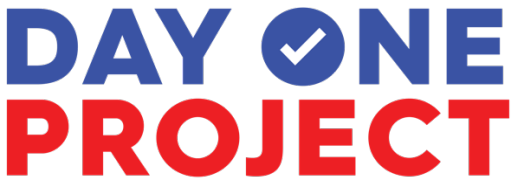
A National Strategy on Privacy and Civil Liberties

Alex Marthews and Catherine Tucker

January 23, 2020



dayoneproject.org

Summary

In the 20th century, the costly nature of surveillance made it easier to maintain Constitutional guarantees protecting U.S. persons[1] from mass surveillance. In the 21st century, digitization of our everyday lives and communications has sharply reduced surveillance costs[2]—and indeed, changed the nature of surveillance itself.[3] The core responsibility of any President is to "preserve, protect and defend the Constitution," but recently unsealed federal court rulings show that intelligence agencies such as the Federal Bureau of Investigation (FBI) and the National Security Agency (NSA) are routinely accessing the digital communications of U. S. persons and otherwise using digital surveillance in ways that violate Americans' Fourth Amendment rights against "unreasonable searches and seizures."[4] To fulfill their oath of office, the next president should take concrete steps to reform federal operations with respect to digital surveillance. This is important not only for protecting basic American rights, but also for diplomatic relations with key foreign allies.[5] Instituting meaningful protections against government surveillance in the United States would have the significant diplomatic benefit of helping reestablish the credibility of American calls for other countries to adhere to high human-rights standards.

1. Challenge

The world is no longer divided into communist and capitalist countries. Instead, we can organize countries along a spectrum of how much they deploy surveillance technologies against their own citizens. In some countries, such as China, surveillance concerns take precedence over a human right to privacy of communications, and over religious or political freedoms.[6] At the other end of the spectrum, European courts have begun to invalidate mass surveillance schemes that are not "proportionate" to member states' needs.[7] The United States must determine where it falls—and where it wishes to fall—on

---

[1] Throughout this document, we use the term "U.S. persons" to denote the set of persons who, either through citizenship or through "substantial voluntary connections" to the United States, have Fourth Amendment rights that the federal government is obligated (through prior Supreme Court decisions) to respect. The term "U.S. persons" here includes corporations headquartered in the United States.

[2] The cost of digital surveillance is incomparably lower than the cost of in-person, round-the-clock surveillance by human agents, as is the cost per datum collected. Of course, a "collect it all" mentality has led intelligence agencies to spend more overall on storage of surveillance information in the digital era than in prior eras.

[3] Daniel Zwerdling, "Your Digital Trail: Does The Fourth Amendment Protect Us?", National Public Radio, October 2, 2013, https://www.npr.org/sections/alltechconsidered/2013/10/02/228134269/your-digital-trail-does-the-fourth-amendment-protect-us.

[4] Elizabeth Goitein, "The FISA Court's 702 Opinions, Part I: A History of Non-Compliance Repeats Itself", Just Security, October 22, 2019, https://www.justsecurity.org/66595/the-fisa-courts-702-opinions-part-i-a-history-of-non-compliance-repeats-itself/.

[5] The surveillance scandals under President Obama, where internal documents were leaked showing the NSA to have been collecting both domestic and foreign communications on a mass and suspicionless basis, caused significant and foreseeable diplomatic fallout, especially hampering foreign relations with the European Union and Brazil.

[6] Dominic J. Nardi, "Religious Freedom in China's High-Tech Surveillance State", United States Commission on International Religious Freedom (September 2019).

[7] European Court of Human Rights, *Case of Big Brother Watch and Others v. The United Kingdom*, Judgment (Merits and Just Satisfaction), application nos. 58170/13, 62322/14, and 24960/15, September 13, 2018.

this spectrum. The challenge faced by the federal government is to reinforce meaningful protections against unwarranted surveillance.

2. Proposed action

Responsibility for privacy and surveillance issues in the United States is spread across 17 surveillance agencies, the Department of State, the Federal Communications Commission (FCC), and the Federal Trade Commission (FTC). Inspectors-general and the Privacy and Civil Liberties Oversight Board (PCLOB) provide executive-branch oversight. This diffusion of responsibility across different agencies presents an obstacle to a comprehensive, government-wide effort to limit digital surveillance and protect privacy rights. But there are still ways in which the federal government can begin to address these issues, guided by the following aims:

(1) Reduce spillovers related to mass collection of data on foreign targets that result in incidental collection of data on U.S. persons.
(2) Restrict collation of data on U.S. persons.
(3) Protect commercial software users against scalable software vulnerabilities.

