Against Moral Absolutism: Surveillance and Disclosure After Snowden

Rahul Sagar

Now that the uproar provoked by the disclosure of the National Security Agency's (NSA) surveillance programs has lessened, and the main protagonists, Edward Snowden and Glenn Greenwald, have had a chance to make the case for their actions, we are in a position to evaluate whether their disclosure and publication of communications intelligence was justified. To this end, this essay starts by clarifying the history, rationale, and efficacy of communications surveillance. Following this I weigh the arguments against surveillance, focusing in particular on the countervailing value of privacy. Next I explain why state secrecy makes it difficult for citizens and lawmakers to assess the balance that officials are striking between security and privacy. Finally, I turn to consider whether the confounding nature of state secrecy justifies Snowden's and Greenwald's actions. I conclude that their actions are unjustified because they treat privacy and transparency as trumps. Consequently, their actions embody a moral absolutism that disrespects the norms and procedures central to a constitutional democracy.

Surveillance Old and New

Before analyzing the benefits and costs of communications surveillance, I want to address some common misperceptions relating to its history, rationale, and efficacy. The first misperception is that communications surveillance is a new phenomenon. In reality it has a long history. Prior to the nineteenth century, communication pivoted around the horse and rider (and the roads on which they traversed) and around boats (and the ports at which their voyages began and ended). From the tenth century BCE through to the fifteenth century CE these modes of communication were subject to rudimentary forms of surveillance:

Ethics & International Affairs, 29, no. 2 (2015), pp. 145–159.
© 2015 Carnegie Council for Ethics in International Affairs
doi:10.1017/S0892679415000040

https://doi.org/10.1017/S0892679415000040 Published online by Cambridge University Press

messengers were intercepted and bags were opened; ports were embargoed and ships were searched. This pattern changed as European states, increasingly administered by professionals and reliably funded by taxes, took shape. This is when we first hear of "spymasters" like John Thurloe, secretary to the English Commonwealth's Council of State, who established in 1653 a Secret Office that opened, copied, and resealed suspicious letters over the course of a night. The innovation was adopted by the Stuarts and then expanded by the Hanoverians, making it one of the first organizations dedicated to communications surveillance.

America's revolutionaries were aware of such European practices, which Congress's Committee of Secret Correspondence copied. Nonetheless, removed from European rivalries, post-Revolutionary America had little incentive to establish a surveillance apparatus. In the absence of enduring threats, the organizations created to "tap" telegraphs during the Civil War and the Spanish-American War proved short lived. It was only in the early twentieth century—when technology shrank distance and foreign entanglements grew—that the need for consistent surveillance began to be felt. Fears of German subversion provided an early impetus. The frenetic negotiations following World War I provided an opening for the "Black Chamber," the first American peacetime organization focused on intercepting diplomatic communications. A decade later came the NSA's forerunner, the Signals Intelligence Service, whose code-breaking efforts played a vital role in World War II. With Pearl Harbor still on their minds, America's post–World War II leadership resolved to build a permanent intelligence apparatus. The looming confrontation with the Soviet Union provided the immediate spur, but the decision responded to longer-term pressures emanating from a deepening involvement in international politics.

A second misperception about communications surveillance relates to its growth over the cold war, and since 9/11 in particular. A century ago the Black Chamber had a staff of fifty, whereas today the NSA employs upward of 38,000. The former relied on amateur mathematicians, whereas the latter possesses supercomputers. Greenwald attributes this dizzying expansion to the desire of "elites" to control "populations" stirred up by "worsening economic inequality."[1] A more prosaic view would trace the expansion of surveillance to three factors: first, the explosion in global communication due to technological advances that have lowered the cost and increased the speed of data transmission; second, the persistence of geostrategic rivalries and the spread of violent ideologies—initially communism and more recently religious fundamentalism—within and across

https://doi.org/10.1017/S0892679415000040 Published online by Cambridge University Press

civilian populations; and third, the steady advance in data storage and processing technology that has made it possible to capture and process communications between rival states and violent groups and their local proxies. The first two factors give rise to the need for extensive communications surveillance, whereas the third provides the capability to meet this need. These three factors are not exhaustive. It is not unreasonable to think that rent-seeking by bureaucracies and private contractors is likely to have played some role in the NSA's expansion (though it is difficult for external observers to discern how far this is the case). Still, the deeper point is that there are plausible security- and technology-related explanations for the increased size and sophistication of communications surveillance.

