enabled encrypted connections.

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

References

- Albu, Oana, and Mikkel Flyverbom. 2016. “Organizational Transparency: Conceptualizations, Conditions, and Consequences.” *Business & Society* 58(2): 268–97.
- Alloa, Emmanuel. 2018. “Transparency: A Magic Concept of Modernity.” In *Transparency, Society and Subjectivity*, edited by Emmanuel Alloa and Dieter Thomä: 21–56. London: Palgrave Macmillan.
- Alloa, Emmanuel, and Dieter Thomä, eds. 2018. *Transparency, Society and Subjectivity: Critical Perspectives*. London: Palgrave Macmillan.
- Anderson, David. 2015. “A Question of Trust: Report of the Investigatory Powers Review.” June 2015, <https://terrorismlegislationreviewer.independent.gov.uk/wp-content/uploads/2015/06/IPR-Report-Web-Accessible1.pdf>.
- Anderson, David. 2016. “Report of the Bulk Powers Review.” August 2016, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/546923/56730_Cm_9326_PRINT.PDF.
- Bianchi, Andrea. 2013. “On Power and Illusion: The Concept of Transparency in International Law.” In *Transparency in International Law*, edited by Andrea Bianchi and Anne Peters: 1–20. Cambridge: Cambridge University Press.
- BND Reform Bill. 2016. “Gesetz zur Ausland-Ausland-Fernmeldeaufklärung des Bundesnachrichtendienstes vom 23.” December 2016, www.bgbl.de/xaver/bgbl/start.xav?start=%2F%2F*%5B%40attr_id%3D%27bgbl116s3346.pdf%27%5D#__bgbl__%2F%2F*%5B%40attr_id%3D%27bgbl116s3346.pdf%27%5D__1580989707655.

- Bowcott, Owen. 2019a. "Sajid Javid Wants High Court Hearing into MI5 Failures to Be Secret." *The Guardian*. May 20, 2019, www.theguardian.com/uk-news/2019/may/20/sajid-javid-high-court-hearing-mi5-failures-secret.
- Bowcott, Owen. 2019b. "MI5 Accused of 'Extraordinary and Persistent Illegality.'" *The Guardian*. June 11, 2019, www.theguardian.com/uk-news/2019/jun/11/mi5-in-court-accused-of-extraordinary-and-persistent-illegality.
- Brugger, Philipp, Andreas Hasenclever, and Lukas Kasten. 2013. "Vertrauen lohnt sich." *Zeitschrift für Internationale Beziehungen* 20(2): 65–104.
- Carnegie, Allison, and Austin Carson. 2018. "The Spotlight's Harsh Glare: Rethinking Publicity and International Order." *International Organization* 72(3): 627–57.
- Carson, Thomas. 2010. *Lying and Deception*. Oxford: Oxford University Press.
- Cauley, Leslie. 2006. "NSA Has Massive Database of Americans' Phone Calls." *USA Today*. May 11, 2006, http://usatoday30.usatoday.com/news/washington/2006-05-10-nsa_x.htm.
- Chase, Jefferson. 2016. "Germany Reforms Its Main Intelligence Service." *Deutsche Welle*. October 21, 2016, www.dw.com/en/germany-reforms-its-main-intelligence-service/a-36109764.
- Chase, Jefferson. 2017. "Merkel Testifies on NSA Spying Affair." *Deutsche Welle*. February 16, 2017, www.dw.com/en/merkel-testifies-on-nsa-spying-affair/a-37576690.
- Cook, Karen. 2001. *Trust in Society*. New York: Russell Sage Foundation.
- Cook, Karen, Russell Hardin, and Margaret Levi. 2005. *Cooperation Without Trust?* New York: Russell Sage Foundation.
- Dahl, Robert. 1971. *Polyarchy: Participation and Opposition*. New Haven: Yale University Press.
- Deutscher Bundestag. 2016. "Plenarprotokoll 18/184," <https://dipbt.bundestag.de/doc/btp/18/18184.pdf>.
- Deutsche Welle. 2016. "Parliamentary Report Finds Spying by BND on EU and NATO Governments until 2013." *Deutsche Welle*. July 11, 2016, www.dw.com/en/parliamentary-report-finds-spying-by-bnd-on-eu-and-nato-governments-until-2013/a-19393213.
- Deutsche Welle. 2017a. "NSA Spying Scandal Committee Presents Controversial Final Report." *Deutsche Welle*. June 28, 2017, www.dw.com/en/nsa-spying-scandal-committee-presents-controversial-final-report/a-39453668.
- Deutsche Welle. 2017b. "German Intelligence 'Spied on White House.'" *Deutsche Welle*. June 22, 2017, www.dw.com/en/german-intelligence-spied-on-white-house/a-39365418.
- The Editorial Board. 2015. "Mass Surveillance Isn't the Answer to Fighting Terrorism." *The New York Times*. November 17, 2015, www.nytimes.com/2015/11/18/opinion/mass-surveillance-isnt-the-answer-to-fighting-terrorism.html?_r=0.
- Fehrler, Sebastian, and Niall Hughes. 2018. "How Transparency Kills Information Aggregation: Theory and Experiment." *American Economic Journal: Microeconomics* 10(1): 181–209.
- Fenster, Mark. 2006. "The Opacity of Transparency." *Iowa Law Review* 91: 885–949, <http://scholarship.law.ufl.edu/facultypub/46>.
- Fischer, Mia. 2019. *Terrorizing Gender: Transgender Visibility and the Surveillance Practices of the U.S. Security State*. Lincoln: University of Nebraska Press.

