DECEMBER 2016

PAPERS FOR THE NEXT PRESIDENT

SURVEILLANCE POLICY

A Pragmatic Agenda for 2017 and Beyond

Adam Klein, Michèle Flournoy, and Richard Fontaine

Center for a New American Security

About the Authors

ADAM KLEIN is a Senior Fellow at the Center for a New American Security (CNAS). His research centers on the intersection of national security policy and law, including government surveillance in the digital age, counterterrorism, and rules governing the use of military force. Before coming to CNAS, Klein served as a law clerk to Justice Antonin Scalia of the U.S. Supreme Court and Judge Brett M. Kavanaugh of the U.S. Court of Appeals for the D.C. Circuit and was a Senior Associate at WilmerHale, an international law firm. Klein has also worked on national security policy at the RAND Corporation and the 9/11 Public Discourse Project, the nonprofit successor to the 9/11 Commission. He began his career as a legislative assistant in the office of U.S. Rep. C.W. "Bill" Young. His work on this project was supported in substantial part by a Council on Foreign Relations International Affairs Fellowship.

MICHÈLE FLOURNOY is Co-Founder and Chief Executive Officer of the Center for a New American Security. She served as Under Secretary of Defense for Policy from February 2009 to February 2012. She was the principal advisor to the Secretary of Defense in the formulation of national security and defense policy, oversight of military plans and operations, and in National Security Council deliberations. She led the development of the Department of Defense's (DoD's) 2012 Strategic Guidance and represented the department in dozens of foreign engagements, in the media, and before Congress. Prior to confirmation, Flournoy co-led Barack Obama's transition team at DoD.

RICHARD FONTAINE is President of the Center for a New American Security. He served as a Senior Advisor and Senior Fellow at CNAS from 2009–2012 and previously as foreign policy advisor to Sen. John McCain for more than five years. Fontaine has also worked at the State Department, the National Security Council, and on the staff of the Senate Foreign Relations Committee. Fontaine served as foreign policy advisor to the McCain 2008 presidential campaign and, after the election, as the minority deputy staff director on the Senate Armed Services Committee. Prior to this, he served as Associate Director for Near Eastern Affairs at the National Security Council from 2003–04. He also worked in the NSC's Asian Affairs directorate, where he covered Southeast Asian issues.

Cover Photo
Matthew Henry/Unsplash

Acknowledgments

The authors are grateful to the dozens of experts from the technology, national security, and privacy communities who offered their expertise and insights to inform this work. The authors would also like to thank Loren DeJonge Schulman and Neal Urwitz for their insightful comments on our draft and Maura McCarthy and Melody Cook for, respectively, their editorial guidance and graphic design.

Readers should note that some project participants were affiliated with organizations that support CNAS financially. CNAS maintains a broad and diverse group of more than 100 funders, including private foundations, government agencies, corporations, and private individuals, and retains sole editorial control over its ideas, projects, and publications. A complete list of our financial supporters can be found at www.cnas.org/support-cnas/cnas-supporters.

The authors are solely responsible for the analysis and recommendations in this report.

About the Series

The Papers for the Next President series is designed to assist the next president and his or her team in crafting a strong, pragmatic, and principled national security agenda. The series explores the most critical regions and topics that the next president will need to address early in his or her tenure and will include actionable recommendations designed to be implemented during the first few months of 2017.

SURVEILLANCE POLICY

A Pragmatic Agenda for 2017 and Beyond

Executive Summary

Today, the United States faces a more diverse, more complex array of national security threats than ever before. With ever more human activity taking place on electronic networks, surveillance is an essential tool for protecting the nation from these threats. The American people are fortunate to have a world-leading intelligence community, with a mission-oriented workforce operating under a robust legal and oversight regime. At the same time, the intelligence community's immense capabilities and necessary secrecy raise inevitable and important questions for individual privacy, the rule of law, and public accountability.

In late 2014, the Center for a New American Security began a two-year initiative aimed at developing a new approach to surveillance policy for the next administration. As part of this project, CNAS has held 14 expert workshops and roundtables and conducted more than 80 private conversations and interviews with leaders in the national security, privacy, and technology communities. These experts' participation was invaluable in informing this report; the views expressed here, however, are our own.

While the leaks by former National Security Agency contractor Edward Snowden violated the law and harmed ongoing intelligence-gathering efforts, they also represented a watershed moment in the debate over government surveillance in the digital age. The leaks revealed that the scale of government data collection – even lawful, court-approved data collection – was orders of magnitude greater than most Americans had believed. And the leaks created the impression around the world (fostered in some cases by imprecise media reports) that the United States was indiscriminately collecting the personal data of ordinary people.

Three years after the leaks, their effects continue to reverberate across the policy landscape. The post-Snowden backlash has impeded law enforcement and intelligence gathering, harmed the U.S. technology industry's competitiveness in international markets, and created diplomatic friction with important allies. Most importantly, many Americans remain skeptical that their government respects their digital privacy.

Since 2013, the executive branch and Congress have attempted to repair the damage by making important reforms to surveillance practices and legal authorities. These include:

- President Obama's Review Group on Intelligence and Communications Technologies, many of whose recommendations have become law or policy, and whose balanced, thoughtful report remains an important touchstone for surveillance policy.
- Presidential Policy Directive 28 (PPD-28), which, most notably, required U.S. signals-intelligence (SIGINT) practices to consider the privacy interests of non-Americans overseas – a commitment still unequaled by any other country.
- The USA Freedom Act, which ended the NSA's bulk collection of Americans' telephone call records and adopted a number of important, but underappreciated, measures to enhance transparency in government surveillance.
- The intelligence community's unprecedented efforts to explain its work, and the robust legal and compliance regime under which it operates, directly to the American people.
- The emergence of the Privacy and Civil Liberties Oversight Board (PCLOB) as a visible, energetic, public-facing, and credible independent evaluator of key surveillance programs.

