Why a militantly democratic lack of trust in state surveillance can enable better and more democratic security

Miguelángel Verde Garrido

Introduction

Contemporary societies are characterized by a global culture of surveillance, that is, structured by multiple social, economic, and political policies and practices that deploy surveillance to achieve various goals (Verde Garrido 2015). Surveillance can be understood as “the operations and experiences of gathering and analysing personal data for influence, entitlement, and management,” mostly performed by states and corporations, but “may also be carried out by people in everyday life” (Lyon 2018, 6). Additionally, there exists a politically and economically “neutral watching or sensing,” termed “veillance,” which eschews social hierarchies and asymmetric relations of power and knowledge (Verde Garrido 2015, 163–4). Considering these different modalities of collection, analysis, and application of physical, social, and digital data is crucial to understanding contemporary notions and practices of privacy, security, and trust (Verde Garrido 2015, 164). When Edward Snowden’s revelations were reported, it became evident that “global surveillance is not only confined to intelligence agencies’ deployment of surveillance technologies, but extends also to the very cultural and economic characteristics of contemporary society” (Verde Garrido 2015, 155). Global public outrage followed the realization that mass surveillance infringed on the right to privacy as well as other vital human rights (Verde Garrido 2015, 164). In order to contest these violations and abuses, civil societies have expanded their counter-surveillance strategies and practices, strengthened their political agency with a nascent digital agency, and furthered demands for the rule of law and democratic oversight (Verde Garrido 2015, 164–5). This chapter focuses on the nature and particulars of democratic oversight of surveillance policies and practices, questioning the extent to which these require trust and transparency to be most effective. It is important to remember that “the towering institutions and processes of high technology and global government [...] are not relentless and invincible” and that “ordinary people, often acting in concert” can contribute constructively to the “reimagination and shaping” of contemporary technological policies and practices (Lyon 2018, 147). Bearing

that in mind, the first section explores trust and transparency generally and in relation to surveillance, clarifying the nature of intelligent accountability. The second section explains the manner in which, counterintuitively, a lack of trust informs several democratic institutions as well as the governmental, legal, and juridical notion of militant democracy. The notion of militant democracy advances the idea that a liberal democracy can defend its constitutional order from the threat of authoritarian political movements and that it can do so through enacting political and legal measures that fulfill three criteria: legitimacy, legality, and necessity. This section proposes that a militantly democratic approach within civil society can further ensure that oversight of surveillance is effective, democratic, and upholds civil liberties and human rights. In order to illustrate this approach, the third section considers specific instances of surveillance in various countries: Germany, Poland, and the United States, which share the political encroachment of far-right populism, although to varying degrees. This section critically analyzes specific instances of surveillance policies and practices in these countries and notes how these are ideologized to varying extents and fail to fulfill the three criteria promoted by a militantly democratic oversight. This chapter ends by offering some conclusions and recommendations on ensuring a democratic oversight of surveillance policies and practices.

On the relation of trust and transparency to oversight of surveillance

The Snowden revelations provoked a global debate on the nature and implications of surveillance for state—as well as corporate—intelligence functions. There are questions about the levels of privacy intrusion, the “accountability” of intelligence and security functions, the “efficiency of bulk surveillance practices and their compatibility with fundamental rights,” and the manner in which “surveillance-intensive methods” impact the social fabric of democratic societies (Ball et al. 2019, 3; Wetzling and Vieth 2018, 10). The ongoing debate has not changed that “all major democracies allow their national intelligence services to intercept communications data in enormous quantities” or that court rulings admonish them “for flaws or shortcomings” in an oversight regime that must become “more rigorous and effective” (Wetzling and Vieth 2018, 10). Understanding that democratic oversight acts as an effective bulwark against “the erosion of fundamental rights should a government be infested with the illiberal virus that is currently rampant” proves crucial (Wetzling and Vieth 2018, 6). Because “temptations to abuse privileges such as government secrecy are omnipresent,” it is important to remember that “democratic intelligence governance cannot be taken for granted” and “the legitimacy of intelligence action must constantly be earned” (Wetzling and Vieth 2018, 11–12). Therefore, democratic oversight of state—as well as corporate—policies and practices of surveillance should

consider dynamics of trust and trustworthiness and learn from democratic institutions and measures built upon a constructive lack of trust.

Trust can be understood as the belief and confidence on the part of a person or party (trustor) that another person or party (trustee) will reliably do what they have stated. There is never a complete guarantee that people or parties will be trustworthy, so every interaction requires granting trust to a certain extent and involves a risk that others prove that the granted trust was misplaced. The “most systematic evidence” to determine whether contemporary society is experiencing a “crisis of trust” comes from public opinion polls and similar academic research, but these surveys fail to realize their own ambiguities (O’Neill 2002, 3–4). First, surveys do not recognize that people “seek to place trust in a differentiated way” and do not grant “every instance of a certain type of official or [...] person” the same level of trust. Second, surveys seldom ask respondents about specifics. Questions about trust in this or that type of person should be followed by: “To do what?” (O’Neill 2013). Consequently, the status of trust in contemporary societies is better illustrated by the fact that “we still constantly place trust in many of the institutions and professions that we profess to not to trust” (O’Neill 2002, 4).

Prompted by worries about what states and corporations may do with their data, more and more citizens and consumers have “sought ways to avoid observation by specific people, organizations or the government.” These concerns come from “a lack of confidence in the security of everyday communications channels and a lack of trust in all kinds of organizations to protect their data” (Lyon 2018, 67–8). The Snowden revelations showed the limitations of data protection legislation and the reduction of corporate sovereignty over data and “profoundly undermined the trust and confidence” that private lives, human rights, and civil liberties are respected (Bigo et al. 2013, 1–4). Consequently, citizens and consumers wonder whether they should “ever trust that their information is safe on the Web.” While the “main byproduct” of digital technologies—data—has great value for “law enforcement, industry, advertising, science, and other fields,” it is even more valuable for its owners, representing the “center of trust” of their “interaction with technology.” Since individuals must trust their interlocutors to provide them with data, government or corporate mishandling of data implies to “completely mishandle the trust.” Ultimately, “the lack of clarity and consensus on rules for government access to data,” added to the “constant stream of data breaches, intrusions into government systems, and attacks on service providers,” has led civil society to experience “fear and paranoia” and lose “trust in technology” (Jordan 2015). Solely corporate surveillance policies and practices have also impacted citizen and consumer trust significantly. Internet giants such as Facebook and Google, following a business model and logics of data extraction and accumulation termed “surveillance capitalism,” undermine relationships of trust by eschewing “the mutual dependencies and reciprocities” that hold other kinds of corporations accountable. Thriving on

the “public’s ignorance” of their imperatives and operations and offering minimal “meaningful options for privacy self-management,” these corporations establish “unprecedented concentrations of information power,” entrench new structural asymmetries of knowledge, power, and trust, and obfuscate themselves from transparency (Zuboff 2015, 83, 85–6).