- Fung, Archon. 2013. "Infotopia: Unleashing the Democratic Power of Transparency." *Politics & Society* 41(2): 183–212.
- Gallagher, Ryan. 2015. "Profiled: From Radio to Porn, British Spies Track Web Users' Online Identities." *The Intercept*. September 25, 2015, <https://theintercept.com/2015/09/25/gchq-radio-porn-spies-track-web-users-online-identities/>.
- Greenwald, Glenn. 2013. "Edward Snowden: NSA Whistleblower Answers Reader Questions." *The Guardian*. June 17, 2013, www.theguardian.com/world/2013/jun/17/edward-snowden-nsa-files-whistleblower.
- Griffin, Andrew. 2015. "UK Government Plan to Ban WhatsApp Dropped, as Theresa May Abandons Many of Proposed New Powers for Spies." *The Independent*. November 1, 2015, www.independent.co.uk/life-style/gadgets-and-tech/news/uk-government-plan-to-ban-whatsapp-dropped-as-theresa-may-abandons-many-of-proposed-new-powers-for-a6716756.html.
- Guariglia, Matthew. 2019. "Don't Renew Section 215 Indefinitely." *Electronic Frontier Foundation*. August 20, 2019, www.eff.org/de/deeplinks/2019/08/eff-says-no-trump-administrations-push-renew-section-215-indefinitely.
- Guttman, Amy, and Dennis Thompson. 1996. *Democracy and Disagreement*. Cambridge: Harvard University Press.
- Habermas, Jürgen. 1991. *The Structural Transformation of the Public Sphere*. Cambridge: MIT Press.
- Hardin, Russell. 2002a. *Trust and Trustworthiness*. New York: Russell Sage.
- Hardin, Russell. 2002b. "Liberal Distrust." *European Review* 10(1): 73–89.
- Hintz, Arne, and Ian Brown. 2017. "Enabling Digital Citizenship? The Reshaping of Surveillance Policy After Snowden," *International Journal of Communication* 11: 782–801.
- Hollier, James, Peter B. Rosendorff, and James Vreeland. 2011. "Democracy and Transparency." *The Journal of Politics* 73(4): 1191–205.
- Hood, Christopher. 2006. "Transparency in Historical Perspective." In *Transparency: The Key to Better Governance?*, edited by Christopher Hood and David Heald, 3–23. Oxford: Oxford University Press.
- Investigatory Powers Act. 2016. www.legislation.gov.uk/ukpga/2016/25/contents/enacted.
- Knigge, Michael. 2013. "NSA Surveillance Eroded Transatlantic Trust." *Deutsche Welle*. December 27, 2013, www.dw.com/en/nsa-surveillance-eroded-transatlantic-trust/a-17311216.
- Koivisto, Ida. 2019. "Towards Critical Transparency Studies." *Res Publica* 25(3): 439–43.
- Kydd, Andrew. 2000. *Trust and Mistrust in International Relations*. Princeton: Princeton University Press.
- Lester, Genevieve. 2015. *When Should State Secrets Stay Secret?* Cambridge: Cambridge University Press.
- Levy, Gilat. 2004. "Anti-Herding and Strategic Consultation." *European Economic Review* 48: 503–25.
- Levy, Gilat. 2007. "Decision Making in Committees: Transparency, Reputation, and Voting Rules." *American Economic Review* 97: 150–68.
- Loftus, Bethan. 2019. "Normalizing Covert Surveillance: The Subterranean World of Policing." *British Journal of Sociology* 70(5): 2079–91.

