REFORMING SURVEILLANCE AUTHORITIES

Congress should

- reform Section 702 of the FISA Amendment Act to close its "backdoor search" and "about search" loopholes;
- update the Electronic Communications Privacy Act to provide meaningful protection for stored communications and location data;
- protect the integrity of strong encryption technologies against proposals to create government backdoors; and
- develop a statutory framework regulating government hacking—in particular, the use and disclosure of software vulnerabilities.

The United States, perhaps uniquely among nations, owes its existence in no small part to its people's outrage against government invasions of privacy. The Founders' abhorrence of the general warrants and writs of assistance wielded by the British Crown left its mark on our Constitution in the form of the Fourth Amendment's guarantee that our persons, homes, and papers shall remain secure against unreasonable government searches. In our more recent history, the systematic abuse of surveillance authorities uncovered by the Church Committee of the 1970s provided a sobering reminder of how readily the powers we grant government to protect our democracy can be perverted to threaten it.

As we face a daunting array of novel 21st-century threats, from violent global terror groups to sophisticated cybercriminals, Americans routinely hear that we can purchase our safety only by giving up essential liberty, that our Founders' resistance to government intrusions is a luxury we can no longer afford in a dangerous world, and that our commitment to liberty and limited government is a weakness and a source of vulnerability. In the coming years, legislators will confront that Faustian bargain in myriad forms—but a Congress guided by reason rather than fear will consistently reject it.

Close Section 702's "Backdoor Search" and "About Search" Loopholes

In 2008, Congress amended the Foreign Intelligence Surveillance Act of 1978 (FISA), empowering the director of national intelligence and the attorney general to jointly authorize programmatic interception, at domestic communications facilities, of communications pertaining to foreign intelligence targets. Under Section 702 of that statute, the Foreign Intelligence Surveillance Court (or FISA court) approves only broad targeting and minimization procedures governing such collection, whereas the selection of specific targets and accounts to be collected is left to the discretion of National Security Agency (NSA) analysts.

Although only non-U.S. persons located abroad may be formally targeted under these general warrants, the massive scale of collection nevertheless ensures that enormous numbers of American communications are swept up by the NSA. In 2015, more than 94,000 foreign "persons"—potentially including corporate entities—were "targets" of Section 702 collection. A 2014 review by the Privacy and Civil Liberties Oversight Board (PCLOB) noted that, by 2011, the NSA was collecting more than 250 million internet communications annually under this authority alone; the review also noted that the current number was "significantly higher." Though collection must be conducted for some legitimate foreign intelligence purpose, there is no statutory requirement that the particular accounts identified for interception belong to a terrorist or other foreign agent.

The PCLOB's review of Section 702 indicates that, unlike the bulk telephony metadata program ended by the USA Freedom Act of 2015, such surveillance has yielded intelligence of significant value. Less clear is whether an essential component of Section 702's utility is the collection of communications of identifiably U.S. persons—not targeted in themselves but incidental to the collection of targeted communications. The Framers of the Constitution did not prohibit general warrants on the premise that they would never yield valuable information about criminal conduct; clearly they would. The relevant question is whether the marginal benefit of general searches, relative to what could be obtained with more traditional particularized warrants, is so enormous as to justify the ancillary invasion of the privacy rights of many thousands of Americans.

Over the longer term, then, Congress should authorize a thorough inquiry into whether the value of Section 702 collection would be materially diminished by requiring additional judicial approval for the collection of communications to or from accounts known or reasonably believed to pertain to U.S. persons, even when such collection is incidental to the warrantless targeting of foreign-

ers. The Fourth Amendment, after all, guarantees citizens a right to be secure against unreasonable *searches*, not unreasonable "targeting": the fact that general warrants do not explicitly target the persons they render subject to search has not traditionally been understood as a mitigating factor but rather as a key component of what makes them so onerous.