2.1 Reduce data spillovers

In the pre-digital era, collection of foreign intelligence data was largely done on a person-by-person basis and hence did not usually involve U.S. persons *en masse*. The Foreign Intelligence Surveillance Act (FISA) of 1978, passed after the Watergate scandal, was intended to authorize spying on individual foreign nationals who, as agents of a foreign power, were not protected by Fourth Amendment constraints on searches and seizures of their communications.

In the digital era, however, the adoption of "programmatic warrants" (through Section 702 authority established by the FISA Amendments Act of 2008) has moved the NSA away from individualized data collection.[8] Even where there continues to be an individual foreign target, current law gives NSA authority to collect metadata on the communications of that target's contacts and their contact's contacts ("two-hop collection"). Hence, a single order from the Foreign Intelligence Surveillance Court permitting the search of particular "selectors"[9] can translate into tens of thousands of foreign "targets" who use those selectors and tens of thousands of their contacts whose

[8] Section 702 "allows the government to get what is called a programmatic warrant. It lasts for an entire year and authorizes the government to collect a potentially large number of phone calls and e-mails, with no requirement that the senders or recipients be connected to terrorism, espionage--the threats we are concerned about." Source: Sen. Ron Wyden (Oregon), "FISA Amendments Act Reauthorization Act of 2012", *Congressional Record* 158, Pt. 168 (December 27, 2012) p. S8384–S8410.
[9] A "selector", in surveillance terminology, is a search string linked to a target, used to identify communications of interest. including email addresses, phone numbers, bank account numbers, or other identifiers.

communications are "incidentally" collected. These targets and their contacts include many U.S. persons.

For the small subset of communications that cannot be gathered under the NSA's Section 702 authority,[10] the Call Detail Records (CDR) program, operating under the business records provision of PATRIOT Act section 215, permits similar collection of the metadata (but not the content) of communications between presumed U.S. persons. In 2018, collection on just 11 acknowledged targets in the "Call Detail Records" (CDR) program resulted in collection relating to 19 million phone identifiers, for a total of over 434 million records.[11]

It is inevitable that as long as "two-hop collection" exists, it will sweep the communications of many U.S. persons into surveillance conducted by the U.S. government. This places us as a nation very far from a world where, in line with the Fourth Amendment, individualized probable cause is established prior to searching or seizing someone's communications. If foreign-intelligence information is made available relatively easily to domestic law enforcement, then the Fourth Amendment effectively no longer applies to the millions of Americans who are contacts of contacts of foreign-intelligence collection targets, or who are contacts of targets of domestic "business records" orders under Section 215 of the PATRIOT Act.

The federal government should compartmentalize data derived from foreign-intelligence collection to prevent this kind of "end run" around the Fourth Amendment rights of U.S. persons. Specifically, the federal government should ensure that that domestic law enforcement cannot access warrantlessly collected data related to U.S. persons without an individualized warrant—issued by an independent judge based on probable cause of involvement in a crime—for its decryption. In addition, the federal government should update Department of Justice (DOJ) policies to make it unlawful for the FBI to access NSA or other foreign-intelligence data related to U.S. persons if a significant purpose of accessing a foreign target's communications is to obtain data on U.S. persons' data.[12] The FBI should confine its "assessments" of threats to circumstances where there is a factual predicate to suspect violations of federal law. These actions are in line with proposals embodied in the proposed USA RIGHTS Act of 2017[13] and supported by

[10] Section 702 authority covers only communications where one end of the conversation is deemed (with over 50% probability) to not be a U.S. person. Communications where the IP address is masked, such as those occurring over the encrypted search engine Tor, are deemed by default to be of non-U.S. persons.
[11] Office of Civil Liberties, Privacy, and Transparency, *Statistical Transparency Report Regarding the Use of National Security Authorities: Calendar Year 2018*, Office of the Director of National Intelligence (April 2019).
[12] Currently, this is only prohibited if the *sole* purpose is to obtain data on U.S. persons.
[13] U.S. House, 115th Congress, *H.R. 4124, USA RIGHTS Act.*

several presidential candidates.[14] Finally, the federal government should support a permanent statutory end to the CDR program.