While these changes are a strong beginning, they cannot be the end, for several reasons. They are not widely known overseas; indeed, given the technical and bureaucratic nature of many of the changes, they are unknown even to most Americans. The post-Snowden focus on collection of Americans' personal data, while understandable, overshadowed other important issues, such as outreach to foreign publics and the challenges facing the U.S. technology sector. Finally, these successes are fragile. New leaks could rekindle latent skepticism and mistrust. Some changes, such as PPD-28 and the intelligence community's transparency efforts, could be rolled back by a new president or altered by new legislation.

For these reasons, surveillance reform should be seen as a work in progress rather than a finished product. The agenda we propose would take the next step toward rebuilding trust with the American people, the technology industry, and partners and publics abroad. It would enable the new administration to speak with one voice in support of a pragmatic, privacy-enhancing agenda. It would make clear to foreign populations that their countries and the United States share basic values on data privacy and surveillance. It would safeguard the United States' enviable position as the world leader in information technology. It would help inoculate the new administration against the risk of future unauthorized disclosures. And it would further these goals while preserving needed national security capabilities.

Six Principles for Pragmatic Surveillance Policy

Six basic premises underlie our pragmatic approach to surveillance policy:

1. The next president and Congress should take meaningful steps both to enhance Americans' digital privacy and to reassure the American people that government surveillance is consistent with American values and the rule of law. Protection from unwarranted government intrusion into personal privacy is a bedrock element of American liberty. But greater transparency about surveillance practices is also needed to shore up public faith in government institutions. When the public learns that government surveillance practices dramatically outstrip what laws and the statements of government officials would lead a reasonable observer to believe, it erodes faith in governing institutions, with corrosive and dangerous long-term effects for U.S. democracy.
2. A thriving, world-leading American technology industry is in the United States' economic interest. It also benefits U.S. intelligence and counterterrorism efforts. Millions of American jobs rely on the information-technology industry, and tech is a vital and growing export sector. But the benefits of technological pre-eminence are not economic alone: U.S. law enforcement, counterterrorism, and intelligence efforts also benefit from the fact that much of the world's data is stored on U.S. soil and much of the world's internet traffic passes through the United States. Unfortunately, in the wake of the Snowden revelations, other governments have begun taking regulatory steps to align the storage and transfer of their citizens' data with physical borders. Below, we recommend various steps to help slow or reverse this trend.
3. Signals-intelligence collection and analysis are vital national security tools. The United States will and should continue to maintain world-leading SIGINT capabilities. Dramatically curtailing the government's electronic surveillance capabilities is neither prudent from a national security perspective nor politically realistic. No president could responsibly surrender vital, lawful national security capabilities at a time of serious threat to the nation.
4. Improving public and foreign trust on surveillance and digital-privacy issues is an important goal, but no reform agenda can dispel completely the aftereffects of the Snowden leaks. The heightened skepticism and expectation of transparency that the Snowden leaks created will not simply disappear. Rather, they are features of the new landscape, and policymakers and the intelligence community will have to acknowledge and adapt to them.
5. The oft-employed metaphor of "balance" between civil liberties and security is a poor guide for optimizing surveillance policy. In a time of diverse national security threats, Americans will demand robust counterterrorism, law enforcement, and intelligence capabilities to secure the homeland. They will also insist on safeguards for personal privacy and fidelity to the rule of law. The answer is not to choose between security or liberty but to work toward both. A focus on zero-sum tradeoffs between privacy and security deters security officials from embracing a privacy-enhancing reform agenda and assumes incorrectly that surrendering some amount of one value automatically yields a concomitant benefit for the other.
6. Signals intelligence and the powers of the NSA are not neatly severable from other issues affecting domestic and international data privacy. In practice, issues that experts would consider only loosely related to signals intelligence – such as debates over iPhone encryption and whether the government needs a warrant to read Americans' email – powerfully influence Americans' willingness to entrust the government with collecting, monitoring, and analyzing communications and user data. A pragmatic surveillance-policy agenda must not artificially exclude other data-privacy issues that are highly salient to the public and where constructive reform is possible.

The Case for Pragmatic Surveillance Reform

The next administration has an opportunity to refresh the narrative surrounding the U.S. government's approach to surveillance and digital privacy – if it acts proactively. But this opportunity is perishable. As the new president's term unfolds, other controversies and crises will inevitably arise, making it far harder for the administration to dictate the policy agenda. And reforms undertaken reactively after a crisis tend to garner less public goodwill than those enacted before a crisis occurs.

Some might argue in favor of a bold, controversial surveillance-policy agenda – whether reformist (such as allowing the FISA Amendments Act to sunset) or security-driven (such as pushing aggressively for decryption legislation). Yet either course would be both impracticable and inadvisable for a new administration. The new president's first actions, if divisive, will consume the president's political capital and harden political opposition. In addition, the public will hold the new administration responsible for any terrorist attacks that occur on its watch. By contrast, the agenda we outline below would expand the new president's political capital, earn public support and bipartisan credibility, and to some extent inoculate the president against a backlash should there be future unauthorized disclosures.

A new administration would be best served by announcing the measures recommended in this report as a unitary reform agenda rather than simply farming them out to various parts of the government for quiet implementation. The reforms will be more effective as a restorative tonic for past breaches of trust if they are widely known. And a major initiative, publicly promoted by the White House, will more effectively define the new administration in the public mind as serious about Americans' digital privacy than a series of atomized technical changes quietly implemented by the bureaucracy.