Ideally, then, collections under Section 702 would be limited—to the greatest extent feasible—to foreign–foreign communications. Thus, providers would have to segregate messages between foreign targets and users identifiably based in the United States before sending the foreign–foreign communications to the NSA. Such messages could be retained by providers in case subsequent scrutiny establishes probable cause for a warrant to obtain them. Providers themselves frequently retain quite accurate information about the geographical location of their users for their own business purposes. Thus, they should often be able to conduct such segregation without the need for additional government scrutiny of communications for the purpose of locating the participants in the conversation.

In the interim, Congress should, at minimum, close the two loopholes that raise the most significant constitutional and practical concerns about the overcollection and potential misuse of U.S. citizen communications: the "backdoor search" and "about search" loopholes. Though Section 702 authorizes only the targeting of foreign persons for intelligence purposes, the subsequent querying and use of the data collected (including, of course, the communications of American citizens) are less stringently restricted. Databases containing the fruits of the PRISM data-collection program—that is, Section 702 collection directly from and with the participation of major U.S. internet communications platforms—are made available to cleared analysts, at both the NSA and other intelligence agencies, and can be queried using U.S. person "identifiers." In 2015, intelligence agencies *other than the Federal Bureau of Investigation* retrieved raw communications content using such queries 4,672 times. The FBI is statutorily exempt from tracking or reporting the frequency with which it performs such queries but has acknowledged that it does so routinely. Thus, the true total number of "backdoor" queries is likely at least an order of magnitude higher.

Under current law, then, FBI agents—even those conducting preliminary investigations not predicated on any hard evidence of wrongdoing—may deliberately search for and obtain the private communications of U.S. persons in these vast data stores, even though a warrant based on probable cause would be required to obtain such communications directly. Perversely, the FBI is exempt from reporting to Congress or the public on the frequency of these backdoor searches precisely because they apparently occur so routinely that officials have indicated it would be infeasible even to attempt to quantify

them. This point is particularly disturbing in light of press reports that law enforcement agencies engage in a practice known as "parallel construction" to conceal from both courts and defendants the intelligence origins of electronic communications evidence introduced in criminal trials.

Congress should therefore act to ensure that broad powers justified by the exigencies of foreign intelligence cannot be surreptitiously used to circumvent the safeguards that properly govern criminal investigations. The FBI, like other agencies with access to Section 702 databases, should be required to design its computer systems to facilitate the automatic logging and classification of queries to those databases. That way, Congress and other oversight bodies can be adequately informed about how the information collected is being used. Analysts should be informed when intelligence databases contain results responsive to a query on a U.S. person identifier. However, if a judicial warrant founded on probable cause would be required to *directly* target a person or account, then law enforcement should be held to the same standard to access communications in Section 702 databases.

The second major loophole Congress should address is the use of "about searches," an element of the "upstream collection" the NSA conducts by filtering traffic flowing over the internet backbone. Until relatively recently, the general public believed—and the government even falsely represented to the Supreme Court—that Section 702 authorized the acquisition only of communications either sent to or originating from an account reasonably believed to belong to a foreign target. In fact, as we now know, the NSA engages in mass filtering of the *contents* of international internet communications, which it also uses as a basis for acquisition. Thus, for example, the NSA may acquire an email from an American citizen to any person abroad if the email merely *mentions* the email address or other electronic identifier of an intelligence target, even though neither the sender nor the recipient is designated as a target, and neither the sending nor receiving account has been tagged for collection. Though the FISA Amendments Act forbids the intentional acquisition of wholly domestic communications, the FISA court estimated in 2011 that, under the "upstream" procedures then in place, the NSA would likely acquire some 56,000 wholly domestic emails annually—a result of the technical difficulty of segregating the domestic from the international emails that might be received or transmitted by the same user during a single online session. Although the procedures at issue in that case were subsequently modified by order of the FISA court, the broader practice of "about" searching persists.

These searches raise especially acute constitutional concerns. The legality of warrantless Section 702 collection is predicated on the idea—never explicitly affirmed by the Supreme Court—that such collection falls within a "foreign intelligence exception" to the Fourth Amendment's presumptive requirement

that searches of the contents of Americans' communications be authorized by a particularized warrant founded on probable cause. Declassified FISA court opinions have articulated a two-pronged test defining the limits of this exception. Surveillance must be conducted "to obtain foreign intelligence for national security purposes" *and* must be "directed against foreign powers or agents of foreign powers reasonably believed to be located outside the United States."