A third misperception concerns the efficacy of contemporary communications surveillance. Though surveillance has become more organized and technologically sophisticated, it does not follow that we now confront an omniscient Big Brother. Greenwald asserts that contemporary surveillance programs are especially troubling because "all prior spying systems were by necessity more limited and capable of being evaded."[2] But recent events suggest that this claim is exaggerated. As Greenwald himself observes, over the past decade "major international attacks from London to Mumbai to Madrid proceeded without detection, despite involving at least dozens of operatives."[3] A focus on electronic surveillance also misses the evasiveness of other modes of communication. Osama Bin Laden, for instance, was able to evade American surveillance by relying on personal couriers.

Surveillance and Privacy

I have challenged the conspiratorial view that state surveillance serves to reinforce the hegemony of a shadowy elite. A basic premise of the discussion that follows is that in contemporary liberal democracies, communications surveillance is a legitimate activity. What, then, ought to be the bounds of such surveillance and how far can we be confident that these bounds are being observed?

In order to ascertain the rightful bounds on communications surveillance we need to weigh the interests it furthers against those it threatens. The interest it furthers is national security. Greenwald questions this link on a number of grounds. He argues that surveillance is a disproportionate response to the threat of terrorism, which has been "plainly exaggerated" because the "risk of any American dying in a terrorist attack is . . . considerably less than the chance of being struck by lightning."[4] Furthermore, even if the threat of terrorism is real, surveillance is

https://doi.org/10.1017/S0892679415000040 Published online by Cambridge University Press

unjustified because to "venerate physical safety above all other values" means accepting "a life of paralysis and fear."[5] He also questions surveillance's relevance to national security on the grounds that it is often employed to further other national or commercial interests. He asks how, for instance, does "spying on negotiation sessions at an economic summit or targeting the democratically elected leaders of allied states" serve national security?[6]

Arguably these criticisms miss the mark. That terrorist plots thus far have been amateurish does not mean that terrorists will not learn and eventually succeed in causing greater harm. Nor is being concerned about terrorism tantamount to "pursuing absolute physical safety."[7] The terror in terrorism comes from the unpredictability and the brutality of the violence inflicted on civilians. There is a difference between voluntarily undertaking a somewhat risky bicycle ride in rush hour traffic and being unexpectedly blown to bits while commuting to work. Finally, it is widely accepted that countries have a right to pursue their national interests, subject of course to relevant countervailing ethical considerations. It is not hard to imagine how intercepting Chancellor Angela Merkel's conversation could serve the United States' national security interests (for example, it could provide intelligence on Europe's dealings with Russia).

What are the countervailing values that have been overlooked in this case? The President's Review Group on Intelligence and Communications Technologies, set up in the wake of Snowden's disclosures, warns that surveillance of foreign leaders must be "respectful." But the justification offered is strategic rather than moral: the group urges caution out of recognition for "the importance of cooperative relationships with other nations."[8] A moral justification would have weak legs since American allies, including Germany, reportedly engage in similar practices.[9] As Greenwald himself acknowledges, the NSA's surveillance of foreign leaders is "unremarkable" because "countries have spied on heads of state for centuries, including allies."[10]

Greenwald also raises objections from a national security perspective. He warns that mass surveillance undermines national security because "it swamps the intelligence agencies with so much data that they cannot possibly sort through it effectively."[11] He also questions the efficacy of communications surveillance, arguing that it has little to show in terms of success in combating terrorism. But these criticisms are equally unpersuasive. It is certainly possible that a surveillance program could generate so much raw data that an important piece of information is overlooked. But in such a case the appropriate response would not be to shut down the program

https://doi.org/10.1017/S0892679415000040 Published online by Cambridge University Press

but rather to bulk up the processing power and manpower devoted to it. Finally, both the President's Review Group and the Privacy and Civil Liberties Oversight Board have examined the efficacy of the NSA's programs. Both report that the NSA's foreign surveillance programs have contributed to more than fifty counterterrorism investigations, leading them to conclude that the NSA "does in fact play an important role in the nation's effort to prevent terrorist attacks across the globe."[12]

