

What Changed After Snowden? A U.S. Perspective

BEN WIZNER
American Civil Liberties Union, USA

Did the Snowden revelations change the ways in which surveillance is implemented, regulated, and accepted? In this short contribution, Snowden’s lawyer explains how institutions that may serve as counterweights to the security state were strengthened and have challenged surveillance practices. Courts, the U.S. Congress, media, and technology companies, he argues, have substantially altered their behavior since the beginning of the disclosures.

Keywords: Snowden, surveillance, NSA, ACLU

In June 2015—two years after Edward Snowden’s disclosures to *The Guardian* and other news organizations launched an extraordinary global debate about mass surveillance and democracy—former NSA and CIA director Michael Hayden addressed a gathering of corporate chief financial officers. In his remarks, he was casually dismissive of the surveillance reforms that had been achieved in the United States post-Snowden. He insisted that, had he been told two years earlier that the result of the debate would be the NSA’s loss of one “little” telephone metadata program, his response would have been, “Cool!”¹

Hayden, a master propagandist, hoped to convey that Snowden’s act of conscience had been in vain, that others would be foolish to follow his example, and that the movement for reform had been a flop. Yet while Hayden is a uniquely cynical public figure, he is not alone in insisting that for all of the political drama of the Snowden disclosures, very little has changed. Is this view correct?

I think not.

What we can observe since the beginning of the revelations is that Snowden’s act of placing surveillance on the public agenda has strengthened institutions that serve as counterweights to the authorities and capabilities of the security state. In most democracies, those institutions are the courts, the legislatures, and the independent media. In the United States, the Snowden revelations have

Ben Wizner: bwizner@aclu.org
Date submitted: 2016–12–10

¹ <https://theintercept.com/2015/06/17/hayden-mocks-extent-post-snowden-surveillance-reform-2-years-cool/>

demonstrably empowered each of these institutions, as well as an unlikely fourth source of intelligence oversight. The point can be illustrated with brief “before and after” snapshots.

The Courts

In March 2013—just three months before the first Snowden revelations—the U.S. Supreme Court dismissed a constitutional challenge to an NSA surveillance program.² The decision in *Amnesty International v. Clapper* ended the lawsuit without even considering the lawfulness of the program. Instead, the Court held that the plaintiffs had no right to bring the action because they could not establish that they themselves had been targeted by the challenged program, nor could they use the litigation to answer that question because the necessary evidence was a “state secret.” The result was that neither those plaintiffs nor any others could establish the requisite standing to obtain a judicial determination of the legality of the NSA’s conduct. The U.S. security state had, for decades, used this same “catch 22” to keep its activities beyond the reach of judicial review.

On June 6, 2013, *The Guardian* published the first Snowden story and, with it, a previously secret order from the U.S. Foreign Intelligence Surveillance Court directing a company called Verizon Business Records to turn over, on a daily basis, all telephony metadata of all its U.S. customers, to be stored for five years.³ One of those customers was the American Civil Liberties Union, which, within a week, had challenged the program in federal court.⁴ And in May 2015, the U.S. Court of Appeals for the Second Circuit issued a resounding 100-page rejection of the legal basis of the program—a decision that will have repercussions far beyond the particular facts of the case. Other lawsuits based on Snowden revelations are pending in other federal courts in what has become a revitalized judiciary.

The U.S. Congress

In the same month in which the U.S. Supreme Court was dismissing *Amnesty International v. Clapper* for lack of standing, James Clapper himself testified before Congress. In a now-notorious exchange, Clapper, the U.S. director of national intelligence, denied that the NSA was collecting any information about Americans on a mass scale:

SEN. RON WYDEN: Does the NSA collect any type of data at all on millions or hundreds of millions of Americans?

CLAPPER: No, sir.

SENATOR WYDEN: It does not?

CLAPPER: Not wittingly.

(Greenberg, 2013, video)

² <https://www.aclu.org/cases/amnesty-v-clapper-challenge-fisa-amendments-act>

³ <http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order>

⁴ <https://www.aclu.org/cases/aclu-v-clapper-challenge-nsa-mass-call-tracking-program>

Of course, the very first Snowden story proved these answers false. Most observers have characterized Clapper's testimony as lying under oath to Congress, but that may not be entirely accurate. Senator Wyden and other members of the Senate Intelligence Committee knew that the testimony was false, yet they failed to correct the public record. The exchange provides a rare public example of how the security state regularly defies congressional oversight: Even members of Congress like Senator Wyden, who objected to the intelligence community's policies and lies, felt powerless to enlighten the public. Years earlier, Senator Wyden stood on the floor of the Senate and declared, "When the American people find out how their government has secretly interpreted the Patriot Act, they will be stunned and they will be angry" (Savage, 2011, para 3). This turned out to be true, but it was Edward Snowden, and not any member of Congress, who ensured that the American people had a voice in the debate.