According to the intelligence community's traditional understanding of these terms, the "target" of surveillance is the person or entity *from or about whom* information is sought (typically but not necessarily a party to the intercepted communication), whereas surveillance is "directed against" the communications facility that either originates or receives an intercepted message. Because Section 702 does not require that its foreign targets be agents of foreign powers, it is not clear that the exception covers the interception of communications between a U.S. person and foreign persons whose accounts are targeted for either upstream or PRISM collection. It does seem clear, however, that the exception cannot plausibly be stretched to accommodate searches directed at *neither* the sending nor receiving account and, indeed, conducted without regard to whether the sender or receiver is even an intelligence target, let alone a suspected foreign agent.

In addition to the constitutional concerns, Section 702 has created an international backlash, with potentially serious consequences for global digital commerce. In 2015, the Court of Justice of the European Union (EU) cited Section 702 in a ruling invalidating the "Safe Harbor" arrangement governing commercial transfer of personal data about EU citizens to U.S. firms. Despite subsequent efforts to negotiate a new agreement addressing European concerns, the risk of an adverse ruling in future cases remains high as long as Section 702 is perceived as effectively granting the government discretionary access to the private data of foreign persons held by American firms. More transparent and restrictive targeting rules limiting the applicability of Section 702 to suspected foreign agents would substantially mitigate this risk.

Congress should therefore amend Section 702 to ensure that collection pursuant to this authority, at a minimum, falls within the bounds of the warrant exception articulated by the FISA court and to clarify that the acquisition of content entering or leaving the United States is limited to communications whose sender or intended recipient is a valid intelligence target. In cases where the sender or recipient of a message, whether acquired via upstream or PRISM collection, *is* a Section 702 target but has not been affirmatively determined to be an agent of a foreign power, the NSA should be required to develop procedures designed to minimize, to the greatest practicable extent, the collection, retention, or dissemination of communications to or from identifiable U.S. person accounts.

Update the Electronic Communications Privacy Act to Provide Meaningful Protection for Stored Communications and Location Data

Although intelligence surveillance has received the lion's share of public attention in recent years, our increasing reliance on digital communications technologies means that ordinary law enforcement agencies, too, depend increasingly on electronic data gathering in the course of criminal investigations. Yet in contrast to intelligence authorities, which have been amended many times since 2001, they do so largely under the aegis of the increasingly outdated Electronic Communications Privacy Act (ECPA) of 1986.

The structure of ECPA may have made sense at the time of passage, but the law is now dramatically out of step with the realities of 21st-century communications practices. It makes unclear distinctions between "remote computing" and "electronic communications" services that are difficult for both government lawyers and technology companies to apply coherently to the vast array of online services Americans use. Inconsistent levels of protections may be applied to different types of electronic data—and even to the same communication at different times. Perhaps most egregiously, ECPA authorizes law enforcement agencies to obtain the contents of private emails without satisfying the requirements for a probable cause search warrant, depending on factors such as the amount of time a message has been in storage or even (according to one Justice Department interpretation) whether it has been read by the recipient. As a growing number of courts have already held, these provisions violate the Fourth Amendment.

Congress should amend ECPA to establish a uniform requirement, consistent with the Fourth Amendment, of a probable cause search warrant to obtain the contents of both private electronic communications and remotely stored personal data not available to the general public. Though major communications providers, backed by several appellate courts, have already insisted that they will produce user content only pursuant to a warrant, that requirement should be codified in statute to ensure clarity and consistency for both police and providers. (This would not, of course, affect the ability of government agencies to continue serving subpoenas directly to the owners of stored data, just as they would for data stored locally on a user's hard drive.)