So far I have argued that communications surveillance can further national security. However, national security is not the only value liberal democracies and their citizens deem important. Hence we need to consider how far communications surveillance impinges on other important interests and values.

Greenwald identifies two major harms. The first is political in nature. Mass surveillance is said to stifle dissent because "a citizenry that is aware of always being watched quickly becomes a compliant and fearful one." Compliance occurs because, anticipating being shamed or condemned for nonconformist behavior, individuals who know they are being watched "think only in line with what is expected and demanded."[13] Even targeted forms of surveillance are not to be trusted, Greenwald argues, because the "indifference or support of those who think themselves exempt invariably allows for the misuse of power to spread far beyond its original application."[14]

These claims strike me as overblown. The more extreme claim, that surveillance furthers thought control, is neither logical nor supported by the facts. It is logically flawed because accusing someone of trying to control your mind proves that they have not succeeded in doing so. On a more practical level, the fate met by states that have tried to perfect mass control—the Soviet Union and the German Democratic Republic, for example—suggests that surveillance cannot eliminate dissent. It is also not clear that surveillance can undermine dissident movements as easily as Greenwald posits. The United States' record, he writes, "is suffused with examples of groups and individuals being placed under government surveillance by virtue of their dissenting views and activism—Martin Luther King, Jr., the civil rights movement, antiwar activists, environmentalists."[15] These cases are certainly troubling, but it hardly needs pointing out that surveillance did not prevent the end of segregation, retreat from Vietnam, and the rise of environmental consciousness. This record suggests that dissident movements that have public opinion on their side are not easily intimidated by state surveillance (a point reinforced by the Arab Spring).

Surveillance may make it harder for individuals to associate with movements on the far ends of the political spectrum. But why must a liberal democracy refrain

https://doi.org/10.1017/S0892679415000040 Published online by Cambridge University Press

from monitoring extremist groups such as neo-Nazis and anarchists? There is the danger that officials could label as "extreme" legitimate movements seeking to challenge the prevailing order. Yet the possibility that surveillance programs could expand beyond their original ambit does not constitute a good reason to end surveillance altogether. A more proportionate response is to see that surveillance powers are subject to oversight.

The second harm Greenwald sees surveillance posing is personal in nature. Surveillance is said to undermine the very essence of human freedom because the "range of choices people consider when they believe that others are watching is . . . far more limited than what they might do when acting in a private realm."[16] Internet-based surveillance is viewed as especially damaging in this respect because this is "where virtually everything is done" in our day, making it the place "where we develop and express our very personality and sense of self." Hence, "to permit surveillance to take root on the Internet would mean subjecting virtually all forms of human interaction, planning, and even thought itself to comprehensive state examination."[17]

This claim too seems overstated in two respects. First, it exaggerates the extent to which our self-development hinges upon electronic communication channels and other related activities that leave electronic traces. The arrival of the Internet certainly opens new vistas, but it does not entirely close earlier ones. A person who fears what her browsing habits might communicate to the authorities can obtain texts offline. Similarly, an individual who fears transmitting materials electronically can do so in person, as Snowden did when communicating with Greenwald. There are costs to communicating in such "old-fashioned" ways, but these costs are neither new nor prohibitive. Second, a substantial part of our self-development takes place in public. We become who we are through personal, social, and intellectual engagements, but these engagements do not always have to be premised on anonymity. Not everyone wants to hide all the time, which is why public engagement—through social media or blogs, for instance—is such a central aspect of the contemporary Internet.