Fast forward, again, to 2015: On June 2 of that year, Congress enacted and the president signed the "USA Freedom Act" (Congress, 2015), a law that—for the first time since 1978—restricted rather than expanded the surveillance authority of the U.S. intelligence community. The vote followed a heated debate in which the intelligence community and its most loyal defenders deployed their whole playbook of threats and innuendo, suggesting that legislators who allowed the full powers of the Patriot Act to expire would be to blame for any future terrorist attack. This line of argument had virtually ensured congressional acquiescence in previous decades, but in the wake of the Snowden revelations, a bipartisan coalition of legislators called the intelligence community's bluff. While the USA Freedom Act does not resolve the challenges posed by mass surveillance, its passage represents a reinvigoration of legislative oversight that would have been inconceivable before Snowden.

The Media

In 2004, two investigative reporters at *The New York Times* discovered that President George W. Bush had authorized the NSA to conduct widespread domestic eavesdropping, in direct contravention of the Foreign Intelligence Surveillance Act. They did not publish their findings, however, until December 2005—after President Bush had been narrowly reelected. Rather, *The Times* was persuaded to suppress the story for more than a year after national security officials—including the president himself—warned the newspaper that publication would compromise a critical program and place American lives in peril. *The Times* reversed that decision only when it risked being scooped in a book by its own reporter James Risen. And, of course, no one has ever credibly argued that the exposure of the NSA's program caused a shred of harm to national security.

It was this episode that helped persuade Edward Snowden that he should not entrust the documents to a single news organization. That decision, in turn, forced news organizations like *The Washington Post* and *The Guardian* to worry not only about the government's predictable warnings but also about being scooped by rivals. And as other news organizations have been brought into the story, there has been a profound change in the landscape of national security reporting. First, more news organizations have been willing to stand up to government claims that publication of secrets would cause harm—at least in part because the Snowden documents exposed blatant lies by the same officials who argued against publication. And second, because government officials do not know what documents the news organizations are holding, it is more difficult to play the usual game of admitting as little as possible

and denying everything else. In all, the performance of the media in reporting on surveillance post-Snowden has, in large part, been admirable, and the national security press corps has been emboldened and empowered by the new climate.

Technology Companies

In 2016, the high-profile legal battle between the top law enforcement agency in the United States (the FBI) and the world's most profitable corporation (Apple) over access to an encrypted phone made headlines around the globe. This was not the first time since the Snowden revelations that the FBI had taken aim at Silicon Valley. In October 2014, FBI Director James Comey delivered a speech at the Brookings Institution, a prominent Washington think tank, in which he complained that the government was "going dark" because of more widespread deployment of encryption. Comey singled out Apple and Google for moving to encryption by default on their new operating systems, meaning that "the companies themselves won't be able to unlock phones, laptops, and tablets to reveal photos, documents, e-mail, and recordings stored within" (Comey, 2014, para 25).

This emergent public adversity between law enforcement and intelligence agencies, on the one hand, and powerful technology companies, on the other, may in time represent the most effective institutional constraint on government surveillance overreach. It is possible, as some have suggested, that the technology companies are principally concerned about their global business and cannot afford to be seen as conscripted pawns of the U.S. security state. But I also believe that these companies were genuinely shocked by some of the Snowden disclosures. They learned that even as the U.S. government was knocking on their front doors with court orders under programs like Prism, it was secretly breaking into their back doors to siphon off billions of communications.⁵ Whatever the motive (and it is likely that the companies have multiple motives), the growing willingness of powerful corporations to push back against the demands of the security state, and the more widespread deployment by these corporations of end-to-end encryption, constitutes a new kind of bulwark against the dangers of aggregated executive powers.

Conclusion

In sum, four critical mechanisms of intelligence oversight have been significantly strengthened by the debate that Snowden helped launch. It may seem ironic that a dramatic act of lawbreaking had the effect of reinvigorating meaningful democratic oversight, but in the United States, we have seen that pattern before.⁶ And while all Western democracies can and should do more to improve the structure of intelligence oversight, there will always be a need for individual acts of conscience and courage.

⁵ See, e.g., https://www.washingtonpost.com/world/national-security/nsa-infiltrates-links-to-yahoo-google-data-centers-worldwide-snowden-documents-say/2013/10/30/e51d661e-4166-11e3-8b74-d89d714ca4dd_story.html

⁶<http://www.nytimes.com/2014/01/07/us/burglars-who-took-on-fbi-abandon-shadows.html>

References

- Comey, J.B. (2014, October 16). Going dark: Are technology, privacy, and public safety on a collision course? *Speech delivered at Brookings Institution*. Washington, DC. Retrieved from <https://www.fbi.gov/news/speeches/going-dark-are-technology-privacy-and-public-safety-on-a-collision-course>
- Congress (2015). H.R.2048 — USA Freedom Act of 2015. *114th Congress*. Retrieved from <https://www.congress.gov/bill/114th-congress/house-bill/2048/text>
- Greenberg, A. (2013, June 6). Watch top U.S. Intelligence officials repeatedly deny NSA spying on Americans over the last year. *Forbes*. Retrieved from <http://www.forbes.com/sites/andygreenberg/2013/06/06/watch-top-u-s-intelligence-officials-repeatedly-deny-nsa-spying-on-americans-over-the-last-year-videos/#7067e34f21d3>
- Savage, C. (2011, May 26). Senators say Patriot Act is being misinterpreted. *The New York Times*. Retrieved from http://www.nytimes.com/2011/05/27/us/27patriot.html?_r=0