The warrant requirement should also apply to at least some forms of communications metadata, which both privacy advocates and many law enforcement officials acknowledge is increasingly as sensitive and revealing as communications' content. Detailed internet transactional logs, for example, often effectively reveal a user's detailed reading habits, or vitiate the First Amendment right to speak anonymously online, as surely as any wiretap designed to capture the

contents of those data transactions. Yet ECPA adopts the mechanical assumption that all transactional data stored by a third party—even data never normally reviewed by any human observer—fall outside the protection of the Fourth Amendment and is subject to compulsory production under standards far less stringent than probable cause. Although some types of communications records, such as "basic subscriber information," should reasonably be available to law enforcement via subpoena or court order, judges should be afforded greater discretion to impose the higher Fourth Amendment standard of probable cause when investigators seek internet transactional data that are either functionally equivalent to communications content or otherwise implicate core privacy interests. The mere fact of third-party custodianship should not be the sole factor in determining whether government acquisition of such transactional data implicates citizens' reasonable expectations of privacy.

Geolocation data—whether obtained via prospective Global Positioning System (GPS) tracking of a subject or from such sources as cellular connection records—similarly enables increasingly precise monitoring of Americans' physical movements and patterns of activity, in both public and private spaces. In 2012, a unanimous Supreme Court held in *U.S. v. Jones* that the installation of a GPS tracking device on a vehicle—especially when used for protracted monitoring—constitutes a search subject to the requirements of the Fourth Amendment. Congress should recognize that the privacy interest invaded by location tracking does not depend on the details of the technical mechanism by which the tracking is accomplished and should establish a uniform warrant standard for electronic location surveillance.

Protect the Integrity of Strong Encryption Technology against Demands for Government Backdoors

As high-profile cyberattacks regularly demonstrate the vulnerability of Americans' most sensitive data to malicious actors—from domestic criminals to foreign governments—we increasingly (and often unwittingly) rely on the critical protection of strong data encryption. Indeed, the flourishing digital economy we all now take for granted is in significant measure a product of the government's decision in the late 1990s to ease export restrictions on strong encryption software.

Recently, however, some law enforcement officials have issued renewed calls—wisely rejected when they were first heard more than two decades ago—for legislation requiring communications services and technology manufacturers to design deliberately insecure products, with built-in backdoors enabling law enforcement to unlock encrypted data. Unbreakable encryption has long been available for traditional personal computers—refuting dire prophecies

that such software would quickly render criminal investigations all but impossible. Now, the increasing deployment of default encryption on mobile computing devices, and in digital communications platforms such as instant messaging services, has resurrected the idea that companies must be prohibited from selling Americans "too much" privacy or security.

Such demands are not only offensive in principle but would be futile and destructive in practice. The principled problem should be all too clear: a backdoor mandate effectively treats millions of law-abiding Americans as presumptive criminals who may be forced to store their own private data, not in a format of their own choosing but in one dictated by the government. Such a proposal applied to more traditional forms of communication—a mandate that Americans tape their verbal conversations for the convenience of police or ensure that their personal diaries are legible to government investigators—would be obviously abhorrent. It is no less offensive when our thoughts and conversations are mediated by digital bits rather than air or paper.

The practical pitfalls of backdoor mandates are nearly as obvious to technologists and security professionals. First, experts broadly agree that it is extremely difficult, if not impossible, to build a "backdoor" that opens for law enforcement officers without simultaneously rendering the technology less secure and more vulnerable to other attackers, including repressive foreign governments. Though secure mechanisms for "exceptional access" by law enforcement have been described in theory, the general consensus of security experts is that they are extremely unlikely to be securely implementable at scale across many thousands of providers in a rapidly changing software ecosystem requiring frequent updates and patches to adapt to newly discovered bugs, vulnerabilities, and threats.

Second, unbreakable encryption tools are already widely available. Sophisticated cybercriminals—those for whom such digital evidence is most likely to be critical to an investigation—will not rely on products with backdoors to protect their private data; instead, they can choose from an array of widely available, secure products regardless of any mandates the United States chooses to impose. Indeed, several recent surveys of the current technological landscape have found that a substantial majority of widely used encrypted messaging tools are produced either by foreign firms or via a globally distributed "open source" model of development untethered to any physical location.