By doing so, the next president can seize the near-term – and possibly unique –opportunity to repair the various deficits in trust that have emerged in the wake of the NSA disclosures. In so doing, the government can ensure respect for critical civil liberties, protect national security, and bolster the strength of the American economy. The window for action will not remain open indefinitely; the time to act is now.

The National Security Agency's headquarters at Fort George G. Meade, in Maryland. (NSA)

Recommendations

A. STRENGTHENING PUBLIC TRUST

Email Privacy and Government Access to Other Personal Data

1. If the Email Privacy Act does not pass during the 114th Congress, the next president should, in the first 100 days of the new administration, call for legislation (i) requiring a warrant to obtain the content of email and documents stored in the cloud and (ii) imposing reasonable limits on nondisclosure orders.
2. The new administration should launch a White House initiative to propose standards for government access to other types of sensitive data, such as cell-site location data, data generated by "internet of things" devices, license-plate readers, facial recognition systems, and other foreseeable technologies with significant implications for personal privacy.

Intelligence Transparency and Secret Law

3. The NSA should expand its efforts to demystify the agency's work in the mind of the general public.
4. Senior leaders should not hesitate to defend the many valid purposes of signals intelligence beyond counterterrorism. Limiting the public defense of SIGINT to counterterrorism alone invites a backlash when uses other than counterterrorism are revealed.
5. The next president should publicly embrace the principle that all domestic surveillance and surveillance of Americans overseas will be based on clear statutory authority, publicly interpreted, with sufficient oversight to hold the government to its construction of the statute.
6. The president should task the general counsels of the Office of the Director of National Intelligence, NSA, FBI, and CIA, and the Assistant Attorney General for National Security, in consultation with the PCLOB, with proposing, within six months, other ways to reduce the amount of classified legal interpretation and programmatic guidance governing electronic surveillance. This could include, where consistent with national security, further declassification of relevant presidential directives, agency procedures, interagency memoranda of understanding, opinions of the Justice Department's Office of Legal Counsel, and classified annexes to legislation.
7. Even those documents in these categories that cannot be safely declassified and published should be shared, in a manner consistent with their classification and to the extent permitted by executive privilege, with the congressional intelligence committees.

Section 702

8. Section 702 should be reauthorized, but with reforms to enhance public confidence, transparency, and privacy.
9. The FBI should publicly explain with greater precision why it needs to search databases containing 702 information for data about U.S. persons.
10. The FBI should consider, and explain, whether it would be sufficient for it to continue to query databases containing 702 data for U.S.-person identifiers but, where such a search returns 702 information, to receive only the responsive metadata rather than the content.
11. Congress, as a condition of reauthorization, should mandate further transparency about several aspects of the 702 program:
    - » Require and enable NSA to fully implement Recommendation 9 from the PCLOB's report on Section 702.
    - » Estimate the overall scale of incidental collection, if a valid and practicable methodology can be found.
    - » Publish annually the number of instances in which an FBI query in an investigation unrelated to national security returns 702 information about a U.S. person.
    - » Estimate the total number of U.S.-person queries of databases containing 702 data conducted by the FBI in non-national-security criminal investigations.
    - » Provide more detail about which cybersecurity offenses the Department of Justice considers "serious crimes" for which it will use 702-derived information in a criminal proceeding.
    - » Publish the Justice Department's standard for determining whether evidence introduced in a criminal proceeding is "derived from" 702 information.
    - » Mandate the appointment of an amicus curiae in 702 certification proceedings.
    - » Provide to the public as much detail as possible about the national security value of Section 702.

The Privacy and Civil Liberties Oversight Board

12. The next president should swiftly appoint new members or reappoint existing members and work with the Senate to ensure that they are promptly confirmed.
13. Congress should pass legislation that permits the remaining members to collectively appoint staff in the absence of a chairman.
14. Congress should enact legislation exempting the Board from the Government in the Sunshine Act.
15. While is appropriate that the Board's activities focus on protecting the privacy rights of U.S. persons, Congress should not expressly restrict the Board's statutory jurisdiction to only the rights of U.S. persons.
16. Congress should not require the Board to keep the Director of National Intelligence or other elements of the intelligence community "fully and currently informed" of its activities.

Whistleblower Laws

17. The next president should issue an executive order making Presidential Policy Directive 19's whistleblower protections binding within the executive branch and clarifying that they extend to contractors working at all intelligence community components.
18. Congress should extend the full panoply of statutory whistleblower protections to contractors working in the intelligence community.
19. The next president should support legislation updating the FBI's whistleblower process in the next Congress.

B. PROTECTING A FLOURISHING TECHNOLOGY INDUSTRY

Encryption

20. Given the impasse over decryption legislation, and given that the debate itself has damaged relations between the government and the technology industry, the next administration should de-escalate the public debate over encryption.
21. The FBI should support its argument for an encryption mandate by publishing more data about the precise contours of the technical challenge posed by encryption.
22. To help the FBI cope with the status quo, Congress should scale up the FBI's resources for gaining access to encrypted devices and communications without compelled assistance from providers.
23. This scaling up should also include resources to enable the FBI to create a centralized repository of expertise and technical assistance for the 15,000 state and local law enforcement agencies in the United States.