- MacAskill, Ewen. 2016. "'Extreme Surveillance' Becomes UK Law with Barely a Whisper." *The Guardian*. November 19, 2016, www.theguardian.com/world/2016/nov/19/extreme-surveillance-becomes-uk-law-with-barely-a-whimper.
- March, James, and Johan Olsen. 2011. "The Logic of Appropriateness." In *The Oxford Handbook of Political Science*, edited by Robert E. Goodin: 1–22. Oxford: Oxford University Press.
- McCarthy, Daniel, and Matthew Fluck. 2017. "The Concept of Transparency in International Relations: Towards a Critical Approach." *European Journal of International Relations* 23(2): 416–40.
- Meijer, Albert. 2014. "Transparency." In *The Oxford Handbook of Public Accountability*, edited by Mark Bovens, Robert E. Goodin, and Thomas Schillemans, 1–20. Oxford: Oxford University Press.
- Meister, Andre. 2015. "Interne E-Mail: BND und Deutsche Telekom haben auch Österreich, Tschechien und Luxemburg abgehört (Update)." *Netzpolitik.org*. May 15, 2015, <https://netzpolitik.org/2015/interne-e-mail-bnd-und-deutsche-telekom-haben-auch-oesterreich-tschechien-und-luxemburg-abgehoeert/>.
- Meister, Andre. 2016a. "Secret Report: German Federal Intelligence Service BND Violates Laws and Constitution by the Dozen." *Netzpolitik.org*. September 2, 2016, <https://netzpolitik.org/2016/secret-report-german-federal-intelligence-service-bnd-violates-laws-by-the-dozen/>.
- Meister, Andre. 2016b. "Das neue BND-Gesetz: Alles, was der BND macht, wird einfach legalisiert. Und sogar noch ausgeweitet." *Netzpolitik.org*. June 30, 2016, <https://netzpolitik.org/2016/das-neue-bnd-gesetz-alles-was-der-bnd-macht-wird-einfach-legalisiert-und-sogar-noch-ausgeweitet/>.
- Nakashima, Ellen. 2019. "Repeated Mistakes in Phone Record Collection Led NSA to Shutter Controversial Program." *The Washington Post*. June 25, 2019, www.washingtonpost.com/world/national-security/repeated-mistakes-in-phone-record-collection-led-nsa-to-shutter-controversial-program/2019/06/25/f256ba6c-93ca-11e9-b570-6416efdc0803_story.html.
- Obama, Barack. 2013. "Transcript: Obama's Remarks on NSA Controversy." *Wall Street Journal*. June 7, 2013, <https://blogs.wsj.com/washwire/2013/06/07/transcript-what-obama-said-on-nsa-controversy/>.
- Obama, Barack. 2015. "Statement by the President on the USA FREEDOM Act." *The White House*. June 2, 2015, <https://obamawhitehouse.archives.gov/the-press-office/2015/06/02/statement-president-usa-freedom-act>.
- Office of the Director of National Intelligence. April 2018. "Statistical Transparency Report Regarding Use of National Security Authorities Calendar Year 2017." www.dni.gov/files/documents/icotr/2018-ASTR----CY2017----FINAL-for-Release-5.4.18.pdf.
- O'Neill, Onora. 2002. *A Question of Trust: The BBC Reith Lectures 2002*. Cambridge: Cambridge University Press.
- Perraudin, Frances. 2019. "Liberty Loses High Court Challenge to Snooper's Charter." *The Guardian*. July 29, 2019, www.theguardian.com/law/2019/jul/29/liberty-loses-high-court-challenge-to-snoopers-charter.
- Peters, Anne. 2013. "Towards Transparency as a Global Norm." In *Transparency in International Law*, edited by Andrea Bianchi and Anne Peters: 534–607. Cambridge: Cambridge University Press.