Classified Oversight

Thus far I have challenged the claim that communications surveillance obliterates dissent and privacy. It is not my intention, however, to claim that surveillance has no negative implications at all. On the contrary, entrusting officials with this dangerous

https://doi.org/10.1017/S0892679415000040 Published online by Cambridge University Press

power raises two concerns. First, surveillance can be used mischievously—that is, to target political opponents and dissidents. Such action is unethical because it involves a misuse of public authority and resources. Second, because surveillance violates the important right of privacy, it must not be gratuitous—that is, it must be minimized when possible and only be undertaken when it truly serves an important public purpose. As a consequence, surveillance programs must be evaluated carefully for deleterious impacts. Yet ensuring that values such as the rule of law and privacy are respected or weighed correctly is not easy. Consider, for instance, a report by CNN on former U.S. Attorney General Alberto Gonzales's defense of a controversial NSA surveillance program:

> Gonzales said the warrantless surveillance has "been extremely helpful in protecting America" from terrorist attacks. However, because the program is highly classified, he said he could not make public examples of how terrorist attacks were actually disrupted by the eavesdropping.[18]

This example underscores that evaluating the costs and benefits of a particular surveillance program usually requires access to contextual details. In the national security domain, however, such details are typically classified, making it difficult for citizens to ascertain whether our interests are being balanced in a lawful or reasonable manner. The obstacle that state secrecy poses in this sense is widely recognized, of course. What is less well understood is how difficult it is to surmount this obstacle.

Communications surveillance programs are typically cloaked in secrecy, as their efficacy depends on those who are being observed not being fully aware of the scope and reach of such programs. Greenwald considers such secrecy undemocratic:

> The danger posed by the state operating a massive secret surveillance system is more ominous now than at any point in history. . . . Democracy requires accountability and consent of the governed, which is only possible if citizens know what is being done in their name. The presumption is that, with rare exception, they will know everything their political officials are doing.[19]

This statement expresses a caricatured view of democracy. Conceptually, democracy does not hinge on near complete transparency. A self-governing polity is entitled to authorize secrecy when this serves a public purpose. Indeed, republics have long employed secrecy. The Framers of the American Constitution drew upon this record when they created the Presidency and the Senate—institutions

https://doi.org/10.1017/S0892679415000040 Published online by Cambridge University Press

designed with a view to ensuring that foreign and military relations could be conducted in secret when necessary. In their assessment, to quote George Washington, secrecy was a central "characteristic of good government" as it was "indispensably necessary" for the "accomplishment of many of the most important national objects."[20] To be sure, as the scope and scale of secrecy has increased in the wake of America's immersion in international politics, fears about the misuse of this power have grown too. It is worth underscoring, however, that from World War I to the present day public debate has been more concerned with securing accountability rather than pursuing transparency. That is, the question that has occupied commentators is not how to eliminate secrecy altogether but rather how to ensure that it will not be abused. In part this is because secrecy in government could become truly rare only if the United States retreated from its central role in the current international order. The focus on accountability is also more appropriate in the context of a modern representative democracy grappling with complex security challenges.

The foregoing explains why commentators typically respond to state secrecy by calling for oversight—that is, they propose that lawmakers or judges review classified information on behalf of citizens with a view to assuring the public that secrecy is not being used to conceal unlawful activity. Unfortunately, such proposals are confronted with some understudied obstacles. These obstacles explain why, nearly a half century on from the passage of the Freedom of Information Act and the creation of oversight committees in Congress, many commentators continue to fret about the abuse of secrecy.

Two of the obstacles that overseers confront are structural. First, the Executive holds closely much of the detailed, contextual information overseers require. The Executive is often reluctant to share such information, especially with Congress, on the grounds that the latter's structure and composition, particularly the fact that it is made up of adversarial parties, make it prone to undisciplined disclosures. Second, the expertise required to make sense of such information typically resides within the Executive Branch. Courts in particular are not equipped, and judges are not trained, to make politically charged decisions about the harm that might be caused by the disclosure of such information. This is not a trumped-up charge of judicial incompetence; these are the reasons that judges themselves offer in defense of their record of deference to the Executive Branch on such matters.[21]