Third, and in consequence of the previous point, such mandates would hobble American companies in the global technology marketplace, even as individual and corporate consumers alike are increasingly demanding robust assurances of data security. This concern is particularly acute in the cloud computing sector. Firms conducting sensitive corporate communications or storing valuable intellectual property will naturally want assurances that their

data will not be improperly accessed by the employees of any company entrusted with the data. The simplest way to provide that assurance is to leave the encryption keys for cloud-stored data in the hands of the end users, rendering the data unintelligible to either hackers or unscrupulous employees. A backdoor mandate would ensure that only non-U.S. companies could provide such assurances.

Fourth and finally, any effective mandate would impose design constraints on programmers and manufacturers far more drastic than most nontechnologists recognize, creating pressure to adopt more centralized (and so more easily monitored) communications protocols and to make device operating systems more opaque and resistant to modification by their own users and owners. Requiring developers to comply with government demands for unencrypted data would create an implicit bias in favor of centralized over peer-to-peer communications protocols (for which a secure backdoor is intrinsically more difficult to design) and in favor of closed and proprietary over open-source software development, regardless of which approach would be superior on the technical merits.

In short, Congress should recognize that any legislative attempt to deny Americans access to strong privacy technologies would be economically injurious, practically feckless, technologically uninformed, and morally offensive.

Develop a Statutory Framework Regulating Government Hacking

For both intelligence agencies and ordinary law enforcement, the ability to conduct effective investigations increasingly turns on the ability to access digital communications and other stored data—data that are often encrypted, beyond the easy physical research of investigators, or stored on computers whose geographic location is (at least initially) unknown to the government. As a result, these agencies have found it necessary to develop and deploy capabilities for surreptitious remote access to computer systems—or, more prosaically, government hacking capabilities. Yet to date, this process has not unfolded pursuant to any coherent legislative framework but via a patchwork of internal guidelines, interagency memorandums, rules committee hearings, and warrant applications to low-level judges with limited technical expertise. These forums are inappropriate for balancing the complex constitutional and policy questions raised by government hacking.

Perhaps the simplest step legislators can take toward providing the necessary framework for government hacking is to formalize and codify the Vulnerabilities Equities Process. This process is currently used by the intelligence community to determine when software vulnerabilities identified by intelligence

agencies should be disclosed to developers and when they should be retained for intelligence-gathering purposes. As White House cybersecurity coordinator Michael Daniel explained in a 2014 blog post, this process is appropriately biased toward disclosing software vulnerabilities to developers so that they can be patched. "Building up a huge stockpile of undisclosed vulnerabilities while leaving the Internet vulnerable and the American people unprotected," Daniel explained, "would not be in our national security interest."

There are, however, causes for concern with the status quo. Established in 2010, the interagency vulnerability review process appears to have fallen into disuse until being "reinvigorated" by the Obama administration in 2014. Moreover, no statute or executive order requires participation in the process, meaning it could easily be weakened or even abandoned entirely under future administrations. The process is also unnecessarily opaque, with few mechanisms for holding the Equities Review Board—the body within the NSA tasked with making disclosure determinations—accountable, either to overseers or to the general public. This lack of accountability unnecessarily undermines confidence in the soundness of the process—and may make firms and security researchers wary of collaborating closely with the government.

Congress should formally establish an independent Equities Review Board comprising both members of the intelligence community and cleared representatives of the technology sector and require that vulnerabilities discovered by government agencies be promptly submitted to the vulnerabilities review process. Whereas particular disclosure determinations will properly remain classified, the general principles and guidelines used to arrive at those determinations should be public. In general, the presumption should be that any vulnerability in software used by the private sector or general public must be disclosed eventually—and in most cases immediately. In the rare cases when the balance of considerations favors delaying disclosure of a vulnerability so that it can be retained for intelligence or law enforcement use, that determination should be reviewed at regular intervals, with disclosure as the default in the absence of a continuing compelling interest in retaining it. Statistical information about the average delay between discovery and disclosure of a vulnerability should be made publicly available, and a sampling of specific determinations should be subject to review by the appropriate inspectors general.