Citizens and consumers have become aware that states and corporations deploy mass surveillance and that they employ mendacities and chicaneries in order to do so unnoticed. Lack of trust has grown worldwide as a “reasonable response to growing untrustworthiness” (O’Neill 2002, 12). Accordingly, states and corporations must provide citizens and consumers not only with information that claims they are trustworthy but also “the means to judge that information” independently as well (O’Neill 2002, 17). Transparency on its own does not allow others to fully determine trustworthiness or whether to grant trust and rarely means more than that certain information is being made publicly available. More effective is ensuring that the information in question is intelligible as well as assessable. Oversight of surveillance that not only demands information on specific practices but that also informs about the goals of the surveillance in question can be understood as establishing “intelligent accountability” (O’Neill 2017).

Complete openness and transparency have contributed very little to building or regaining public trust. Quite often, “trust seemingly has receded as transparency has advanced.” This is not because transparency “destroys secrecy,” but rather because restoring trust requires those who are untrustworthy to “reduce deception and lies rather than secrecy” (O’Neill 2002, 18). Most important for reducing asymmetries of power and knowledge resulting from asymmetric kinds of transparency are “legal measures to prohibit certain kinds of surveillance and to impose penalties on those whose watching transgresses acceptable transparency” (Lyon 2018, 162). There is no benefit in granting trust blindly: “well-directed trust and [...] well-directed mistrust” are desirable because “we want mistrust in the untrustworthy [...] and trust in the trustworthy” (O’Neill 2017). States and corporations who deceive citizens and consumers are untrustworthy and, hence, do not deserve trust. For these various reasons, addressing states and corporations with a lack of trust can, counterintuitively, prove to be a constructive approach.

A constructive lack of trust and a militantly democratic approach within civil society

The previous section explained that trust is granted without complete guarantees, relying on ostensible trustworthiness. Awareness of the nature and extent of surveillance has led citizens and consumers to lose much trust in states and corporations. This lack of trust comes not only from state and corporate failure to fulfill promises about how surveillance is deployed but also from their obscuring facts about why: namely, to establish new asymmetries

of power and knowledge. Ensuring transparency is neither sufficient for trust to be built or recovered nor is it desirable unless there is intelligent accountability: clearer explanations and more opportunities to contest and decide which goals are desirable in relation to surveillance policies and practices. This section will explain why a lack of trust informs certain democratic principles and institutions, how it can be embodied by a militantly democratic civil society, and why it can prove to be constructive for oversight of surveillance.

Liberal democracies have formal institutions built upon a constructive lack of trust. Examples include the separation of powers, secret ballots, and whistleblowing. The separation of powers implies a lack of trust because it recognizes that dividing government into branches, separate and independent, is crucial to avoiding an unchecked concentration of power. Secret ballots, which exist in a number of voting systems, also imply a lack of trust inasmuch as they acknowledge that mechanisms to avoid excessive influences are required. Institutional whistleblowing implies a lack of trust since it accepts that wrongdoings within states—as well as corporations—may be intentionally obscured to avoid consequences. Therefore, protections are established to shield whistleblowers from suffering retaliatory measures, and protocols are designed to investigate and right these wrongdoings. Civil societies can learn to constructively apply a lack of trust to oversight of security and intelligence functions, even if certain levels of secrecy are obligatory and limited transparency is the norm.

Contrary to arguments that security and privacy are incompatible, efforts to simultaneously ensure privacy and security can be valuable in terms of “public policy” since addressing the intrusiveness of certain instances of security and surveillance can maximize “security benefits and privacy protections” (Ball et al. 2019, 14). “Good oversight is good security” because it “pushes governments to be as effective as possible in allocating their resources and selecting their targets” (Wetzling and Vieth 2018, 87). Furthermore, because of the contemporary drift toward authoritarianism within liberal democracies (Zeid 2018; Human Rights Watch 2018; Amnesty International 2018; Freedom House 2018), a militantly democratic approach to oversight is crucial because it can help ensure better and more discerning transparency and technical literacy, hold states intelligently accountable for their relations with corporations and vice versa (Jordan 2015; Schneier 2015), and enact modernized legislation addressing the complexities of domestic as well as global surveillance.

Karl Loewenstein developed the notion of militant democracy (i.e., *streitbare* or *wehrhafte*, defensive, *Demokratie*) during the summer of 1937, shortly before the totalitarianisms of fascism and communism violently set off World War II. He addressed with grave concern why numerous states were experiencing authoritarian drifts, and several others had already fully devolved into authoritarianism (Loewenstein 1937a, 1937b). Loewenstein proposed that liberal democracies should “become militant” in defense of

their constitutional values: that is, these states needed to enact and implement constitutional political and legislative measures restricting the manners in which authoritarian political movements weaponized democratic freedoms, rights, and institutions in order to consolidate power and ultimately suspend them (Loewenstein 1937a, 422–3, 438–9). Militant democracy is a decisive response to the proven untrustworthiness of authoritarian politics.

Loewenstein differentiated constitutional governments from authoritarian ones, noting that the former signified the rule of law, rational and calculable administration, and the protection of private law and fundamental rights. The latter, in contrast, replaced the rule of law with “legalized opportunism,” merged private law into public law, and collapsed fundamental rights and the rule of law, their interest being to achieve “unchallengeable command.” Because “no government can rely only on force or violence,” authoritarianism relied strongly on raw “emotionalism,” especially nationalist fervor and a strategic combination of intimidation, “terrorization,” and coercion (Loewenstein 1937a, 417–8). Constitutional governments can be understood as liberal democracies, upholding fundamental rights such as the freedom of speech and the press or the freedom to hold public office, which are not only liberties and freedoms but also civil and political rights (Altman 2017). While constitutional and authoritarian governments contrast starkly, there is also a certain kind of government considered mostly democratic, although a “new type of ‘authoritarian’ or ‘disciplined’ democracy” (Loewenstein 1937b, 644). Nowadays, such a “hybrid” regime, neither fully democratic nor fully autocratic, is termed an “anocracy.” These regimes may uphold a number of freedoms while constraining others and may limit electoral competition as well as prevent political accountability in order to maintain power (Colomer et al. 2016, 19–20).