It is sometimes argued that concerns about partisanship and competence can be addressed by appointing an independent panel to regulate classification decisions.

https://doi.org/10.1017/S0892679415000040 Published online by Cambridge University Press

But consider this: Since the decisions of this panel will not be any more amenable to external scrutiny than are the president's decisions, what prevents its members from behaving in a partisan fashion? We may hope that its members will be nonpartisan, but when this panel is designed to routinely make politically sensitive decisions about state secrets, could the politicization of appointments be far behind? In short, the conceptual problem bedeviling a secrecy regulator is that citizens will lack a good and sufficient reason to trust it, as they will not have access to the information necessary for rational trust.

The above goes some way toward explaining why Congress and the courts have proven easy targets for surveillance critics. Greenwald claims that the relevant oversight committees in Congress have been "thoroughly captured" by the NSA and that the Foreign Intelligence Surveillance Court (FISC), which is meant to approve surveillance warrants, is "a mere rubber stamp."[22] In reality, external observers have no meaningful basis on which to make such claims. Greenwald makes much of the fact that the FISC rarely declines warrant applications. However, this statistic is not as informative as Greenwald thinks it is. The high acceptance rate could be the result of the FISC's general concurrence with the NSA's strategy in the face of threats that we are not privy to. Concurrence need not imply cooption, especially when the FISC has a sizable membership that is rotated at regular intervals. The President's Review Group, it should be noted, has praised the FISC's "strong record in dealing with non-compliance issues."[23]

The above also explains why we should be skeptical of proposals aimed at enhancing oversight. Consider, for example, the President's Review Group's recommendation that FISC proceedings be made more adversarial, with a public defender drafted in to represent the intended surveillance targets.[24] This proposal raises a major institutional problem: Who will decide which lawyers receive security clearances? Then there is the deeper conceptual point touched on earlier. Adversarial proceedings or not, the FISC's proceedings will invariably be shrouded in secrecy. So how, then, can the public be confident that the relevant judge or bench has fairly weighed both sides?

So far I have focused on the limited credibility of domestic oversight. If we accept the view that all persons, regardless of citizenship, have privacy rights, then there is a further set of difficulties to overcome. To begin with, we lack an established set of norms that overseers can utilize to regulate international surveillance. Such norms will not be easy to generate given competing conceptions of privacy (China, for instance, is unlikely to consent to a norm that forbids it from operating

https://doi.org/10.1017/S0892679415000040 Published online by Cambridge University Press

its so-called Great Firewall). We also confront grave enforcement difficulties. It is hard to see who could fairly adjudicate between the interests of a particular state (for example, the United States) and a foreign national (for example, an Iraqi). It is hard to foresee support for an international regulatory body. Not only the United States but also countries such as China and Russia are likely to balk at sharing intelligence with an international regulator whose internal controls may be less robust than theirs and whose members may be drawn from rival states. Yet if compliance with international norms were allowed to be voluntary, then little would prevent foreign powers from monitoring peoples and organizations as they see fit. In this event, curtailing the NSA's surveillance operations would not remedy the loss of privacy experienced by persons around the world, since their communications would still be monitored by other nations.

It is tempting to respond to the difficulties outlined above by requiring the United States to proceed unilaterally. This is the position taken by the President's Review Group, which has recommended that for strategic and moral reasons the United States ought to immediately strengthen the privacy protections afforded to foreign persons. It is perhaps worth pointing out that the Group's proposal would not satisfy Snowden and Greenwald, because it still permits surveillance of foreign persons, without a warrant, when there is "reasonable belief" that such persons pose a threat to national security.[25] Then there is the deeper point that unilateral action by the United States will not solve the conceptual problem identified earlier: How are foreigners to tell whether U.S. officials are in fact weighing their interests correctly prior to targeting them for surveillance? This is not to say that the call for increased oversight is meaningless. To the contrary, the Group's praise for the FISC's role suggests that enhanced judicial involvement could better safeguard the privacy of foreign nationals. But even if a proposal such as this one were adopted, foreigners would still not know how credible the promised protection of their privacy is, since they would continue to lack internal knowledge about the proceedings of—let alone representation in—the relevant oversight body. The credibility problem, in other words, remains.