2.2 Restrict collation of data on U.S. persons

In the pre-digital era, it was not practical to merge different data sources about large segments of the population at scale. Today's technology has made such mergers possible. After the 9/11 terrorist attacks, the U.S. government established data "fusion centers", funded in part by the Department of Homeland Security (DHS), to provide actionable, "joined-up" intelligence.

However, the fact that we have the capacity to merge data at scale does not guarantee that the inferences we make from those data are either accurate or useful. The accuracy of large, synthesized databases depends on the quality and interpretation of inputs. Research on private-sector efforts to create user profiles through merged data reveals how unreliable such profiles can be. For example, private data-broker firms worth billions of dollars were unable to accurately state gender for an individual more than 50% of the time—in other words, for all their data collected, they achieved results no better than flipping a coin.[15] Indeed, data derived from the fusion centers themselves suggest that insights derived from merged data are often irrelevant to thwarting terrorist attacks.[16]

The federal government should withdraw DHS funding for "fusion centers". The federal government should also require purging of all fusion-center data on individuals that are found to not meet basic Fourth Amendment standards of constituting reasonable, articulable suspicion of a crime.

2.3 Protect against scalable software vulnerabilities

An exploit that uses an individual's information to compromise a single target computer is not a systemic threat. However, a security vulnerability that allows a nefarious actor to attack multiple computers at little cost represents a large threat to economic prosperity and societal well-being. At present, the intelligence community does not appropriately weight these relative risks when deciding whether or not to disclose an identified security vulnerability in a piece of software to the software manufacturer. The federal government

---

[14] Of those running as of January 2020, this includes Bernie Sanders, Elizabeth Warren, and Tulsi Gabbard. *See* https://www.decidethefuture.org/?filtered=All&membership=All&party=All&candidacy=Yes for details on votes taken.

[15] Nico Neumann, Catherine E. Tucker, and Timothy Whitfield, "How Effective Is Third-Party Consumer Profiling and Audience Delivery?: Evidence from Field Studies", *Marketing Science - Frontiers* (June 2019).

[16] "A lot of [the reporting] was predominantly useless information," one former Senior Reports Officer, who worked in the Reporting Branch from 2006 to 2010, told the Subcommittee. "You had a lot of data clogging the system with no value." Overall, the former official estimated 85% of reports coming out of the Reporting Branch were "not beneficial" to any entity, from Federal intelligence agencies to state and local fusion centers." *See* "Federal Support For And Involvement In State And Local Fusion Centers", U.S. Senate Permanent Subcommittee on Investigations, October 3, 2012, p. 27, https://www.hsgac.senate.gov/imo/media/doc/10-3-2012%20PSI%20STAFF%20REPORT%20re%20FUSION%20CENTERS.2.pdf.

should reform the NSA's "Vulnerabilities Equities Process" such that scalable software vulnerabilities identified by the NSA and other agencies are always shared promptly with the software firm concerned. The federal government should also resist calls to mandate lawful access to encrypted content and metadata held on the computer systems of U.S. firms. Such measures will erode data security and cannot guarantee that only law enforcement will take advantage of the weaknesses such a mandate would introduce.

3. Rationale

In the laws governing surveillance, distinctions abound between how communications of U.S. and non-U.S. persons are treated. Privacy protections for the communications of those inferred to be U.S. persons are generally stronger. The Fourth Amendment to the U.S. Constitution sets stringent limits on the circumstances under which, for domestic law enforcement purposes, the government may search or seize the "persons, houses, papers or effects" of U.S. persons. To be "reasonable", such a search or seizure must generally be accompanied either by consent of the person targeted, or by a warrant issued by an independent judge.