Risk Management in SIGINT Decisions

24. Operations that, if exposed, would pose a significant risk to an American company or business sector should be approved by senior political appointees after a process that incorporates, to the greatest extent possible, external input about the scale of the risk.
25. The government should create regularized channels for candid communication between NSA and the technology industry, such as creating an industry advisory board of corporate officials who hold security clearances.
26. To the extent that a dialogue would, for some companies, raise concerns about appearing complicit in NSA practices, NSA should also establish a formalized one-way channel for receiving comment from American companies about the risks that signals-intelligence practices pose to their businesses and other issues of concern.
27. Where the U.S. government wishes to obtain data held by a U.S. company, it should generally seek to access the data through the "front door" provided by U.S. domestic law rather than through overseas intelligence operations or liaison relationships.
28. To the extent that the government contemplates operations that involve tampering with or introducing vulnerabilities into an American company's product before it reaches its end customer,[1] any such operations should be approved by the National Security Advisor with input, where appropriate, from the Deputy National Security Advisor for International Economic Affairs, or another senior official with analogous responsibilities.
29. The government should not, as a rule, pressure American technology companies to compromise their own products or hand over their source code.

30. The government should not pressure American companies that sell to the government to disclose to it vulnerabilities that the company discovers before the company discloses them to other customers.
31. The Vulnerabilities Equities Process should be formalized in an executive order.
32. The executive order should, to the maximum extent consistent with national security, list all agencies that have a say in the process and should specifically state which agencies have a vote on whether to retain or disclose a vulnerability.
33. In order to ensure that the process takes account of the broader interests of the U.S. technology sector, the Department of Commerce should have a regular seat at the table.
34. The executive order should also describe the process to be followed in deciding whether to retain or disclose a vulnerability. In particular, it should clearly state the government's substantive standard for deciding whether a vulnerability's potential national security benefits outweigh the risks of retaining it.
35. The executive order should also require that there be periodic review of whether a retained vulnerability should be disclosed.
36. The executive order should provide for public annual reports containing as much detail about the process's operation as is consistent with national security, along with a classified annex for the relevant congressional committees.

C. MITIGATING THE INTERNATIONAL CONSEQUENCES OF SURVEILLANCE POLICY

Surveillance Diplomacy and PPD-28

37. The next administration should offer to hold a political dialogue, among willing allies with similar rule-of-law cultures, on norms to govern surveillance of one another's citizens and institutions.
38. This dialogue should seek to exchange high-level, public, political (rather than legal) commitments analogous to the public commitments the United States has already made, most notably in PPD-28. For example, the United States should ask partners to mutually agree:
    - » To incorporate in their signals-intelligence practices protections for the privacy interests of one another's citizens.
    - » To publish, with the maximum detail consistent with national security, agency procedures implementing such protections, including minimization requirements limiting the dissemination and retention of personal information of one another's citizens.
    - » To establish a presumptive time limit for retaining the personal information of one another's citizens.
    - » To agree to limitations on the use of signals intelligence collected in bulk.
    - » To designate a senior official to serve as a point of contact for implementation of these commitments and other concerns related to signals-intelligence practices.
    - » To require individualized judicial approval for electronic surveillance of one another's citizens when on the other country's territory.
39. These discussions should also include mutual, public, high-level commitments about the purposes and boundaries of "liaison" cooperation between one another's intelligence services – in particular, the circumstances in which they will exchange information about one another's citizens.
40. In order to encourage allied governments to enter into such discussions and extend appropriate privacy protections to the American people, the United States should make clear to allied publics and their governments that while it is prepared to commit itself to protect their privacy, the American people's privacy deserves equivalent respect and it expects such protections to be reciprocated.
41. The next administration should reaffirm that PPD-28's basic recognition that signals-intelligence activities must consider the basic dignity and privacy of all people, and the fundamental commitments of Section 1 of PPD-28 (signals-intelligence activities must be be authorized by law; no use for discrimination or suppressing dissent; no espionage for commercial advantage of U.S. companies; narrow tailoring), will remain applicable to all countries and their citizens without regard to their own governments' policies.
42. The new administration should announce that after one year, the heightened commitments in PPD-28 Sections 2 and 4 will be guaranteed only to citizens of countries that agree to extend comparable protection to Americans. There is no reason why other countries, and particularly U.S. allies, should resist extending to Americans the same consideration that the U.S. government grants to their citizens.

43. The next administration should also offer to elevate these commitments to an executive order for countries that make credible reciprocal promises.
44. The United States should insist that European Union member states grant to Americans the same judicial-redress rights and access to a surveillance "ombudsperson" that the United States extended to Europeans under Privacy Shield.
45. The United States should demand that allied countries publicly commit not to spy on one another's nationals for the economic benefit of domestic companies – a practice the United States has long forsworn but some close allies have not.
46. The next administration should also make clear that it will consider excluding from any list of allied leaders whose personal communications are off-limits from surveillance the leaders of any country that refuses to publicly renounce such economic espionage against American companies.
47. The next administration and Congress should establish regularized, formal exchanges between congressional, judicial, and executive branch compliance and oversight bodies, including the Privacy and Civil Liberties Oversight Board, and their foreign counterparts.

Public Diplomacy

48. The United States should explain, in a modest and factual manner, the many ways in which the U.S. intelligence community supports Europe in its fight against terrorism.
49. The intelligence community should, with as much specificity as is consistent with national security, offer greater detail about how much and what kind of counterterrorism data the United States shares with European partners, as well as the types of information it receives from them.
50. The next administration should also consider raising the profile of joint counterterrorism efforts by making American ambassadors and senior national security officials available to discuss them with local media, and asking European counterparts to publicly acknowledge the cooperation.