The Ethics of Disclosure

We have seen there are national security reasons to endorse surveillance as well as privacy-related reasons to be troubled by it. Unfortunately, the secrecy that pervades surveillance programs makes it difficult to know whether officials are

https://doi.org/10.1017/S0892679415000040 Published online by Cambridge University Press

striking a reasonable balance between our interests in security and privacy. This veil of secrecy is not easily lifted: the quest for transparency is ill advised, and oversight is confronted with structural and conceptual obstacles. Does the confounding nature of state secrecy justify exposing secret surveillance programs, as Snowden and Greenwald claim? To answer this question we need first to examine when whistle-blowing is appropriate.

Government employees who handle classified information are required to pledge that they will never disclose it. They are also subject to laws prohibiting unauthorized disclosure of the same. It is sometimes argued that these pledges and laws make it unethical for an employee to blow the whistle. But this position is untenable. Given the structural obstacles that overseers confront—their dependence on the Executive for classified information and security expertise—it is possible that unlawful surveillance activities may go unnoticed. In such a case an employee may well be morally justified in disobeying the law in order to bring incriminating information to the attention of citizens and lawmakers.[26]

At the same time, an employee cannot disobey the law simply because covert surveillance activities offend his personal conscience. Such action is often justified as an instance of civil disobedience. But such a claim is untenable for two reasons. First, unlike an unhappy conscript contemplating his conscience, the employee in question has volunteered to be entrusted with classified information. If the president's policies run counter to the dictates of his conscience, he ought to resign. Second, the potentially adverse consequences of his disobedience will be borne not by him alone, but by other citizens as well, whose safety he potentially endangers. Because he imposes a burden on his fellow citizens, an employee who makes an unauthorized disclosure must evaluate wrongdoing in terms of the violation of shared interests.

The preceding arguments suggest that an employee is justified in disclosing classified information when this exposes an abuse of public authority, understood as the violation of law. The employee must proceed on the basis of clear and convincing evidence of abuse, and the resulting disclosure should not impose a disproportionate burden on national security. In particular, the employee in question should utilize the least drastic means of disclosure—that is, he should minimize harm to national security by limiting the scope and scale of disclosures as far as possible, making public only what is required to allow overseers and citizens to perform their constitutionally mandated roles. The above conditions are based on a common principle: An employee who discloses classified information

https://doi.org/10.1017/S0892679415000040 Published online by Cambridge University Press

is acting—indeed breaking the law—on behalf of fellow citizens who have not authorized him to do so. His warrant is therefore tenuous and so his actions must be correspondingly modest.

It is sometimes mistakenly believed that the First Amendment permits journalists to publish whatever classified information they come across. In fact, 18 USC § 798(a) specifically penalizes the publication of communications intelligence because such disclosures invariably expose surveillance methods, thereby undermining intelligence gathering more generally. As a result, a reporter or publisher who decides to violate § 798—and to thereby burden national security—has a distinct set of moral obligations. Principal among these is an obligation to approach the Executive prior to publication so as to allow it to offer reasons against disclosing classified information and to take preventive national security measures in the event there are unconnected missions that rely on the methods that the news report will expose.

In my view, Snowden's and Greenwald's actions do not meet the standards outlined above. Three deficiencies stand out. The first is that Snowden and Greenwald proceeded in the absence of evidence of the abuse of authority. They were aware that all three branches of government had approved the domestic and foreign communications surveillance programs in question. They disregarded the decisions of these institutions on the grounds that the public ought to be informed. However, transparency is only one of the values central to democracy. Citizens and their representatives are entitled to authorize secrecy when this is necessary to secure important public ends. For example, they may authorize officials to eavesdrop on the conversations of German leaders with a view to uncovering double-dealing. By exposing the NSA's programs, and thereby alerting the Germans as well as other less friendly nations to the United States' capabilities, Snowden and Greenwald have now taken this option off the table (or at least made it more difficult to employ).