Authoritarianism adapted perfectly to democracy and its tolerance for other competing political ideologies. Employing novel “technical wonders” and democratic institutions, authoritarian regimes spread discourses that inflamed “emotionalism in its crudest and its most refined forms” among the masses, set different groups against each other, and discredited “the democratic order” as “unworkable.” Liberal democracies responded slowly, concerned that restricting authoritarian “use of democratic institutions” weakened their legality. Loewenstein proposed that constitutional governments wishing to uphold their own values needed to act upon their lack of trust in the outward conformance to “the principles of legality and free play of public opinion” of authoritarian political movements and confront their dangerous political techniques. It is in this sense that “democracy must become militant” (Loewenstein 1937a, 423–4).

Liberal democracy cannot prove the superiority of its achievements and counter emotionalism by means of the same emotional techniques. Rather, it must employ “political and legislative” measures appealing to “reason” (Loewenstein 1937a, 428). Politically, the approach can be to establish “a

united and uniform action among the democratically-minded sections of the people"; legislatively, it can be to enact antiauthoritarian laws and regulations "without flagrant violation of democratic principles," enabled by means of "parliamentary vote and public opinion at large" (Loewenstein 1937a, 429–30, 438–9). Political and civil restrictions serve the purpose of "ultimately preserving these very fundamentals," and liberal democratic constitutions and governance anticipate "emergency powers." Loewenstein was convinced—and World War II validates his contention—that such measures were warranted because authoritarianism had "declared war on democracy." Liberal democracies had to "live up to the demands of the hour" and make "every possible effort" to survive, establishing political unity and counterintuitively enacting legislation to confront authoritarian political movements, even when it appeared to imply "the risk and cost of violating fundamental principles" (Loewenstein 1937a, 432).

Defending democracy through restricting fundamental institutions and rights can dangerously lead to the opposite: weakening it and making it more susceptible to authoritarianism (Invernizzi Accetti and Zuckerman 2017, 182, 183–4). Loewenstein recognized that several European states hollowed out their constitutionality and destroyed the rule of law to the extent of becoming anocracies and authoritarians (Loewenstein 1937b, 638–40). This is an important lesson in the context of securitization and the expansion of surveillance since history shows that authoritarianism often encroaches through claims and proposals that are seemingly those of embattled liberal democracies. Nowadays, the emergency powers of the "state of exception" have increasingly become a "dominant paradigm of government" even in constitutional governments (Agamben 2005, 1–2). Their normalization should be viewed with caution as these can radically alter constitutional forms and establish the state of exception as the "threshold of indeterminacy between democracy and absolutism" (Agamben 2005, 2–3). Accordingly, it is important to clarify the legal and juridical understanding that states and institutions have of a "democracy capable of defending itself" (O'Connell 2009, 84).

The Basic Law of Germany and international frameworks such as the Universal Declaration of Human Rights (UDHR) and European Convention of Human Rights note, respectively, the duty to prevent "enemies of democracy" from employing the "rights and freedoms of democracy to undermine it"; that human rights cannot be used or abused to "undermine the purposes of the United Nations"; and that parties to the Convention cannot destroy the "rights and freedoms" that it sets forth (O'Connell 2009, 84–5). General legal and juridical understanding is that restrictions to rights must satisfy three criteria: these should be "for a legitimate purpose, prescribed by law and necessary in a democratic society." (O'Connell 2009, 86). Accordingly, the language of militant democracy is used to confront political violence, to combat discriminatory and extremist movements, to secure the transition to democracy in an anocracy, and to ensure constitutional or human rights.

Even so, restrictions and preventative measures are only legitimate and justified when states or institutions prove their commitment to democratic means and goals. History also shows that “even established democracies fall short of the ideal” of liberal democracy (O’Connell 2009, 86–90). Altogether, a militantly democratic approach to the oversight of surveillance within civil society can constructively employ a lack of trust in order to determine whether state and corporate policies and practices satisfy the three criteria of legitimacy, legality, and necessity. Doing so further establishes intelligent accountability and ensures the defense of liberal democracy while upholding human rights, civil liberties, and privacy and data protections.

Oversight of surveillance policies and practices in times of authoritarian drift

The previous section explained that various established democratic institutions are built upon a constructive lack of trust so as to check abuses of power. Questioning whether surveillance policies and practices can further defend liberal democracy is especially relevant in contemporary politics, where authoritarian drift is rampant. Militant democracy ensures constitutional government, avoids liberal democracy devolving into anocracy, and checks authoritarianism and its divisive emotionalism. The three criteria that determine whether militantly democratic means are justified can also be applied to the oversight of surveillance. Considering the above, this section will explore instances of surveillance policies and practices in Germany, Poland, and the United States—countries experiencing the political encroachment of far-right populism to varying degrees. It will critically analyze the policies and practices in question so as to clarify the manner in which these are also ideologized to varying extents and fail to fulfill the three criteria required for a militantly democratic oversight of surveillance.

Germany: oversight of intelligence and law enforcement agencies

The historical experiences of having devolved into far-right as well as far-left authoritarianisms have taught Germany the importance of militantly democratic institutions. Once the National Socialist Third Reich was defeated, the Federal Republic of Germany (1949) established the Federal Office for the Protection of the Constitution (BfV) through its Basic Law. A domestic security and counterintelligence agency, the BfV defends the “free democratic basic order” of Germany, monitors anticonstitutional activities, mostly those of far-left and far-right groups, and formally embodies militant democratic principles. The agency reports to the Ministry of Interior, and its principal executive agent is its president. A critical analysis of the case of former BfV president Hans-Georg Maaßen serves to clarify that a militantly democratic approach is required even within the oversight of the surveillance deployed

by an ostensibly militantly democratic institution. Maaßen, president of the agency from August 2012 to November 2018, was fired when he publicly contradicted the federal government by downplaying antimigrant violence that occurred during protests against a murder in the town of Chemnitz. When several government officials, including Chancellor Angela Merkel, condemned the violence, Maaßen not only argued that journalistic reporting on far-right gangs hunting foreigners in the streets was “deliberate misinformation,” but also—astonishingly—claimed that “arrest records, various videos, media reports and photos of protestors doing the Hitler salute” were not “reliable information” (Jordan 2018).