Privacy Shield

51. While legal challenges are pending, U.S. officials should seek to foster a climate conducive to ensuring that Privacy Shield passes judicial muster.
52. This includes continuing to make the case that U.S. and European privacy protections are, at a minimum, "essentially equivalent."
53. U.S. officials should also seek to publicly reinforce the significance of the new ombudsperson mechanism and the Judicial Redress Act.
54. Consumer-protection officials should work to publicly demonstrate that Privacy Shield's consumer protections are being rigorously enforced.
55. American ambassadors in Europe and visiting U.S. government principals should be encouraged to highlight U.S. privacy protections and emphasize that in the United States, as in Europe, the right to privacy is a fundamental right.
56. The next administration should begin to consider what the United States' response will be, other than further concessions, if Privacy Shield is struck down.
57. It should also begin communicating quietly to European partners that while the United States respects their legal institutions, shares their values, and has taken every reasonable measure to help European partners satisfy the Court of Justice, the United States has a "Plan B" and will not respond to another flawed, *Schrems*-like decision with more unilateral concessions.
58. To amplify this message, Congress should consider legislation providing that if a judicial decision restricts data transfers from Europe to the United States, the same limitations will apply to data transfers from the United States to Europe by European companies.

Cross-Border Data Requests

59. If the Justice Department's proposal does not pass during the current Congress, the next administration should seek, and Congress should enact, similar legislation authorizing executive agreements on cross-border data requests.
60. Once the enabling legislation is enacted, the executive branch should move quickly to conclude executive agreements with countries with similar human-rights and rule-of-law standards.
61. Legislation creating an alternative to the Mutual Legal Assistance system should be accompanied by parallel efforts to streamline the existing system.

Introduction

In January 2014, President Obama delivered a landmark speech on signals intelligence at the Department of Justice. "Throughout American history," he noted, "intelligence has helped secure our country and our freedoms."[2] Today, intelligence community personnel work to protect the American people and U.S. allies from a range of threats – from terrorism to military aggression, from the theft of American trade secrets to the subversion of democratic institutions.

In the digital age, electronic surveillance is a necessary component of these efforts. Led by the National Security Agency (NSA), the intelligence community collects and analyzes signals intelligence subject to a system of "oversight, review, and checks-and-balances," which "reduce[s] the risk that elements of the Intelligence Community would operate outside of the law."[3] Yet even with these safeguards in place, these agencies' powerful capabilities and unavoidable secrecy pose serious challenges for individual privacy, public accountability, and democratic control.

The Snowden leaks broke the law and harmed ongoing intelligence operations, yet they produced a watershed moment in the public debate over government surveillance. Importantly, the leaked documents and the subsequent inquiry by the Review Group on Intelligence and Communications Technologies uncovered "no evidence of illegality or other abuse of authority [by the U.S. government] for the purpose of targeting domestic political activity."[4] At the same time, the leaks demonstrated that the scale of government data collection – even lawful, court-approved data collection – was much greater than most Americans would have believed given the available public information. They also created the impression around the world (fostered in some cases by inaccurate media reports) that the United States was indiscriminately collecting the personal data of ordinary people.

Three years after the Snowden disclosures, their effects continue to reverberate across the policy landscape and the U.S. technology industry. Many Americans remain skeptical of their own government's commitment to their digital privacy. Internationally, the widespread misperception that the NSA indiscriminately reads ordinary people's email and wiretaps their phone calls continues to harm American interests. This belief has triggered harmful policy responses abroad, endangering the cross-border data flows that are vital to the global business models of American technology companies. European consumers, companies, and governments continue to question the trustworthiness of American companies' products and services, undermining their competitive standing in foreign markets. The disclosures have damaged U.S. diplomatic ties, including with key allies. And they have undermined efforts by the U.S. government to promote global internet freedom and preserve the free flow of information online.

This status quo is harmful to U.S. diplomatic and economic interests overseas and corrodes faith in government institutions here at home. Despite the significant changes made to policy and messaging since the Snowden disclosures, the U.S. government has yet to adequately mitigate the negative fallout.

Fortunately, the authors believe that the next administration can materially improve upon the status quo on all three fronts – domestic, economic, and diplomatic – while preserving key national security capabilities. This report outlines *how* the next administration can do this and *why* doing so is both urgent and politically feasible.

Three years after the Snowden disclosures, their effects continue to reverberate across the policy landscape and the U.S. technology industry.

Beginning in late 2014, the Center for a New American Security (CNAS) began a two-year initiative aimed at developing a new approach to surveillance policy for the next administration. As part of this project, CNAS has held 14 expert workshops and roundtables and more than 80 private meetings and interviews with leaders in national security, privacy, and technology.

These consultations contributed directly to the analysis and recommendations we present below. They also persuaded us of six basic premises that underlie the pragmatic approach to surveillance policy that follows.

1. ***The next president and Congress should take meaningful steps to enhance Americans' digital privacy and reassure the public that government surveillance is consistent with American values and the rule of law.*** Protection from unwarranted government intrusion into personal privacy is a bedrock element of American liberty. That principle is given effect by the Constitution's Fourth Amendment, which protects the "right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures." The American legal order presupposes that privacy is inherently valuable.

Personal privacy, however, is not the only important value at stake; greater transparency and improved oversight of government surveillance are also needed to strengthen the public's trust in government institutions.[5] Or, as the post-Snowden Review Group on Intelligence and Communications Technologies put it, surveillance policy should foster, not erode, "a general sense … that the nation's practices and decisions are worthy of trust."[6] When the public learns that government surveillance practices dramatically outstrip what public laws and the statements of government officials would lead a reasonable observer to believe, it erodes faith in governing institutions, with corrosive and dangerous long-term effects for democracy.