- Pozen, David. 2020. "Seeing Transparency More Clearly." *Public Administration Review* 80(2): 326–31.
- Pozen, David, and Michael Schudson. 2018. "Introduction." In *Troubling Transparency: The History and Future of Freedom of Information*, edited by David Pozen and Michael Schudson: 1–10. New York: Columbia University Press.
- Prat, Andrea. 2005. "The Wrong Kind of Transparency." *American Economic Review* 95: 862–77.
- Priest, Dana, and William Arkin. 2011. *Top Secret America: The Rise of the New American Security State*. New York: Little, Brown, and Company.
- Rathbun, Brian. 2012. *Trust in International Cooperation*. Cambridge: Cambridge University Press.
- Rawls, John. 1971. *A Theory of Justice*. Cambridge: Harvard University Press.
- Rawls, John. 1993. *Political Liberalism*. New York: Columbia University Press.
- Riechmann, Deb. 2018. "Cost of Snowden Leak Still Mounting 5 Years Later." *Associated Press*. June 4, 2018, <https://apnews.com/797f390ee28b4bfb0e1b13cfedf0593/Costs-of-Snowden-leak-still-mounting-5-years-later>.
- Risen, James, and Eric Lichtblau. 2005. "Bush Lets US Spy on Callers Without Courts." *The New York Times*. December 16, 2005, www.nytimes.com/2005/12/16/politics/16program.html?pagewanted=all.
- Savage, Charlie. 2019. "Trump Administration Asks Congress to Reauthorize N.S.A.'s Deactivated Call Records Program." *The New York Times*. August 15, 2019, www.nytimes.com/2019/08/15/us/politics/trump-nsa-call-records-program.html.
- Schneier, Bruce. 2013. "The Only Way to Restore Trust in the NSA." *The Atlantic*. September 4, 2013, www.schneier.com/essays/archives/2013/09/the_only_way_to_rest.html.
- Schneier, Bruce. 2015. *Data and Goliath*. New York: Goliath.
- Snowden, Edward. 2019. *Permanent Record*. New York: Macmillan Publishers.
- Spiegel International. 2013a. "Merkel Comments on Spying Allegations." *Spiegel International*. October 24, 2013, www.spiegel.de/international/germany/merkel-comments-on-allegations-the-us-spied-on-her-cell-phone-a-929870.html.
- Spiegel International. 2013b. "German Trust in United States Plummets." *Spiegel International*. November 8, 2013, www.spiegel.de/international/germany/nsa-spying-fallout-majority-of-germans-mistrust-united-states-a-932492.html.
- Steinke, Ronen, and Reiko Pinkert. 2016. "Früherer BND-Chef kritisiert Kontrollsystem des deutschen Geheimdiensts." *Süddeutsche Zeitung*. September 22, 2016, www.sueddeutsche.de/politik/bundesnachrichtendienst-angriff-auf-die-lauscher-1.3174459.
- Strobel, Warren, and Patricia Zengerle. 2015. "Obama's Signature on the Freedom Act Reverses Security Policy That's Been in Place since 9/11." *Business Insider*. June 2015, www.businessinsider.com/obamas-signature-on-the-freedom-act-reverses-security-policy-thats-been-in-place-since-911-2015-6.
- Strobel, Warren, and Dustin Volz. 2019. "NSA Recommends Dropping Phone-Surveillance Program." *The Wall Street Journal*. April 24, 2019, www.wsj.com/articles/nsa-recommends-dropping-phone-surveillance-program-11556138247.
- Tye, John Napier. 2014. "Meet Executive Order 12333: The Reagan Rule That Lets the NSA Spy on Americans." *The Washington Post*. July 18, 2014, www.washingtonpost.com/opinions/meet-executive-order-12333-the-reagan-rule-that-lets-the-nsa-spy-on-americans/2014/07/18/93d2ac22-0b93-11e4-b8e5-d0de80767fc2_story.html.

- UK Home Office. 2017. *Investigatory Powers Act 2016 Consultation: Codes of Practice*, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/593725/IP_Act_codes_consultation_Feb2017_FINAL_WEB.pdf.
- Uslaner, Eric M. 2002. *The Moral Foundations of Trust*. Cambridge: Cambridge University Press.