The year before, however, Maaßen showed no qualms about arguing without any kind of reliable information for the expansion of surveillance of the “wives and children of German ‘IS’ fighters” returning to the country, stating that the agency should “keep them in our sights” since they “could pose a risk” (Deutsche Welle 2017). The children, he warned, “could be living time bombs [...] brainwashed with a mission to carry out attacks” (Shalal and Siebold 2018), and therefore were not an “insignificant potential threat” (Deutsche Welle 2018). The state had already lowered its age limit for surveillance from 16 to 14 in 2016, but Maaßen argued that it should be expanded to include children under the age of 14. A civil rights organization explained that it was “unreasonable to consider children a threat to the constitutional order” and that their surveillance represented “a massive violation of their fundamental rights” (Deutsche Welle 2018). Remarkably, earlier that year, a former leader of the youth wing of the right-wing Alternative for Germany (AfD) denounced Maaßen for allegedly advising party leaders on strategies to “avoid being placed under surveillance.” As reporting on Maaßen’s contradictory policies intensified, it was revealed that the BfV had “failed for months to act on [...] concerns about local [AfD] youth chapters” (Reuters 2018).

The BfV denied the leaks and stated that suspicions of party sympathies were “entirely without foundation” (Koch and Neuerer 2018). Governmental as well as public outcry ensured the removal of Maaßen, but interior minister Horst Seehofer proposed he become “deputy interior minister”—which was “technically a promotion with a pay rise” (Associated Press 2018a). When this backfired, Seehofer proposed Maaßen become his “special advisor” (Associated Press 2018a). Even more political and public outcry followed, especially when BfV agents blew the whistle on a video where Maaßen told “European domestic spy chiefs” that the Social Democratic Party (SPD), Germany’s ruling coalition partner, were “radical left-forces” conspiring against him. Only then did Seehofer send Maaßen into “early retirement” (Escritt 2018).

A militantly democratic approach to oversight of surveillance is crucial because the ideologization of policies and practices is a threat to ensuring security. Thomas Haldenwang, the new BfV president, announced a significant expansion of agents monitoring far-right groups, explaining that the

violence in Chemnitz illustrated “developments in right-wing extremism,” as numbers were rising and more than half were “violence-oriented” (Associated Press 2018b). Questioned whether the AfD has contributed to this growth, he replied that “in any case, it doesn’t seem to be detrimental.” The BfV announced surveillance of the far-right party, AfD critics claiming “an increasing blurring of boundaries between the party and the extreme right neo-Nazi scene” (Associated Press 2018b). The monitoring included AfD member Björn Höcke—a “driving force” in moving the party to “the extreme right” and “a threat to the liberal democratic principles of Germany’s constitution”—as well as the party’s youth wing (JA) (Connolly 2019). When Walter Lübcke, a conservative pro-refugee politician, was murdered by a right-wing extremist, the debate illustrated a lack of trust whether the BfV had “underestimated the threat posed by the militant far right” (Oltermann 2019). The agency’s annual report, mostly written while Maaßen was BfV president, had failed to mention Nordkreuz, a far-right extremist group shown to have “close links to the police and military,” which accessed police records to create a “death list” including “almost 25,000 names and addresses of local politicians” who had contributed to “civil efforts during the refugee crisis in 2015” (Oltermann 2019). Investigations of Nordkreuz further revealed members to be in the military, law enforcement, and reservists and that it was stockpiling of weaponry, ammunitions, and even body bags and quicklime to dissolve the corpses of “political enemies” (Bennhold 2020).

News coverage and public outcry led the federal government to propose 300 additional positions within the BfV to better monitor right-wing extremism, focus on early detection of radicalization of law enforcement and military personnel, and strengthen international cooperation with similar state agencies (Wiedmann-Schmidt 2019). This militantly democratic approach to oversight remains necessary, especially considering leaked classified documents that reveal authorities arguing to allow state security and intelligence “to read encrypted chats” and reports that the BfV is considering “artificial intelligence to identify suspicious postings online and on social media” (Der Spiegel 2019). Such efforts to further automate surveillance practices risk undermining intelligent accountability in the absence of militantly democratic oversight.

Oversight of surveillance technologies outsourcing

Poland not only has a history of occupation by far-right and far-left authoritarianisms, but it also had a pivotal role in the former Soviet sphere’s transition toward democracy. In recent years, however, the European Union launched an unprecedented procedure to monitor “threats to the rule of law in Poland” because of measures enacted by the Law and Justice (PiS) party, which presently rules the government (Jankovic 2016, 51). A critical analysis of state untransparency and prevention of intelligent accountability

over surveillance technology in Poland sheds light on why a militantly democratic approach is recommended not only within civil society but also within the political opposition when there is an institutional lack of oversight. Importantly, the measures enacted by the PiS include nonacceptance of elected judges, which effectively paralyzed the Constitutional Tribunal, and “new laws relating to the media, civil service, the police, and prosecution” that allowed security and intelligence services to “obtain information from internet providers without a court order” or informing those surveilled (Jankovic 2016, 55, 58). Considered altogether, “the line between democracy and dictatorship seems to be very thin” and also “fragile and profoundly susceptible to subversion” (Jankovic 2016, 64). Consequently in 2017, the European Commission activated Article 7 of the Treaty on European Union against the country for “persistently flouting democratic rules.” Years later, the vice president of the European Commission warned that it “had not yet had any impact on Warsaw’s behavior” (Reuters 2019).

To be clear, the expansion of surveillance in Poland started before the PiS came to power, but the party’s willingness to threaten the rule of law and the independence of the judicial branch has allowed this trend to intensify. The state has exploited events such as the 2016 North Atlantic Treaty Organization (NATO) summit or the papal visit to further surveil foreigners without judicial warrants and extend the time that suspects can be detained without charges (Szary 2016). In anticipation of the 2018 Conference of the Parties (COP) to the United Nations Framework Convention on Climate Change (UNFCCC), agencies were authorized to “collect, obtain, gather, verify, process and use information, including personal data about persons posing a threat to public safety and order, including outside the borders of the Republic of Poland” with few restrictions (Aronoff 2018). Furthermore, information on foreigners attending the conference, including “police records and intelligence gathered by state surveillance,” could be collected without their “knowledge or consent” and stored several months after the event ended. Various UN bodies and special rapporteurs sent concerned letters to Polish authorities, warning that the measures “may lead to human rights violations” as acts of reprisal against individuals “for their cooperation with the United Nations” (Aronoff 2018).