Here the objection may be raised that Snowden and Greenwald have merely informed citizens of what has been done in their name. But this argument puts the cart before the horse. We allow our representatives to employ secrecy precisely because we recognize that it is self-defeating to publicly debate the contours of a surveillance program. Furthermore, assume that the ensuing public debate leads citizens to support eavesdropping on German officials. How can this preference be respected if the cat has already been let out of the bag? Here we see how unauthorized disclosures can actually limit rather than facilitate public choice.

https://doi.org/10.1017/S0892679415000040 Published online by Cambridge University Press

A second deficiency relates to the disproportionality of the disclosures. Even though the NSA's domestic surveillance program was deemed lawful by the FISC, we could take the view that the lack of public debate about the capture of domestic metadata justified Snowden and Greenwald's disclosure of this particular program. But even so, it is hard to see how we could justify their disclosure of domestic surveillance methods, bearing in mind that these methods could help gather intelligence on what even Snowden and Greenwald might consider legitimate targets, namely, domestic terror plots.

It is harder still to understand what purpose was served by disclosing NSA foreign surveillance methods such as the deployment of "backdoors" in commonly used hardware and software. Apparently the purpose was to alert countries and individuals around the world to the threat that the NSA poses to their privacy. Snowden and Greenwald have since encouraged countries to develop new infrastructure so that their communications do not have to transit through the United States, and have urged individuals to employ encryption and to cease using the services of companies that collaborate with the NSA. But this approach misses the point: if channels of communication that are immune to surveillance exist, these would be used not only by dissidents but also by terrorists. This is why the NSA is obliged to use all available means to crack new channels of communications (or else they could rightly be accused of negligence in the wake of a terrorist attack that relies on such channels). The approach taken by the President's Review Group is more balanced. Troubled by the prospect that aggressive surveillance methods could lead to a loss of trust in Internet-based services, they recommend that the United States should typically disclose known vulnerabilities in widely used software and hardware, but allow nonetheless that "in rare instances" the government may "briefly authorize" using such a vulnerability for "priority intelligence collection."[27]

A third deficiency relates to the mode of disclosure. As noted earlier, in view of the unique sensitivities and specific legal provisions associated with the publication of communications intelligence, it is a norm for media organizations to warn the government of impending stories, allowing it to make the case against proceeding. Snowden and Greenwald sought to undermine this norm. Having disclosed some classified information to the *Washington Post*, Snowden became "livid" when the *Post* sought advice on the legality of proceeding with the story.[28] He then approached Greenwald, who pressed the *Guardian* to publish the disclosures without hearing out the government.

https://doi.org/10.1017/S0892679415000040 Published online by Cambridge University Press

Greenwald's justification for this stance is that the "idea of a fourth estate is that those who exercise the greatest power need to be challenged by adversarial push-back and an insistence on transparency."[29] Now, such adversarialism is understandable when it leads to the disclosure of obvious wrongdoing. An example here is reporting on prisoner abuse at Abu Ghraib, which was carried out in spite of the very real threat of repercussions against American military personnel stationed in Iraq. In the case at hand, however, seeing as the NSA's programs were not unlawful or being used abusively, Greenwald's praise for his own "adversarialism" could be viewed as an effort to ennoble impatience. According to him, journalists abdicate their watchdog role when they follow the norm of informing the government prior to publication—what he describes as "fear-driven, obsequious journalism."[30] But the norm exists for a reason. Reporters do not always know the big picture, such as which surveillance methods are being used, where, and to what ends. It is not sufficient justification to claim that there is no evidence showing that a particular disclosure has caused harm. The NSA has little incentive to publicly declare that disclosures A and B have led it to lose intelligence on plot X or Y (nor, for that matter, will terrorist groups and rival states want to confess to having been outwitted in the past).

The Need for Responsibility

This essay has chiseled away at the justifications Snowden and Greenwald have offered on behalf of their actions. I have disputed their claims that communications surveillance obliterates privacy and the possibility of dissent, and that the secretive nature of such surveillance violates democratic principles. Setting aside these more extreme claims allows us to focus on a genuinely important problem—namely, whether liberal democracies can ensure that communications surveillance will be employed to further national security, and will not be employed maliciously or gratuitously.