This distinction is harder to manage in the digital era, where surveillance tools can be easily deployed on a mass scale. Digital surveillance has dramatically increased the amount of data accessible by U.S. intelligence agencies, and engenders several serious problems. First, large-scale data collection for foreign intelligence purposes leads to warrantless data collection on U.S. persons. Such data-collection "spillovers" create "chilling effects" on the speech and associations of U.S. persons.[17] Second, digital surveillance by the U.S. government compromises the security reputation of U.S.-headquartered firms, diminishing these firms' ability to market to consumers.[18] Third, U.S. intelligence agencies sometimes allow vulnerabilities in publicly available software to go unaddressed so that these vulnerabilities can be exploited for U.S. intelligence collection. These vulnerabilities can be exploited by foreign governments and criminals as well as domestic law enforcement. Executive-branch regulations and legislative statutes must be updated to address these problems and ensure that Fourth Amendment protections are maintained in the digital era.[19]

[17] See Marthews and Tucker, "Government Surveillance and Internet Search Behavior", for a quantification of these chilling effects as they relate to users of Google search.

[18] Catherine E. Tucker, "Social networks, advertising and privacy controls", *Journal of Marketing Research* 51, no. 5 (2014): 546–562.

[19] In the healthcare sector, a regime focused on giving patients meaningful ownership of their data encourages patients to take wiser decisions than a consent-based privacy regime. *See* Amalia R. Miller and Catherine Tucker, "Privacy protection, personalized medicine, and genetic testing", *Management Science* 64, no. 10 (2018): 4648–4668.

3.1 Reduce data spillovers

The Cold War imbued the U.S. government with an increased sense of the need for foreign intelligence. However, it was not obvious how foreign-intelligence collection would fit inside the framework of the Fourth Amendment. If foreign-intelligence collection was only permissible if the foreign national in question was suspected of breaking U.S. law, then U.S. intelligence agencies would miss reams of economic, diplomatic, and military information that the Soviet Union and other rivals were more than happy to collect. The challenge of threading this needle meant that for decades, there were few formal regulations governing foreign-intelligence collection in the United States. Between 1945 and 1974, the newly founded Central Intelligence Agency (CIA) and the NSA informally collected increasing amounts of information via old-fashioned human intelligence and telephone networks.

Things came to a head with the Watergate scandal. Watergate revealed that the Johnson and Nixon administrations had used these foreign-intelligence collection tools against U.S. persons via the "COINTELPRO" domestic surveillance program, to investigate and disrupt the anti-war left and the civil rights movement. The result of that realization was the Foreign Intelligence Surveillance Act (FISA). FISA legitimated many, though not all, of the data-collection practices already being used informally by the intelligence community. FISA also explicated the circumstances under which foreign intelligence could be gathered in the context of the Fourth Amendment. The idea was that whenever members of the intelligence community wanted to spy on an individual, they would get permission from a new, secret Foreign Intelligence Surveillance Court—permission that would not require probable cause of involvement in a crime. In exchange, new mechanisms would ensure that the FBI and local law-enforcement agencies could not readily access information collected in a way that infringed on Fourth Amendment rights.

The provisions created by FISA made sense in the pre-digital era. The costs and labor requirements of pre-digital methods of intelligence collection such as phone taps meant that surveillance would involve the foreign target and those whom they directly wrote to or spoke with, which was unlikely to implicate U.S. persons at scale. Digitization has changed this calculus. Digital data-collection tools make it cheap to collect information on lots of people at scale. It is also harder to separate foreign from domestic traffic on packet-switched networks (a type of network widely implemented on local computer networks and on the internet) than it is on phone landlines.

The legal regime protecting U.S. persons from the spillovers of foreign data collection has failed to keep up with the expansion of data collection enabled by digital-surveillance tools. Documents released by the Privacy and Civil Liberties Oversight Board

(PCLOB) in 2016 noted that while "FBI analysts and agents who solely work on non-foreign intelligence crimes are not required to conduct queries of databases containing Section 702 data [referring to data collected under the 2008 Amendments to FISA], they are permitted to conduct such queries and many do conduct such queries."[20] In other words, data on U.S. persons collected as a byproduct of foreign-intelligence efforts are being viewed by more people much more than originally envisioned under FISA. The PCLOB recommended that internal FBI supervisory approval (but not a warrant) should be needed for such queries.[21]