Surveillance policies and practices in Poland, as with many postcommunist states, were characterized by “swift commercialisation of [...] the police state’s security apparatus” during the political transition, blurring the “lines between the private security industry” and state security and intelligence agencies (Łoś 2018, 363–4). Consequently, members of this industry “became the primary providers of risk definitions and risk management technologies” (Łoś 2018, 364). Unsurprisingly, Poland has continued expanding its surveillance capabilities by outsourcing to national and international corporations. According to a technical and academic report, Poland has deployed “Pegasus” surveillance malware created by NSO Group, a surveillance technology corporation based

in Israel (Marczak et al. 2018). The report led journalists and political opposition to inquire whether the malware was purchased and deployed by security and intelligence agencies. It is noteworthy that NSO Group has a scandalous record of its technologies being deployed to violate human rights and civil liberties (Gera 2019; Bing and Satter 2019). For this reason, a lack of trust in state purchases and deployments of Pegasus is entirely advisable. A Polish NGO defending freedom and human rights from contemporary technological threats argues that institutional lack of oversight of surveillance is the reason for the lack of clarity on whether the Central Anti-Corruption Bureau (CBA) and/or the security and intelligence agencies purchased and deployed malware such as Pegasus (Panoptikon Foundation 2019). The Civic Platform (PO) opposition party has publicly supported the interpretation that the purchase and deployment of Pegasus would be illegal since there is “no place for such systems in democratic countries respecting rule of law” because the malware would presumably “be used by secret police under the radar of the courts” (Kość 2019).

A militantly democratic approach is evident within political opposition and civil society attempts at oversight of surveillance policies and practices—and is recommended. Organizations such as Panoptikon Foundation have scrutinized previous instances of state untransparency and have questioned whether it is defensible to purchase security and intelligence goods from corporations that enable the surveillance policies and practices of authoritarian regimes and obfuscate the availability of such surveillance capabilities (Panoptikon Foundation 2015). Furthermore, they argue, the deployment of such surveillance technologies is worrisome for at least four other reasons: first, deploying Pegasus, “even if a court order were obtained,” would most likely “not [be] legal under Polish law”; second, “oversight over secret services” in Poland is lacking, and “there is no obligation to inform people” who are being surveilled; third, parliamentarians are concerned these surveillance technologies are being deployed “against independent journalists” and “opposition politicians”; and, fourth, Poland “does not follow human rights standards,” a claim supported by the fact such malware is “used by authoritarian regimes to spy on citizens” (Gera 2019). Civil society and the political opposition should continue their attempts at oversight with a militantly democratic approach, especially considering that Prime Minister Mateusz Morawiecki merely responded that everything “will be explained in due time” (Kość 2019), and Deputy Prime Minister Jacek Sasin entirely dismissed any concerns, offering discursive platitudes as divisive as the claim that “honest citizens” do not to worry about such matters (Kość 2019).

United States: oversight of governmental agencies and outsourcing of surveillance and intelligence technologies and services

The United States has not experienced devolution from liberal democracy to anocracy or authoritarianism. However, its global hegemony depends not

only on its economy and culture but also on the power of its military and intelligence. Moreover, no other liberal democracy has more state and corporate surveillance capabilities than the United States. A critical analysis of how these functions are increasingly outsourced clarifies why a militantly democratic approach to oversight is vital to limiting abuses of power and defending the political agency of civil society—especially those resulting from the ideologization of surveillance. It is clarifying to consider the ways in which immigration is being ideologized at the same time as securitized. Ongoing debate, domestically and globally, on this matter intensified after the revelation that thousands of immigrant children were separated from their families and detained in facilities without relatives (Aguilera 2019). This family separation practice was later disclosed as a “migration deterrent” within the wider scope of a “zero tolerance” antiimmigration policy (Miroff and Dawsey 2019). The extension of the state and corporate surveillance assemblage built in order to realize these and other immigration policies and practices is entirely unprecedented (Fox Cahn 2019).

This state–corporate nexus partners federal departments and agencies such as Homeland Security (DHS) and Immigration and Customs Enforcement (ICE) with corporations as recognizable as Amazon, Microsoft, and Hewlett-Packard (Corbett 2018) as well as other, more obscure, ones. Palantir Technologies, focused on big data mining and analytics, is such a corporation. The state has extensively outsourced matters concerning the military, intelligence, and law enforcement agencies to it. When public outrage against family separation began, Palantir insisted that it provided goods and services for “cross-border criminal investigations,” not “interior civil immigration enforcement”—i.e., the deportation and detention of undocumented immigrants. However, an advocacy network obtained documents revealing that ICE employs “Investigative Case Management” (ICM), a Palantir software platform, to build “profiles of immigrant children and their family members” and facilitate their arrest and prosecution. The corporation’s untrustworthiness was further exposed by the fact that ICM allows ICE agents to also access the intelligence platforms of various “other federal and private law enforcement entities” (Biddle and Devereaux 2019).

The function creep and drift of this surveillance assemblage is evidenced by the fact that fusion centers established for counterterrorism “not only monitor and target immigrants” but political activists as well. Diverse kinds of biometric information are collected in “cases of mass arrests at protests,” stored, analyzed, and then shared with a multitude of federal agencies (Corbett 2018). Surveillance of those documenting, protesting against, or working with the consequences of present-day immigration policy goes further. A DHS whistleblower leaked documents revealing a secret database on people concerned with immigration to the United States as well as the migrant caravan approaching San Diego from Central America in late 2018. Alerts were placed on some of the passports of these concerned individuals—who

included political activists, lawyers, journalists, advocates, and social media influencers—to screen them at the border with Mexico and stop them from entering and working there as journalists or lawyers. Others were “arrested, interviewed, or had their visa or [expedited travel] pass revoked.” These revelations confirmed previous reports from journalists, who denounced becoming “targets of intense inspections and scrutiny by border officials.” Besides ICE, the database was made available to other federal law enforcement agencies, including Customs and Border Protection (CBP). The whistleblower warned that the creation of the dossiers constituted an abuse, since the DHS focuses on “criminal investigation” and not “intelligence.” When local news media confronted the CBP with the leak, it confirmed neither the authenticity nor the legality of the dossiers. The agency only stated that assaults on law enforcement agents were made after the caravan arrived and the border wall was breached, which represented crimes and a “risk to public safety.” As such, the event was being “routinely monitored and investigated” and evidence was collected “to determine if the event was orchestrated.” Once the leak was reported, the CBP stated that those surveilled “were present during the violence” (Jones et al. 2019).