Of more direct relevance to hacking by law enforcement, Congress should act to supplant a recent amendment to Federal Rule of Criminal Procedure 41 permitting broad extrajurisdictional warrants for digital searches. Under the revised Rule 41, law enforcement agencies may apply for warrants to remotely search computers outside the jurisdiction in which the warrant is issued when the location of the target computers "has been concealed through technological means" or when more than five target computers "have been

damaged without authorization and are located in five or more districts." The latter provision is generally understood as authorizing the issuance of broad warrants to compromise and identify computer systems that have been infected by criminal "botnets."

These amendments raise serious concerns about both extraterritoriality and Fourth Amendment particularity. When search warrants are issued for computers that cannot be reliably located in the physical world, it is all but certain that some will prove to be outside the United States. In practice, then, the amendment authorizes the extraterritorial enforcement of U.S. search warrants, in likely violation of the law of the country in which the target computer is located. International agreements, not the determinations of magistrate judges, provide the appropriate process for regulating such potential cross-border searches.

In addition, the FBI has already obtained court approval in at least some cases for "watering hole" searches, in which large numbers of computers accessing government-operated sites and purporting to offer illicit content are remotely compromised, raising novel questions about the appropriate standard of particularity for authorizing such searches. In the case of government hacking to identify botnet victims, this lack of particularity is all but guaranteed—with the added difficulty that the targets are the purported victims, rather than perpetrators, of a crime. And in both cases, the enormous variety of computer systems and software configurations that would be targeted by any large-scale government exploitation make it difficult to ensure that a government-installed exploit would not damage the targeted systems or otherwise interfere with their normal operations.

At a minimum, Congress should restrict the use of hacking tools against either targets of unknown location or botnet victims to the purpose of identifying the computer systems in question, in cases where no less intrusive means of identification are available. This restriction would allow investigators to seek an appropriately particularized warrant in the former case and to notify the victims in the latter case. It would also minimize the danger of unanticipated side effects on the targeted machines and reduce the risk of hacking warrants being used to facilitate fishing expeditions for evidence of criminal conduct unrelated to the initial purpose of the warrant.

Suggested Readings

Abelson, Harold, Ross Anderson, Steven M. Bellovin, Josh Benaloh, Matt Blaze, Whitfield Diffie, John Gilmore, et al. "Keys under Doormats: Mandating Insecurity by Requiring Government Access to All Data and Communications." Massachusetts Institute of Technology, Computer Science and Artificial Intelligence Laboratory Technical Report no. MIT-CSAIL-TR-2015-026, July 6, 2015.

Donohue, Laura. "Section 702 and the Collection of International Telephone and Internet Content." *Harvard Journal of Law and Public Policy* 38, no. 1 (2015): 117–265.

President's Review Group on Intelligence and Communications Technologies. Liberty and Security in a Changing World. White House Report and Recommendations, December 12, 2013.

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.

Sanchez, Julian. "Leashing the Surveillance State: How to Reform Patriot Act Surveillance Authorities." Cato Institute Policy Analysis no. 675, May 16, 2011.

———. "Reforming the Surveillance Process: Tweak or Overhaul." *Just Security* (blog), June 30, 2021.

———. "Smartphone 'Backdoors' and Open Computing." *Just Security* (blog), October 6, 2014.

———. Testimony on "Continued Oversight of U.S. Government Surveillance Authorities" before the Senate Committee on the Judiciary, December 11, 2013.

Schwartz, Ari, and Rob Knake. "Government's Role in Vulnerability Disclosure: Creating a Permanent and Accountable Vulnerability Equities Process." Harvard Kennedy School, Belfer Center for Science and International Affairs discussion paper, June 2016.

Wilson, Andi, Ross Schulman, Kevin Bankston, and Trey Herr. *Bugs in the System: A Primer on the Software Vulnerability Ecosystem and Its Policy Implications*. Washington: New America Foundation, July 2016.

—Prepared by Julian Sanchez