2. ***A thriving, world-leading American technology industry is in the United States' economic interest, but it also benefits U.S. intelligence and counterterrorism capabilities.*** Technology has always been a key determinant of national power. But as digitization becomes ubiquitous in both commerce and national security, predominance in information technology (IT) will increasingly define which countries are seen as the world's economic and political leaders. Millions of American jobs already rely on the information-technology industry, and tech is a vital and growing export sector. It is also an immense source of economic and cultural influence for the United States. Lest there be any doubt about this industry's importance to modern economies, many other countries and foreign cities are desperately imitating Silicon Valley in the hopes of igniting their own startup booms.[7]

Recent controversies, such as the dispute between the Justice Department and Apple over an encrypted iPhone, have overshadowed the many national security benefits of being home to the world's leading technology industry. The most obvious is economic strength, a fundamental determinant of national power. Less obvious, but equally significant, are the advantages for U.S. intelligence, law enforcement, and defense[8] that derive from having much of the world's data stored on U.S. soil and much of the world's internet traffic pass across the United States. One powerful illustration of how valuable this is: The PRISM program – under which the government can obtain an intelligence target's data, if stored in the United States, directly from providers – was apparently the signals-intelligence activity most frequently cited in NSA's reporting. That U.S. companies hold this data trove yields enormous benefits for the intelligence community and law enforcement, and thus for the security of the United States.

Unfortunately, in the wake of the Snowden revelations, other governments have begun taking regulatory steps to align the storage and transfer of their citizens' data with physical borders. This movement will only abate if the United States can persuade foreign governments and users that their data held by U.S. companies is protected by an adequate legal regime, and that this regime is comparable or superior to that in their home countries. Fortunately, the authors believe that the United States has a strong case that its legal architecture for government access to data is comparatively robust. That said, this report makes recommendations both for further strengthening this legal architecture and for encouraging, in a constructive way, a fair comparison between the United States' architecture for access to data and the relevant law and policy in other countries.

Another significant advantage of IT predominance for U.S. intelligence and counterterrorism is that the intelligence community can purchase the world's best information-technology products from trusted American providers. For example, the CIA paid Amazon Web Services (AWS), the market leader in cloud computing,[9] $600 million to build a cloud-computing infrastructure for the intelligence community.[10] The CIA's Chief Information Security Officer recently described the new system as "a godsend for folks trying to implement systems quickly and for us to secure workloads better."[11] AWS has also launched a classified software "marketplace" from which IC agencies can "evaluate and buy common software" for use in the cloud.[12] Cloud services could ultimately allow the IC to "bypass acquisition problems that have plagued government for decades," with $9.2 billion wasted on large-scale IT acquisitions in the last decade alone.[13]

The ability to purchase the products and services of world-leading, homegrown, trusted technology providers is an enormous advantage for the U.S. national security apparatus over the nation's competitors. But this advantage will only persist as long as companies are able to reconcile doing business with the intelligence community with their (far larger) private-sector customer

Protection from unwarranted government intrusion into personal privacy is a bedrock element of American liberty.

President Obama meets with U.S. intelligence community officials in the Cabinet Room of the White House, April 17, 2012. (Pete Souza/ Official White House Photo)

base. As Peter Swire, a member of the Review Group on Intelligence and Communications Technologies, noted earlier this year: "Post-Snowden, American-based information technology companies don't want to be seen as an arm of the U.S. intelligence community."[14] To take one small example of how this can affect the government's ability to acquire cutting-edge technology: In May, Twitter barred Dataminr, a startup that analyzes Twitter's entire real-time stream of public tweets to derive insights about unfolding events, from selling to the intelligence community.[15] Twitter was reportedly concerned about "seeming too close to American intelligence services."[16]

Of course, this tendency is only one competing factor in companies' decisionmaking and is often not decisive, as AWS's contract with the CIA shows. But if there are future Snowden-like revelations and near-peer competitors emerge to challenge U.S. technology companies, it could become significantly more damaging.

3. ***Signals-intelligence collection and analysis are vital national security tools. The United States will and should continue to maintain world-leading SIGINT capabilities.*** Some previous surveillance-reform efforts have recommended that the United States restore the balance between civil liberties and national security by dramatically curtailing the government's electronic surveillance capabilities – for example, by allowing Section 702 of the FISA Amendments Act to lapse or requiring judicial review of all surveillance activities conducted overseas under Executive Order 12333.

Whatever the merits of such an approach as a matter of abstract first principles, it is neither prudent from a national security perspective nor politically realistic. Senior intelligence community leaders reported earlier this year that the Islamic State (ISIS) is "likely" to attempt attacks in the United States in 2016 and that the United States faces the most diverse global threat environment in 50 years.[17] Recent attacks in Europe and the United States have shown that ISIS-directed and ISIS-inspired terrorists intend and are able to kill civilians in the West. Nor is terrorism the only relevant threat. Signals intelligence is also a vital tool for monitoring Iran's adherence to last year's nuclear accord, China's intentions and actions in the South China Sea, Russia's activities in Ukraine and apparent attempts to interfere in the presidential election, and the many other pressing geopolitical challenges facing the United States.

No president could responsibly surrender vital, lawful national security capabilities at a time of serious threat to the nation. But even if it were desirable as an abstract matter to substantially reduce government data collection and analysis, a mass-casualty terrorist attack on U.S. soil could trigger a public clamor for measures even more vigorous than those in use today, as well as a political backlash against the administration that had reduced its

counterterrorism capabilities in the face of an obvious threat. This report recommends reforms that the authors believe are both responsible and politically realistic given the diverse array of grave threats facing the U.S. homeland and American interests worldwide.

4. ***Improving public and foreign trust on surveillance and digital privacy is an important goal, but no reform agenda can dispel completely the aftereffects of the Snowden leaks.*** This report recommends many ways in which the next administration can improve public faith in the government's approach to digital privacy and can reduce or mitigate international skepticism of American surveillance practices. Yet these trust deficits cannot realistically be eliminated altogether; not even the most forward-leaning surveillance-reform agenda would restore pre-Snowden levels of public agnosticism about electronic surveillance practices. The heightened skepticism and expectation of transparency that the Snowden leaks created are not going away. Rather, they are features of the new landscape – features policymakers and the intelligence community will have to acknowledge and adapt to. This is not entirely a bad thing. Digital-age technologies would pose immense dangers if misused by the state, so heightened vigilance is appropriate.