When dozens of civil society and nongovernmental organizations as well as senators sent letters of protests to the DHS acting secretary, the agency stated without evidence that those surveilled had “some level of participation in the violent incursion events.” Only several months later did the DHS inspector general promise the senators to launch an investigation into “the creation of the secret dossiers” and “specific allegations of targeting and/or harassment” (Hussain and Cope 2019). Not only did the faltering CBP statements expose the agency as untrustworthy, but the instance of surveillance in question also failed to satisfy the three criteria of legitimacy, legality, and necessity. The American Civil Liberty Union (ACLU) qualified it as “outrageous,” violating the constitutional freedoms of speech, of the press, and of assembly, and serving as “the latest example of abuse of power by the CBP,” underscoring the “dire need for meaningful agency oversight and accountability” (Jones et al. 2019).

Although travel and immigration not only in the United States but worldwide, have greatly decreased as a result of the global COVID-19 pandemic (Connor 2020), it is worth remembering that shortly before the pandemic began, the administration of President Trump proposed collecting DNA samples from immigrants detained by law enforcement agencies, dubiously arguing that it could help “detect fraud and solve cold criminal cases”—even though multiple studies have shown immigrants commit less crimes than native-born citizens (Trotta 2019). It is reasonable to respond to the emotion-alism underlying such a discourse with a lack of trust. The ACLU has warned that biometric surveillance can seriously impact privacy and civil liberties, with DNA collection employed in “criminal investigation” becoming used for “surveillance of the population” with “xenophobic goals”—i.e., establishing

immigrants as security “threats” (Trotta 2019). A militantly democratic oversight of surveillance can ensure that a liberal democracy does not devolve into an anocracy when ideologized policies and practices become commonplace, and that state accountability is not obfuscated behind the outsourcing of security and intelligence functions to corporate partners.

Some lessons for and from militant democracy

An examination of recent political dynamics in the United States, Poland, and Germany, provides evidence that contemporary liberal democracies are never exempt from experiencing authoritarian drift. Furthermore, while the exact circumstances and actors involved can vary widely, these diverse examples have in common the fact that surveillance policies and practices require strict oversight, lest they contribute to obscuring emotional appeals to ideology and make violations of civil liberties even more opaque. Surveillance, whether state or corporate or a synergy of both, trusted blindly and left unaccountable, can become a peril to liberal democracy. However, when guarded against by a militant commitment to values, institutional mechanisms, and political actions that are liberal and democratic in nature and realization, the potential of this threat can be kept from being actualized.

Conclusions and recommendations

This chapter began by addressing the dynamics of trust and transparency in relation to oversight of surveillance. It explained that granting trust to others, whether people or organizations, depends on their trustworthiness. Because the Snowden revelations proved a number of states and corporations to be untrustworthy in their surveillance policies and practices, the resulting lack of trust within civil society on the part of citizens and consumers requires constructively confronting the fact that these technologies can be deployed in manners that are obfuscated by untransparency, deceptions, and authoritarian emotionalism, oftentimes concealed within discourses of securitization and transparency that prevent intelligent accountability. Oversight of surveillance should not only demand clearer information in order to be transparent but also more instances to contest and resemantize—i.e., reinterpret and establish a new meaning for—surveillance policies and practices so as to ensure these are democratic, respecting and upholding human rights and civil liberties.

Accordingly, this chapter continued by arguing that democratic principles and institutions should be built on a constructive lack of trust, which only grants trust to the trustworthy. It was explained that the contemporary threat of authoritarian drift can exploit surveillance technologies to structure power and knowledge asymmetries that can threaten liberal democracy. Consequently, a militantly democratic approach within civil society is

recommended to oversee surveillance deployed by states, corporations, or the state–corporate nexus. Actors within civil society, governments, and corporate institutions can employ the three criteria of legitimacy, legality, and necessity to ensure that surveillance policies and practices establish security in a democratic manner, not only within their national contexts but within the global context as well.

This chapter addressed and critically analyzed contemporary experiences and lessons learned in Germany, Poland, and the United States concerning the oversight of surveillance, illustrating the manner in which a militantly democratic approach is practiced to check untransparency, emotionalism, and encroachment on civil liberties and human rights. Liberal democracy is not a state that is achieved and then maintained evermore, but a state that is accomplished by means of recurrent decisions to strive toward principles, establish institutions, and commit to courses of action that are liberal and democratic.

This chapter offered these explanations and recommendations in order to argue that a militantly democratic approach to surveillance oversight enables political agency within civil society to democratically reimagine and resemantize the direction and consequences that technologies have in structuring our societies, economies, and politics. Oversight of surveillance can be understood as a modality of resistance, contestation, and resemantization of policies and practices of surveillance so as to further enable a nascent digital agency, which can contribute to constructively structuring a “meaningful data politics” in which “human dignity and especially agency” decide the courses of action required to establish “alternative futures that embody holistic, reflexive and democratic imaginaries and practices” (Lyon 2019, 73). A constructive lack of trust and a militantly democratic approach to contemporary surveillance technologies and socioeconomic-political dynamics can loudly voice two crucial questions for reimagining and resemantizing our societies: “Do we really need this?” and “How does it contribute to the common good and human flourishing?” (Lyon 2019, 75).

References

- Agamben, Giorgio. 2005. *State of Exception*. Chicago: University of Chicago Press.
- Aguilera, Jasmine. 2019. “Trump Administration Has Separated 1,556 More Migrant Children than Previously Known.” October 26, 2019, <https://time.com/5710953/trump-administration-confirms-more-migrant-family-separation/>.
- Altman, Andrew. 2017. “Civil Rights.” *Stanford Encyclopedia of Philosophy*, <https://plato.stanford.edu/entries/civil-rights/>.
- Amnesty International. 2018. *Annual Report 2017/18*, www.amnesty.org/en/latest/research/2018/02/annual-report-201718/.
- Aronoff, Kate. 2018. “Poland’s New Surveillance Law Targets Personal Data of Environmental Advocates, Threatening UN Climate Talks.” July 2, 2018, <https://theintercept.com/2018/07/02/cop24-poland-surveillance-law/>.

