The Transformation of the National Security Agency

David Pan

The NSA is undergoing a transformation. The days when it could be No Such Agency are a distant memory, and it must now develop and maintain an extensive publicity campaign. Though this change was forced upon it by the documents stolen and divulged by former contractor Edward Snowden in June 2013, these revelations were merely the catalyst for publicizing a fundamental change in the relationship between the NSA and the broader public that has been quietly taking place for several years, ever since the internet and the digitization of our lives started becoming mass phenomena. Even if the NSA resisted disclosing the nature of these changes in its role in public life, they would have eventually become clear one way or another. Many of its programs will need to be reevaluated in light of the new relation the NSA now has with the public. On the one hand, some programs may need to be curtailed or amended as a result of this new era of NSA transparency. On the other hand, new programs will be developed that respond to and take advantage of this newfound prominence in American public life. What are the underlying global shifts that have made these changes for the NSA inevitable, and how will they affect NSA activities for the future?

In the first place, it must be made clear that the NSA did not do anything wrong; indeed it has been carrying out the missions assigned to it with skill and integrity. Even though the programs for collecting telephone metadata on U.S. numbers and data from internet companies on foreign targets remained secret,[1] they did not go beyond the legal restrictions on

1. Ellen Nakashima, "Verizon Giving Call Data to NSA," *Washington Post*, June 6, 2013; Barton Gellman and Laura Poitras, "U.S. Mines Internet Firms' Data, Documents Show," *Washington Post*, June 7, 2013.

Telos 169 (Winter 2014): 162–69.
doi:10.3817/1214169162
www.telospress.com

NSA activity. The President's Review Group on Intelligence and Communications Technologies noted that it "found no evidence of illegality or other abuse of authority for the purpose of targeting domestic political activity."[2] In addition, the Review Group affirms that NSA surveillance has been in no way indiscriminate but has focused on national security and has operated according to an extensive system of oversight, review, and checks-and-balances established by the Foreign Intelligence Surveillance Act of 1978 to prevent violations of the law.[3] Since the NSA has up to now been acting legally and with extensive oversight, the focus of discussion has not been on any past violations of privacy but on the potential for abuse that the mass collection of data would entail.

Liberal Democrats and libertarian Republicans both see a serious threat to privacy in the bulk collection of data. Sue Halpern treats it as a form of spying in itself.[4] Rand Paul describes it as a form of "generalized warrants, where soldiers would go from house to house, searching anything they liked."[5] The difficulty with these characterizations is that the bulk collection of data goes on already in many contexts outside of the NSA. Telecommunications companies, internet service providers, search engines, financial institutions, and government agencies such as the IRS all do bulk collection of data to create vast databases. If such collection by the government were a form of spying, then it would already be prohibited by the Fourth Amendment, which protects citizens from all unreasonable search or seizure, regardless of which government agency carries it out. But the crucial issue is not the creation of the database but the carrying out of a search upon that database. Indeed, if we were to find out that employees of a telecommunications company were running indiscriminate searches on their data, we would be just as concerned about the propriety of those searches as with the federal government. Business records, including those of financial institutions and health providers, as well as tax records to which governments have access, have existed from well before

2. Richard A. Clarke, Michael J. Morell, Geoffrey R. Stone, Cass R. Sunstein, and Peter Swire, *The NSA Report: Liberty and Security in a Changing World: Report and Recommendations of the President's Review Group on Intelligence and Communications Technologies* (Princeton, NJ: Princeton UP, 2014), pp. 31–32.

3. Ibid., p. 31.

4. Sue Halpern, "Partial Disclosure," *New York Review of Books* 61, no. 12 (July 10, 2014): 16–20.

5. Rand Paul, "Big Brother Really Is Watching Us," *Wall Street Journal*, June 11, 2013.

the digital age, and the collection of those records has never been found to be a form of search. The search begins when a specific query is put to the data.

The essential disquieting difference between the search on the telephone database and the Redcoat rifling through the records of, say, a post office is the ease and the surreptitiousness with which the modern data search can be carried out. Consequently, the federal government has established an elaborate set of controls to ensure that every NSA search on the data is not conducted on any U.S. person (defined as any U.S. citizen or permanent resident anywhere in the world and any person at all who is on U.S. soil) and, in addition, is based on a "'reasonable articulable suspicion' that terrorist activities are taking place and that the searches would help uncover them."[6] Administratively developed and court-approved guidelines have been established to govern searches, and analysts receive extensive training to ensure compliance. A team of three hundred compliance officers oversees the searches, and all searches are documented and subject to subsequent review by all three branches of government.[7] The secret nature of these processes and controls creates fears of possible abuse, but now that the collection programs have been disclosed, secrecy is no longer the problem, and they may even be expanded, though with more public oversight.