This climate of persistent skepticism has important implications for policymakers and for the recommendations in this report. Going forward, surveillance policy will have to account not merely for national security needs but also respond to the public's demand for rigorous oversight and transparency – as well as the risk of "involuntary transparency" wrought by disgruntled employees or cyber-penetrations from abroad. This means that surveillance decisions will have to account for the risk of future disclosures. This report recommends several ways in which existing policies and practices can be adjusted to account for these features of the post-Snowden world.[18]

5. ***The metaphor of finding a "balance" between civil liberties and security is a poor guide for optimizing surveillance policy.*** It is artificially limiting to see the universe of policy options as a set of zero-sum choices between these two essential values. A zero-sum framework is a poor guide for intelligent policymaking in this area, for several reasons.

Most fundamentally, in a time of grave and diverse national security threats, Americans will demand robust, effective counterterrorism, law enforcement, and intelligence agencies to secure the homeland from external threats. To be sure, policymakers should seek to foster resiliency and avoid overreaction when attacks occur. But while greater resiliency can reduce the risk of overcorrection, the natural human impulse to seek safety in perilous times will persist. If the United States is to safeguard personal privacy and the rule of law – and it must – that means reconciling a strong and capable national security apparatus with the fundamental liberties that define the American way of life.[19]

Second, the notion that by surrendering a certain amount of security capability one automatically receives a concomitant benefit for civil liberties and public trust is incorrect. Put simply, reducing one of these values does not necessarily produce more of the other. Some surveillance authorities, for instance, are too esoteric to be particularly salient to most Americans. Others are not widely viewed as problematic from a privacy perspective. In either case, eliminating the program might inflict substantial harm to national security but produce relatively little public benefit. Conversely, reform opportunities exist that would strengthen digital privacy and public trust without materially degrading counterterrorism or other national security capabilities.[20]

If the United States is to safeguard personal privacy and the rule of law – and it must – that means reconciling a strong and capable national security apparatus with the fundamental liberties that define the American way of life.

Finally, a focus on zero-sum tradeoffs between privacy and security deters risk-averse policymakers from seeking out and embracing a privacy-enhancing reform agenda. Leaders whose primary mission is preventing terrorist attacks are understandably reluctant to take any measures that might undermine their ability to carry out that mission – especially given that there is little to no public tolerance for failure. If reform is cast as shifting a zero-sum "balance" between privacy and security, it is not hard to see why it might be unwelcome to those who, rightly or wrongly, see their primary mission as security.

6. ***Signals intelligence and the powers of the NSA are not neatly severable from other issues affecting domestic and international data privacy.*** This project began with a relatively tight focus on issues related to the intelligence community's signals-intelligence practices and the

The public does not draw a bright line between signals intelligence and other issues affecting data privacy, such as smartphone encryption. (Yuri Samoilov)

legal and institutional mechanisms for overseeing them. The authors quickly realized, however, that this was an artificial and ill-advised limitation. Complex issues like the details of Section 702 or the minimization procedures approved by the FISA Court, while important, are not well understood by the public. The debates over iPhone encryption and whether the government needs a warrant to read Americans' email, by contrast, are far more visible and comprehensible to average Americans. Over the course of a year-long series of conversations and interviews, it became clear that issues that experts would consider only loosely related to signals intelligence can directly influence Americans' willingness to entrust the government with powerful capabilities to collect, monitor, and analyze communications and user data. As one expert noted, the public does not draw a bright line between signals intelligence and other issues affecting data privacy.

This has two important implications for policymaking on surveillance and data-privacy issues. First, policymakers must account for how a decision they take in one area will reverberate in other areas. Second, a pragmatic agenda for surveillance policy should not artificially exclude other data-privacy issues that are highly salient to the public and where constructive reform is possible.

The next section describes several trust deficits opened by the Snowden revelations and the real-world problems they have created or exacerbated. Part III discusses the significant reforms already undertaken by the Obama administration and Congress since 2013. Finally, Part IV sets forth a pragmatic surveillance-reform agenda for the next administration.

Defining the Problem

Historically, the U.S. government's electronic surveillance capabilities were cloaked in deep secrecy. In late 2005, however, that cloak began to slip, when *The New York Times* revealed that the National Security Agency was monitoring, without judicial oversight, communications between Americans and overseas terrorism suspects.[21] That revelation generated substantial controversy, but it did not fundamentally alter the policy landscape. In fact, Congress subsequently granted the NSA statutory authority to continue monitoring these communications without individualized court orders.[22]

The Snowden revelations in 2013 changed everything. Domestically, the most jarring revelation was that the government had been using Section 215 of the USA PATRIOT Act to collect, in bulk, records of all telephone calls carried by major telecommunications carriers – including the call records of tens of millions (perhaps hundreds of millions) of ordinary Americans – even though the statute covered only records that were "relevant to an authorized investigation."[23] (The program did not collect or monitor the *content* of those calls – a distinction some in the media and public missed.)

Public Trust and Government Credibility

The use of Section 215 to collect call records in bulk, once revealed, created a major credibility gap surrounding electronic surveillance and the powers of the NSA. Not because the program was nefariously motivated or undertaken without authorization; it had been blessed by the Foreign Intelligence Surveillance Court (FISC), although that approval rested on a legal theory that was debatable at best and came in an *ex parte* proceeding without adversarial scrutiny.[24]

> ***The scale of government surveillance was revealed to be far greater than ordinary Americans understood – and far greater than they reasonably could have anticipated.***

The larger problem was that the scale of government surveillance was revealed to be far greater than ordinary Americans understood – and far greater than they reasonably could have anticipated based on the text of the relevant public law. The statutory phrase "relevant to a terrorism investigation" would not reasonably suggest to an average citizen that the government could simply collect *everything*. Indeed, the U.S. Court of Appeals for the Second Circuit held last year that the program's "expansive concept of 'relevance'" was "unprecedented and unwarranted."[25] In short, the biggest blow to public trust was that the scale of the collection was far beyond anything the public could have imagined.