The CDR program provides a useful example of the consequences of this "opening up" of foreign intelligence data. Authorized under section 215 of the PATRIOT Act, the CDR program collects metadata such as "an originating or terminating telephone number, an International Mobile Subscriber Identity (IMSI) number, or an International Mobile Station Equipment Identity (IMEI) number, a telephone calling card number, or the time or duration of a call" on calls placed or received by a CDR program target."[22] Program targets may include people two degrees away from the primary target (*i.e.*, contacts of contacts of the primary target), meaning that the vast majority of people surveilled through the CDR program are neither suspected of wrongdoing nor directly in contact with anyone who is.[23] In 2018, the U.S. government used the CDR program to collect data on 11 primary targets, but through that targeting, collected over 434 million telephone records relating to over 19 million phone identifiers. These records can then be used to investigate U.S. persons directly, thereby circumventing Fourth Amendment privacy protections. A 2018 report from the Director of National Intelligence (DNI) identified 164,682 instances when the CDR database was queried using a search term that concerned a U.S. person.[24] In an earlier paper, we collect evidence that surveillance programs such as the CDR program also hurt the commercial success of U.S. companies abroad and at home.[25]

According to the national security adviser for Republican House Minority Leader Kevin McCarthy, the NSA is no longer using the CDR program as of March 2019.[26] However, the Trump administration's new acting DNI has publicly supported renewal of CDR powers.[27] The NSA has recently suggested that, someday, there might be a terrorist

[20] Privacy & Civil Liberties Oversight Board. *Recommendations Assessment Report* (February 2016).
[21] *Ibid.*, footnote 3.
[22] Office of Civil Liberties, Privacy, and Transparency, *Statistical Transparency Report*, 27.
[23] *Ibid.*, 28 and 30.
[24] *Ibid.*, 31.
[25] Marthews and Tucker, "Government Surveillance and Internet Search Behavior".
[26] Charlie Savage, "Disputed NSA Program Is Shut Down, Aide Says", *New York Times*, March 4, 2019, https://www.nytimes.com/2019/03/04/us/politics/nsa-phone-records-program-shut-down.html.
[27] Loren Blinde, "Acting DNI Maguire issues statement on USA FREEDOM Act", Intelligence Community News, September 20, 2019, https://intelligencecommunitynews.com/acting-dni-maguire-issues-statement-on-usa-freedom-act/.

whose communications would be captured under a program like CDR—and that for that reason, CDR authorities should be maintained. As of December 2019, the scheduled sunset of section 215 powers had been temporarily delayed to March 2020.

The federal government should put a statutory end to the CDR program. The best model for surveillance-reform legislation brought to the floor in Congress in recent years was the USA RIGHTS Act of 2017. This bill would have prohibited the "bulk collection" of telephone or communications records of Americans; prohibited National Security Letters (essentially a secret administrative subpoena) from being used for bulk collection; prohibited government collection of communications "about the target" rather than to or from the target in non-terrorism investigations; restricted more strictly the use of unlawfully collected information; and created an independent Constitutional Advocate to argue in significant cases by declassifying Court decisions and allowing Constitutional challenges to federal court decisions.[28] The roll-call votes showcased the strength of cross-partisan support.[29]

3.2 Restrict collation of data on U.S. persons

The cost of combining different data sources has fallen sharply. In the pre-digital era, only a sense that someone was a threat justified investing in the costly process of combining data sources to create a file on that individual. High costs of data collection and integration acted to buttress Constitutional protections against mass surveillance. It is now possible and relatively inexpensive to collect, share and combine a digital dossier on every U.S. person. However, the fact that it is possible does not make it either desirable or Constitutional.

Existing statutes purposefully limit how certain types of government data, notably census data and gun-trace data, can be used and shared. By contrast, increasing data collection and sharing is generally seen as a good thing when it comes to counterterrorism operations. This motivates intelligence agencies to integrate data from multiple sources, including data that was collected from individuals under analog-era expectations (such as state Department of Motor Vehicle (DMV) photos). The main locus for data-sharing and -integration efforts in the intelligence community is the nationwide network of offices known as "fusion centers". The fusion-center network was launched in the wake of the 9/11 terrorist attacks "to address concerns that local, state and federal authorities were

[28] See Lawrence Husick, "The USA Rights Act: What's In There?", Foreign Policy Research Institute, November 1, 2017, https://www.fpri.org/2017/11/usa-right-act-what-in-there/ for a lengthier summary of the bill's provisions. The USA RIGHTS Act votes were 183-233 in the House and 34-65 in the Senate.