While Snowden's revelations were indeed a turning point, this sudden forcing of the NSA into the limelight of American politics after its history of secrecy has ultimately been the result of a long-term process in which it has had to adapt to the blurring of the border between private and public in both its foreign intelligence and domestic security missions. The rise of the internet has meant that more and more of the signals intelligence that the NSA captures comes, not from purely foreign networks, but from worldwide, public networks in which both domestic and foreign, private and public traffic intermingle. As a consequence, the collection, decoding, and offensive capabilities of the NSA have become more and more entangled with the networks we use on a day-to-day basis. Signals intelligence is not just a matter of penetrating an enemy network but of isolating enemy

6. Mike Pompeo and David B. Rifkin, Jr., "Digging the NSA Out of the Snowden Storm," *Wall Street Journal*, November 20, 2013.

7. Siobhan Gorman, "Spy Agency Defends Itself After Privacy Breaches Revealed," *Wall Street Journal*, August 17, 2013; L. Gordon Crovitz, "Information Age: More Surveillance, Please," *Wall Street Journal*, August 26, 2013.

communications from the noise of the entire internet. This disentangling of information will necessarily lead to the accessing of domestic information that is protected by our privacy laws and of foreign information whose disclosure would anger our allies. The discussion of the proper checks and restrictions on this process has to be a broader one that involves more than just the intelligence community, which should not be expected to make such judgments on its own.

So the NSA is entering a new era, in which it is starting to become much more transparent about its activities, disclosing previously classified documents, making public statements, inviting journalists and academics into its discussions, and collaborating with businesses and other institutions on issues such as cybersecurity.[8] In fact, to the extent that its Information Assurance Directorate, in protecting government systems, also contributes to the security of the internet overall, it will have an increasingly important role in guaranteeing its structures. This increasing communication and cooperation with the public will require the NSA to make some compromises in its intelligence gathering mission. If its previous strategy was to go after intelligence wherever they could find it and as secretly as possible, they will now have to make determinations about the consequences of their methods for others. One clear example of unintended consequences is the reduction in international sales that companies such as Verizon have encountered since revelations about their cooperation with the NSA.[9] Another is the move by some countries toward "national" internets that threaten to break up the internet world into separate regions.[10] As the NSA begins to factor in these risks into its deliberations about its methods, it will have to understand its role more and more as a steward of the internet itself.

This new role represents a fundamental shift in the function of the NSA, one that only becomes clear once we understand the precise importance of U.S. authority in maintaining the security of cyberspace as a space of creativity and open exchange. L. Gordon Crovitz has compared this U.S. responsibility to its similar task of safeguarding the freedom of the seas. This freedom is not the product of an absence of sovereignty and control,

8. Daniel Byman and Benjamin Wittes, "Reforming the NSA," *Foreign Affairs* 93, no. 3 (May 2014): 127–38.

9. Anton Troianovski and Danny Yadron, "Germany to End Verizon Contract," *Wall Street Journal*, June 27, 2014.

10. John Blau, "NSA Surveillance Sparks Talk of National Internets," *IEEE Spectrum* 51, no. 2 (February 2014): 14–16.

but rather of the U.S. commitment to maintaining it with the use of its navy.[11] Similarly, the freedom and openness of the internet are not naturally occurring characteristics but are rather the outcome of U.S. efforts to establish and guarantee structures that ensure free access to internet sites, a lack of restrictions on who may establish such sites, and the security of communications. While free access is often restricted by governments, such as China's, that prevent access to certain sites, the Internet Corporation for Assigned Names and Numbers (ICANN), overseen by the U.S. Commerce Department, has maintained a policy of open access to domain names for hosting content. As Crovitz points out, the Obama administration's announcement of plans to relinquish this authority over ICANN, possibly to an international body, risks compromising the current openness.

To understand why, we must consider the importance of the United States and the NSA in guaranteeing the functioning of the internet, whose structure is not a given but has been the result of the U.S. commitment to individual freedom, even at the expense of competing, legitimate government interests. David Post illustrates the complexity of the discussion of internet governance by citing the example of "Women on Web," a Dutch website that provides advice on abortions and arranges for the shipping of medical abortion drugs, mifepristone and misoprostol, to women in countries where such abortions are illegal.[12] Though it operates legally under Dutch law, other countries such as Ireland or Brazil would deem the site illegal and might want to shut it down. At this point, there is no clear way to adjudicate such disputes, but ICANN controls the mechanisms for carrying out judgments about such issues because it oversees the Domain Name System and could shut down a website by causing the removal of its domain name from the system. But who should make this determination? Cases such as the "Women on Web" website fall into a gray area between the child pornography sites, which all agree should be shut down, and those of political opposition groups such as the Free Syrian Army, which are being allowed to operate based on specific political preferences. These kinds of issues cannot be resolved without a governing legal and political framework. At present it is ultimately the responsibility of the

11. L. Gordon Crovitz, "America's Internet Surrender," *Wall Street Journal*, March 19, 2014.

12. David Post, "Abortion, ICANN, and Internet Governance," *Volokh Conspiracy* (blog), *Washington Post*, September 1, 2014, http://www.washingtonpost.com/news/volokh-conspiracy/wp/2014/09/01/abortion-icann-and-internet-governance/; Emily Bazelon, "The Post-Clinic Abortion," *New York Times Magazine*, August 31, 2014, p. 22.