- Associated Press. 2018a. "German Domestic Spy Chief Won't Get New Government Job." November 5, 2018, www.apnews.com/9b6e4f17f172402d8e69c2177312cf65.
- Associated Press. 2018b. "Germany's Intel Chief to Step Up Efforts Against Far Right." December 21, 2018, www.apnews.com/64ac6f21d6be4e2e9e7d6611c5ce2084.
- Ball, Kirstie, Sara Degli Esposti, Sally Dibb, Vincenzo Pavone, and Elvira Santiago-Gomez. 2019. "Institutional Trustworthiness and National Security Governance: Evidence from Six European Countries." *Governance* 32(1): 1–19, <https://doi.org/10.1111/gove.12353>.
- Bennhold, Katrin. 2020. "Body Bags and Enemy Lists: How Far-Right Police Officers and Ex-Soldiers Planned for 'Day X.'" August 1, 2020, www.nytimes.com/2020/08/01/world/europe/germany-nazi-infiltration.html.
- Biddle, Sam, and Ryan Devereaux. 2019. "Peter Thiel's Palantir Was Used to Bust Relatives of Migrant Children, New Documents Show." May 2, 2019, <https://theintercept.com/2019/05/02/peter-thiels-palantir-was-used-to-bust-hundreds-of-relatives-of-migrant-children-new-documents-show/>.
- Bigo, Didier, Gertjan Boulet, Caspar Bowden, Sergio Carrera, Elspeth Guild, Nicholas Hernanz, Paul de Hert, Julien Jeandesboz, and Amandine Scherrer. 2013. "Open Season for Data Fishing on the Web: The Challenges of the US PRISM Programme for the EU." *Centre for European Policy Studies* (no. 293: June 18), www.dw.com/en/german-intel-chief-warns-of-potential-threat-posed-by-wives-children-of-german-jihadis/a-41630197.
- Bing, Christopher, and Raphael Satter. 2019. "Exclusive: Government Officials Around the Globe Targeted for Hacking Through WhatsApp—Sources." October 31, 2019, www.reuters.com/article/us-facebook-cyber-whatsapp-nsogroup-excl/exclusive-government-officials-around-the-globe-targeted-for-hacking-through-whatsapp-sources-idUSKBN1XA27H.
- Colomer, Josep M., David Banerjea, and Fernando Barros de Mello. 2016. "To Democracy Through Anocracy." *Democracy & Society* 13(1): 19–25.
- Connolly, Kate. 2019. "Extreme-Right Wing of Germany's AfD Placed Under Surveillance." January 15, 2019, www.theguardian.com/world/2019/jan/15/extreme-right-wing-germany-afd-under-surveillance.
- Connor, Phillip. 2020. "More Than Nine-in-Ten People Worldwide Live in Countries with Travel Restrictions Amid COVID-19." April 1, 2020, www.pewresearch.org/fact-tank/2020/04/01/more-than-nine-in-ten-people-worldwide-live-in-countries-with-travel-restrictions-amid-covid-19/.
- Corbett, Erin. 2018. "Tech Companies Are Profiting Off Ice Deportations, Report Shows." October 23, 2018, <https://fortune.com/2018/10/23/tech-companies-surveillance-ice-immigrants/>.
- Der Spiegel. 2019. "Deadly Attack Exposes Lapses in German Security Apparatus." October 11, 2019, www.spiegel.de/international/germany/far-right-terrorism-in-germany-shooting-exposes-lapses-in-security-apparatus-a-1291075.html.
- Deutsche Welle. 2017. "German Intel Chief Warns of Potential Threat Posed by Wives, Children of German Jihadis." December 3, 2017, www.dw.com/en/german-intel-chief-warns-of-potential-threat-posed-by-wives-children-of-german-jihadis/a-41630197.
- Deutsche Welle. 2018. "Islamist Children Pose Real 'Threat' to Germany, Spy Chief Warns." August 6, 2018, www.dw.com/en/islamist-children-pose-real-threat-to-germany-spy-chief-warns/a-44963227.

- Escritt, Thomas. 2018. "Outgoing German Spy Chief Sacked for Branding SPD as 'Radical Left.'" November 5, 2018, www.reuters.com/article/us-germany-politics/outgoing-german-spy-chief-sacked-for-branding-spd-as-radical-left-idUSKCN1NA105.
- Federal Republic of Germany. 1949. *Basic Law for the Federal Republic of Germany*, www.bundesregierung.de/breg-en/chancellor/basic-law-470510.
- Fox Cahn, Albert. 2019. "Surveillance by Sanctuary Cities Is Helping ICE Track Undocumented Immigrants." July 9, 2019, www.nbcnews.com/think/opinion/surveillance-sanctuary-cities-helping-ice-track-undocumented-immigrants-ncna1027981.
- Freedom House. 2018. *Freedom in the World 2018: Democracy in Crisis*, <https://freedomhouse.org/report/freedom-world/freedom-world-2018>.
- Gera, Vanessa. 2019. "Poland Pressured to Say if It Bought Israeli Phone Spyware." September 4, 2019, www.apnews.com/461df123f8d84db9965ee2a762e17414.
- Human Rights Watch. 2018. *World Report 2018*, www.hrw.org/world-report/2018.
- Hussain, Saira, and Sophie Cope. 2019. "DEEP DIVE: CBP's Social Media Surveillance Poses Risks to Free Speech and Privacy Rights." August 5, 2019, www.eff.org/deeplinks/2019/08/deep-dive-cbps-social-media-surveillance-poses-risks-free-speech-and-privacy.
- Invernizzi Accetti, Carlo, and Ian Zuckerman. 2017. "What's Wrong with Militant Democracy?" *Political Studies* 65(1): 182–99.
- Jankovic, Sava. 2016. "Polish Democracy Under Threat? An Issue of Mere Politics or a Real Danger?" *Baltic Journal of Law & Politics* 9(1): 49–68.
- Jones, Tom, Mari Payton, and Bill Feather. 2019. "Source: Leaked Documents Show the U.S. Government Tracking Journalists and Immigration Advocates through a Secret Database." March 6, 2019, www.nbcsandiego.com/news/local/Source-Leaked-Documents-Show-the-US-Government-Tracking-Journalists-and-Advocates-Through-a-Secret-Database-506783231.html.
- Jordan, Frank. 2018. "Top German Spy Ousted after Clash with Merkel over Migrants." September 18, 2018, www.apnews.com/02e154035b4b4422810aa48e36e8c873.
- Jordan, Klara. 2015. "Opinion: Why Microsoft's Data Access Case Matters to Everyone on the Internet." September 30, 2015, www.csmonitor.com/World/Passcode/Passcode-Voices/2015/0930/Opinion-Why-Microsoft-s-data-access-case-matters-to-everyone-on-the-Internet.
- Koch, Moritz, and Dietmar Neuerer. 2018. "German Domestic Spy Chief Maassen under Pressure to Resign." October 9, 2018, www.handelsblatt.com/today/politics/monitoring-the-monitors-german-domestic-spy-chief-maassen-under-pressure-to-resign/23583276.html.
- Kość, Wojciech. 2019. "Poland's PiS Faces Questions over Israeli Spyware." September 7, 2019, www.politico.eu/article/poland-pis-israeli-spyware-questions/.
- Loewenstein, Karl. 1937a. "Militant Democracy and Fundamental Rights, I." *The American Political Science Review* 31(3): 417–32.
- Loewenstein, Karl. 1937b. "Militant Democracy and Fundamental Rights, II." *The American Political Science Review* 31(4): 638–58.
- Łoś, Maria. 2018. "Postscript." *Surveillance & Society* 16(3): 362–69.
- Lyon, David. 2018. *The Culture of Surveillance*. Cambridge: Polity Press.