[29] The most recent such effort in the House failed 175-253, with about one-third of Republicans and one-half of Democrats voting in favor.

not sharing information effectively about potential terrorist threats."[30] Fusion centers are located in every state (California alone has six) and are typically set up under the budgetary authority of state and local police departments but receive some grant funding and policy guidance from DHS. The intent of these centers is to provide "joined-up intelligence" to prevent new terrorist attacks, integrating tips and leads from local police with insights from the intelligence community.

Unfortunately, fusion centers have proven ineffective. In 2012, a Senate oversight committee found that there was no known instance of fusion centers helping to thwart a terrorist attack but that there were many instances of fusion centers wasting funds to produce alerts too late to be of use.[31] Fusion centers' "Suspicious Activity Reports" are filed disproportionately on members of ethnic and religious minorities and in over 50% of cases contain nothing of criminal or intelligence value.[32,33] In 2017, fusion centers played a "direct role" in only 14 terror-related incidents (out of 59 total), down from 24 the previous year.[34]

Databases generated by fusion centers are often inaccurate as well as unhelpful. In the private sector, inferring demographics based on browsing data can lead to substantial data inaccuracy, especially where there are other people in a household.[35] In fusion centers' "gang databases", a similar inaccuracy can arise from classifying people as "gang associates" in a database simply because they were seen with or wore similarly colored clothing as people previously identified as "gang members". The consequences of such misclassification can be severe, including increased sentences or deportation.[36] Yet as far as is publicly known, there is no meaningful oversight or audit of fusion-center activities or deletion of inaccurate or irrelevant information in fusion center databases. We therefore recommend that the federal government purge data held by fusion centers and that DHS cease proposing funding for fusion centers in its next budget request.

---

[30] Robert O'Harrow Jr., "DHS 'fusion centers' portrayed as pools of ineptitude and civil liberties intrusions", *The Washington Post*, October 2, 2012, https://www.washingtonpost.com/investigations/dhs-fusion-centers-portrayed-as-pools-of-ineptitude-and-civil-liberties-intrusions/2012/10/02/10014440-0cb1-11e2-bd1a-b868e65d57eb_story.html.

[31] R. Jeffrey Smith, "Senate Report Says National Intelligence Fusion Centers Have Been Useless", *Foreign Policy*, October 3, 2012, https://foreignpolicy.com/2012/10/03/senate-report-says-national-intelligence-fusion-centers-have-been-useless/.

[32] Mark Puente, "Commissioners and critics question LAPD's reports on suspected terrorist activity", *Los Angeles Times*, June 11, 2019. https://www.latimes.com/local/lanow/la-me-suspicious-activity-reports-lapd-20190612-story.html.

[33] Brendan McQuade, *Pacifying The Homeland: Intelligence Fusion and Mass Supervision*, University of California Press (2019).

[34] U.S. Department of Homeland Security, *2017 National Network of Fusion Centers Final Report* (October 2018).

[35] Neumann, N., Tucker, C. and Whitfield, T., "How Effective Is Third-Party Consumer Profiling and Audience Delivery?: Evidence from Field Studies", May 16, 2019. Forthcoming in *Marketing Science - Frontiers*. Available at https://ssrn.com/abstract=3203131 or http://dx.doi.org/10.2139/ssrn.3203131.

[36] Thomas Nolan, "The Trouble with So-Called "Gang Databases": No Refuge in the "Sanctuary", American Constitution Society, June 28, 2018, https://www.acslaw.org/expertforum/the-trouble-with-so-called-gang-databases-no-refuge-in-the-sanctuary/.