I have shown that the nature of state secrecy unfortunately makes it difficult for overseers to perform their tasks, and makes it extremely difficult for citizens to know if they have done so. As a consequence, government employees are justified in making unauthorized disclosures when this exposes wrongdoing, understood here as the violation of public authority. But this reasoning does *not* justify Snowden's and Greenwald's actions, as they have chosen to expose lawful surveillance programs. Even if one is persuaded that the NSA ought not to have

https://doi.org/10.1017/S0892679415000040 Published online by Cambridge University Press

conducted domestic surveillance without seeking some form of public consent—a requirement that stands in some tension with the essentially covert nature of surveillance—the manner in which Snowden and Greenwald have proceeded remains hard to justify. Their stance has been dogmatic, treating privacy and transparency as trumps. And they are unduly dismissive of the authority of democratically elected officials and constitutionally mandated procedures, especially the oversight functions created by the separation of powers. There are instances when moral absolutism may be justified. But the conviction that truth is on one side alone is more often the mark of the ideologue.

NOTES

[1] Glenn Greenwald, *No Place to Hide: Edward Snowden, the NSA, and the U.S. Surveillance State* (New York: Metropolitan Books, 2014), p. 177.
[2] Ibid., p. 6.
[3] Ibid., p. 203.
[4] Ibid., p. 205.
[5] Ibid., p. 208.
[6] Ibid., p. 202.
[7] Ibid., p. 207.
[8] President's Review Group on Intelligence and Communications Technologies, *Liberty and Security in a Changing World*, December 12, 2013, pp. 12–13.
[9] Michael S. Schmidt and Eric Schmitt, "Obama's Portable Zone of Secrecy (Some Assembly Required)," *New York Times*, November 9, 2013.
[10] Greenwald, *No Place to Hide*, p. 141.
[11] Ibid., p. 205.
[12] President's Review Group, *Liberty and Security in a Changing World*, pp. 144–45; Privacy and Civil Liberties Oversight Board, *Report on the Surveillance Program Operated Pursuant to* Section 702 *of the Foreign Intelligence Surveillance Act*, July 2, 2014, p. 2.
[13] Greenwald, *No Place to Hide*, pp. 3, 178.
[14] Ibid., p. 200.
[15] Ibid., p. 183.
[16] Ibid., p. 173.
[17] Ibid., p. 6.
[18] "Gonzales Defends NSA, Rejects Call for Prosecutor," *CNN*, January 17, 2005, www.cnn.com/2006/POLITICS/01/17/gonzales.nsa/.
[19] Greenwald, *No Place to Hide*, pp. 208–209.
[20] "George Washington to James Madison, March 31, 1787," in Worthington Chauncey Ford, ed., *The Writings of George Washington*, Vol. XI (New York: G. P. Putnam's Sons, 1891), pp. 132–33.
[21] For instance, see Center for National Security Studies v. DOJ, 331 F.3d 918, 927–28 (D.C. Cir. 2003); and El-Masri v. United States, 479 F.3d 296, 305 (4th Cir. 2007).
[22] Greenwald, *No Place to Hide*, pp. 251–52.
[23] President's Review Group, *Liberty and Security in a Changing World*, pp. 202–203.
[24] Ibid., pp. 203–205.
[25] Ibid., p. 157.
[26] For a fuller elaboration and defense of the circumstances under which disclosure may be justified, see Rahul Sagar, *Secrets and Leaks: The Dilemma of State Secrecy* (Princeton, N.J.: Princeton University Press, 2013), pp. 127–39.
[27] President's Review Group, *Liberty and Security in a Changing World*, p. 219.
[28] Greenwald, *No Place to Hide*, p. 18.
[29] Ibid., p. 230.
[30] Ibid., p. 56.

https://doi.org/10.1017/S0892679415000040 Published online by Cambridge University Press