- Lyon, David. 2019. "Surveillance Capitalism, Surveillance Culture and Data Politics." In *Data Politics: Worlds, Subjects, Rights*, edited by Didier Bigo, Engin Isin, and Evelyn Ruppert, 64–77. London: Routledge.
- Marczak, Bill, John Scott-Railton, Sarah McKune, Bahr A. Razzak, and Ron Deibert. 2018. "Hide and Seek: Tracking NSO Group's Pegasus Spyware to Operation in 45 Countries." Citizen Lab, September 18, 2018, <https://citizenlab.ca/2018/09/hide-and-peek-tracking-nso-groups-pegasus-spyware-to-operations-in-45-countries/>.
- Miroff, Nick, and Josh Dawsey. 2019. "All the Best People': The Ghostwriter: The Advisor Who Scripts Trump's Immigration Policy." August 17, 2019, www.washingtonpost.com/graphics/2019/politics/stephen-miller-trump-immigration/.
- O'Connell, Rory. 2009. "Militant Democracy and Human Rights," *Constitutional Law Review* 1: 84–90, www.constcourt.ge/uploads/other/3/3824.pdf.
- Oltermann, Philip. 2019. "German Far-Right Group 'Used Police Data to Compile Death List.'" June 28, 2019, www.theguardian.com/world/2019/jun/28/german-far-right-group-used-police-data-to-compile-death-list.
- O'Neill, Onora. 2002. "Reith Lectures: A Question of Trust." BBC, www.immagic.com/eLibrary/ARCHIVES/GENERAL/BBC_UK/B020000O.pdf.
- O'Neill, Onora. 2013. "What We Don't Understand about Trust." *TEDxHousesofParliament*, https://youtu.be/1PNX6M_dVsk.
- O'Neill, Onora. 2017. "Trust vs Trustworthiness." *Huxley Summit of the British Science Association*, <https://youtu.be/XWwTYy9k5nc>.
- Panoptykon Foundation. 2015. "Legalne, ale tajne? Analiza kontrowersji wokół RCS." July 14, 2015, <https://panoptykon.org/wiadomosc/legalne-ale-tajne-analiza-kontrowersji-wokol-rs>.
- Panoptykon Foundation. 2019. "Pegasus, czyli inwigilacyjne zabawki CBA poza kontrolą." September 5, 2019, <https://panoptykon.org/wiadomosc/pegasus-czyli-inwigilacyjne-zabawki-cba-pozza-kontrola>.
- Reuters. 2018. "German Domestic Security Agency Failed to Act on AfD Concerns: Media." September 15, 2018, www.reuters.com/article/us-germany-security/german-domestic-security-agency-failed-to-act-on-afd-concerns-media-idUSKCN1LV0C5.
- Reuters. 2019. "EU's Katainen Says Article 7 Procedure Against Poland Has Had Little Impact." May 1, 2019, www.reuters.com/article/us-poland-katainen-eu-idUSKCN1S73C6.
- Schneier, Bruce. 2015. *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World* (epub version). New York: W. W. Norton & Company.
- Shalal, Andrea, and Sabine Siebold. 2018. "'Brainwashed' Children of Islamist Fighters Worry Germany: Spy Chief." January 31, 2018, www.reuters.com/article/us-germany-security-children/brainwashed-children-of-islamist-fighters-worry-germany-spy-chief-idUSKBN1FK1FJ.
- Szary, Wiktor. 2016. "Poland Approves Closer Surveillance of Foreigners Ahead of NATO Summit, Pope Visit." June 10, 2016, www.reuters.com/article/us-poland-security-lawmaking-idUSKCN0YW1OT.
- Trotta, Daniel. 2019. "U.S. Proposes Collecting DNA Samples from Detained Immigrants." October 21, 2019, www.reuters.com/article/us-usa-immigration-dna/us-proposes-collecting-dna-samples-from-detained-immigrants-idUSKBN1X0250.

- Verde Garrido, Miguelángel. 2015. "Contesting a Biopolitics of Information and Communications: The Importance of Truth and Surveillance after Snowden." *Surveillance & Society* 13(2): 153–67.
- Wetzling, Thorsten, and Kilian Vieth. 2018. "Upping the Ante on Bulk Surveillance: An International Compendium of Good Legal Safeguards and Oversight Innovations." *Publication Series on Democracy* 50. Berlin: Heinrich Böll Stiftung, www.stiftung-nv.de/sites/default/files/upping_the_ante_on_bulk_surveillance_v2.pdf.
- Wiedmann-Schmidt, Wolf. 2019. "Bundesregierung will Verfassungsschutz Massiv Aufstocken." September 24, 2019, www.spiegel.de/politik/deutschland/horst-seehofer-will-verfassungsschutz-massiv-aufstocken-regierungsplaene-a-1288364.html.
- Zeid, Ra'ad H. 2018. "'Human Rights No Longer Treated as a Priority, but as a Pariah,' Zeid Tells 25th Anniversary Gathering in Vienna." May 22, 2018, www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=2311.
- Zuboff, Shoshana. 2015. "Big Other: Surveillance Capitalism and the Prospects of an Information Civilization." *Journal of Information Technology* 30(1): 75–89.