3.3 Protect against scalable software vulnerabilities

A "zero-day vulnerability" is "a flaw in software, hardware, or firmware that is unknown to the party or parties responsible for patching or otherwise fixing the flaw".[37] The NSA collects "zero-day vulnerabilities" in commercially available software, which it is supposed to disclose through the "Vulnerabilities Equities Process" (VEP). The VEP is tasked with taking into account the trade-offs between the value to law enforcement of exploiting the vulnerability and the value of protecting commercial users from the vulnerability.[38]

The most harmful software vulnerabilities are ones that can be easily exploited at scale. "Exploited at scale" means that an attacker can attack a million computers rather than a single computer with little extra cost. By contrast, the ability to scale use of a software vulnerability is less of an important consideration for law enforcement conducting surveillance on a specific target. There is hence generally more societal value to the disclosure of scalable software vulnerabilities than there is to their exploitation. An illustrative example is the EternalBlue vulnerability in Microsoft Windows, which the NSA identified five years prior to the reveal of the vulnerability in the Shadow Brokers breach. EternalBlue could be exploited by attackers at scale with little cost, who then automated ransom demands for restoring software systems. Patching the EternalBlue vulnerability prior to the Shadow Brokers breach would have prevented substantial economic damage. For the WannaCry iteration of the EternalBlue vulnerability developed by North Korea, damages were on the order of $10 billion worldwide.[39]

It is important to recognize that at least some cyberattacks carried out by nefarious foreign actors were enabled by the fact that U.S. intelligence agencies were actively exploiting software vulnerabilities themselves. As Kevin Bankston, director of New America's Open Technology Institute, has observed, "By stockpiling the vulnerability information and exploit components that made WannaCry possible, and then failing to adequately shield that information from theft, the intelligence community made America and the world's information systems more vulnerable."[40] Analysts at the Open Technology Institute have argued that the VEP process, in heavily weighting law-

[37] "zero-day (computer)", TechTarget, May 2019, https://searchsecurity.techtarget.com/definition/zero-day-vulnerability.
[38] The White House, "Vulnerabilities Equity Policy and Process for the United States Government", Annex B, November 15, 2017, https://www.whitehouse.gov/sites/whitehouse.gov/files/images/External%20-%20Unclassified%20VEP%20Charter%20FINAL.PDF.
[39] Andy Greenberg, "The Strange Journey of an NSA Zero-Day—Into Multiple Enemies' Hands", *WIRED*, May 7, 2019, https://www.wired.com/story/nsa-zero-day-symantec-buckeye-china/.
[40] Andy Greenberg, "Hold North Korea Accountable for WannaCry—And the NSA, Too", *WIRED*, December 19, 2017, https://www.wired.com/story/korea-accountable-wannacry-nsa-eternal-blue/.

enforcement interests when determining whether or not a given vulnerability should be disclosed, is inherently biased against consumer protection.[41]

The federal government should revise the VEP to include a presumption against withholding scalable software vulnerabilities. The executive branch should also work with Congressional leaders to pass statutory rules governing the VEP process. In the same spirit, the federal policymakers should be wary of legislation that requires "backdoors" for law enforcement to access encrypted electronic communications and metadata. Such legislation would require U.S. tech companies to weaken product security, thereby increasing user exposure to cyberattacks and undermining the competitiveness of U.S.-manufactured software in the international marketplace. Indeed, a recent Australian law requiring law-enforcement backdoors for Australian-produced software, has "had a material impact on the Australian market and the ability for Australian companies to compete globally."[42]

[41] Sharon Bradford Franklin and Andi Wilson Thompson, "Rules of the Road: The Need for Vulnerabilities Equities Legislation", The Lawfare Institute, November 22, 2017, https://www.lawfareblog.com/rules-road-need-vulnerabilities-equities-legislation.
[42] See quote from the Australian Department of Home Affairs in Rohan Pearce, "Government acknowledges Aussie business have taken hit from 'encryption' law", *Computer World,* July 5, 2019, https://www.computerworld.com.au/article/663711/government-acknowledges-aussie-business-taken-hit-from-encryption-law/.

About the authors

Alex Marthews is a US-UK dual citizen living in Massachusetts and a father of four. Since 2014, he has served as the National Chair of Restore The Fourth, a grassroots nonprofit advocacy group that opposes mass government surveillance. His published research includes articles on the chilling effects of surveillance, problems of identity on the blockchain, and antitrust and social media.

Catherine Tucker is the Sloan Distinguished Professor of Management and a Professor of Marketing at MIT Sloan. She is an expert in the economics of digital data and privacy.

About the Day One Project

The Day One Project is dedicated to democratizing the policymaking process by working with new and expert voices across the science and technology community, helping to develop actionable policies that can improve the lives of all Americans, and readying them for Day One of a future presidential term. For more about the Day One Project, visit dayoneproject.org.