U.S. government to be the final arbiter in such cases, acting according to the U.S. Constitution, which has strong protections on freedom of speech and individual privacy. At the same time, cases such as the website of the Free Syrian Army or the possibility of one for the Islamic State make clear that these decisions are political ones as well. An international or multistakeholder structure would clearly lack the legal and political authority to make such decisions. If there is discomfort about the U.S. government's authority over such issues, it is questionable whether the situation would be improved if Google and Amazon, China and Russia, were determining, for example, which rebel groups in Syria can keep their own websites.

But aside from the need for a sovereign power to make such legal and political decisions about access, the internet itself depends upon U.S. governing authority in order to preserve its current free and open structure. The Snowden disclosures have led many, including the current president of ICANN, Fadi Chehadé, to question U.S. oversight over ICANN and argue for the move toward a "multistakeholder" structure for its governance that would realize the dream of "self-governance by the Internet community."[13] While such supporters of detaching ICANN from U.S. authority generally agree that moving this authority to an international governmental body such as the International Telecommunications Union of the United Nations could subject it to interference from countries that would support more censorship, the alternative they propose is to privatize ICANN so that it can be free of all government control. Both liberal supporters of internationalism such as Chehadé and libertarian promoters of the free market imagine that freedom is a kind of natural state that arises when government sovereignty recedes. Yet, free markets cannot exist without governments that guarantee rules about such matters as private property and binding contracts. Such markets disappear both in locations where the ruling authorities oppose free market practices (e.g., North Korea) and in places where all government has broken down (e.g., Somalia). Similarly, the rise of the internet was not a spontaneous event but was fostered by the U.S. government as a way to link universities and research labs into a network with cheap, open access and freedom of expression. The internet's success compared to other similar networks (e.g., France's Minitel

13. Fadi Chehadé, Testimony before the House Judiciary Subcommittee on Courts, Intellectual Property, and the Internet at an April 10, 2014, hearing titled "Should the Department of Commerce Relinquish Direct Oversight Over ICANN?" *Congressional Digest*, June 2014: 26–30, here 30.

network) hinged upon the U.S. government's continual safeguarding of these principles of operation and governance. To think that the internet has now "matured" to the point that it might govern itself misunderstands the nature of markets and networks. They can easily fragment or dissolve once the governing conditions of their existence no longer hold, and the internet cannot govern itself any more than capitalism can exist without a stable government that would guarantee the rule of law. However ICANN is reorganized, its officers and offices will still have to exist in the real world somewhere and will thus inevitably be subject to governmental control and a legal system that governs its activities. The U.S. has proven itself to be uniquely suited to fulfilling this role through its historic commitments to free speech, open access, intellectual property rights, and a multistakeholder approach to internet governance *within the framework of U.S. government authority*. An alternative authority might bow to pressure from nations such as Russia or China to curtail the current open access policies. Alternatively, the internet could fragment into separate national networks, each with its own governance structure. The way to preserve the current successful structure of the internet is to maintain U.S. oversight over its governing bodies.

The NSA has an important role to play in maintaining this oversight because a crucial element to protecting internet freedom is the protection of data. The NSA's task of safeguarding government systems makes it into a natural partner for data security for non-governmental enterprises as well. The frequency and severity of hacker attacks on businesses has highlighted the ways in which the biggest current threat to privacy is not the NSA but cyberattacks from criminals and foreign governments. As Jack Goldsmith has argued, cyberattacks are already causing serious problems that will only worsen in the future, and as they do, more people will be calling on the NSA to play an increased role in combatting them, even at the expense of allowing it to have more collection and search capabilities.[14] The NSA is poised to become one of the main protectors of privacy and security on the internet—the equivalent of the U.S. Navy for cyberspace.

Like the navy, though, the NSA will continue to maintain its offensive signals intelligence mission of penetrating foreign networks in order to obtain information, often keeping secret so-called "zero-day" vulnerabilities (meaning that they are freshly discovered and security specialists

14. Jack Goldsmith, "We Need an Invasive NSA," *The New Republic*, October 21, 2013, pp. 10–12.

have had "zero days" to fix them) in order to use in its attacks rather than revealing them in order to improve security on all systems. To the extent that firms specialize in finding such vulnerabilities and then selling them to the highest bidder, the NSA is just one of many organizations that stockpile and use them for offensive purposes and would be at a considerable disadvantage if it had to operate without them.[15] The NSA and the United States as a whole will have to continue to weigh the risks and rewards in making judgments about discovered vulnerabilities. It will be important to remember, though, that America's enemies will continue to be the main enemies of free speech and privacy rights all over the world. To the extent that the NSA's offensive capabilities are directed at such enemies, it will be working to defend the current free and open nature of the internet in general. In this new role, the NSA's current prominence in newspaper reporting will be not a temporary phenomenon but a stage in the movement toward a new, closer relationship between the NSA and the public. This shift already began with the rise of the internet. Now that the nature of this shift has been made clear to the world, the NSA can make the case that it is perhaps one of the most important defenders of our privacy and security in a digital world.

15. Tom Simonite, "Welcome to the Malware-Industrial Complex," *MIT Technology Review* 116, no. 3 (May 1, 2013): 16–18.