The initial batch of Snowden documents also described an NSA program called PRISM, which allowed the government to domestically target the electronic communications of non-U.S. persons overseas. Some contemporaneous press reports suggested that the NSA had received unmediated access to the servers of Facebook, Google, Apple, Yahoo, and other providers. That proved incorrect, but the impression that leading American companies had provided such access to U.S. intelligence services was extremely damaging and difficult to correct. Taken together with the revelation of the Section 215 call-records program, the PRISM documents fueled widespread cynicism about the scope of government surveillance and the adequacy of democratic oversight and control.

The domestic outcry that erupted in 2013 has diminished over time, in no small part thanks to the many significant reforms and transparency measures, involving all three branches of government, that have been undertaken since the Snowden leaks. We discuss those changes below in Part III. Yet the Snowden disclosures and the resulting trust deficits continue to harm various important U.S. national interests.

Harms to Intelligence and Law Enforcement Capabilities

The Snowden leaks directly harmed ongoing intelligence efforts, including what Director of National Intelligence (DNI) James Clapper described as "the single most important source of force protection and warning for our people in Afghanistan."[26] Less obviously, but just as importantly, the post-Snowden backlash has also created significant new obstacles for law enforcement and the intelligence community. In the immediate aftermath of revelations suggesting that the U.S. government had compromised their products, technology companies were understandably outraged and feared a massive backlash from their domestic and international customers. Hardware manufacturers were burned when leaked documents suggested that the NSA had tampered with American-made products en route to their end

customers.[27] Internet companies were left backpedaling after an NSA slide deck describing PRISM was widely (but incorrectly) read to suggest that the agency had direct access to the companies' servers. Yahoo and Google were angered when media reports emerged that the NSA and Britain's Government Communications Headquarters (GCHQ) had cooperated in gaining surreptitious access to "the main communications links" connecting each company's international data centers.[28]

To reassure their customers, many industry leaders reacted to the initial Snowden disclosures by publicizing their intention not to voluntarily assist government surveillance, and indeed to resist where possible.[29] Many companies now refuse to give customer data to the government until presented with binding legal process, even where the law permits them to do so, except where immediate access is needed "to prevent death or serious physical harm."[30] This forces law enforcement to expend more time and resources to obtain needed information. One expert told us that the system was simply not designed to handle the volume of litigation that would be required if companies demanded that the government go to court for every request. Moreover, with respect to data stored overseas, Microsoft has now won a court ruling that the U.S. government must use the cumbersome mutual legal assistance (MLA) process to obtain the data rather than seeking it directly from the company.[31]

The post-Snowden backlash has created significant new obstacles for law enforcement and the intelligence community.

Another reaction was to begin deploying powerful encryption technologies and handing the only key to the customer. While companies' business models have precluded them from using encryption to deny the government access to *all* user data, the post-Snowden move toward encryption has gone far enough to create serious problems for law enforcement. Perhaps the most visible manifestation has been Apple's decision to introduce on iOS devices full-disk encryption keyed only to the user's password. This change meant that Apple could no longer extract user data directly from devices running iOS 8 or later.[32] This became the subject of a high-profile national debate in the wake of the San Bernardino shootings earlier this year. The encryption controversy is discussed in greater detail below.

Diplomatic Costs

The damage wrought by the Snowden disclosures was not limited to intelligence and counterterrorism programs; they also undermined American soft power, credibility, and global leadership. To take just one illustration, Obama's approval rating in Germany fell from 75 percent to 43 percent after Snowden documents revealed the NSA's surveillance of Chancellor Angela Merkel's personal cell phone.[33] Even in 2015, two years after the leaks, a YouGov poll found that Edward Snowden was more admired in Germany than President Obama.[34] Perhaps most troubling, from 2013 to 2014 the share of Germans calling for a more "independent" approach to the transatlantic relationship jumped from 40 percent to 57.3 percent.[35]

High-level government-to-government relationships have largely healed – to some degree out of necessity. Yet there remains what one expert called a "residual trauma" that permeates transatlantic ties on issues related to surveillance and data privacy. Another expert described German public opinion as having settled into a "malaise" in which Germans are very aware of the issue and remain dissatisfied, but feel there's little they can do. In a democratic system, such widely held concerns will inevitably influence policy.

Perhaps the most dramatic international effect of the Snowden revelations was the decision by the Court of Justice of the European Union in *Schrems v. Data Protection Commissioner,* which effectively invalidated the "Safe Harbor" agreement allowing companies to transfer their European users' data to the United States. That decision was prompted in part by concern that U.S. authorities might have "access on a generalised basis" to European customer data transferred to the United States by U.S. companies. That concern was unfounded; the PRISM program on which the court focused requires individualized targeting and does not permit bulk collection.[36] Yet the court nonetheless upended Safe Harbor, triggering a period of intense and costly uncertainty for American companies doing business in Europe.

The United States and European Union have now agreed to a successor to Safe Harbor, known as Privacy Shield, which is discussed in greater detail in Part IV.[37] It bears noting, however, that Privacy Shield's future is far from assured; privacy advocates recently filed a lawsuit contending that Privacy Shield suffers from the same legal flaws the Court of Justice discerned in Safe Harbor.[38] U.S. actions over the next several years have the potential to affect the outcome of that case, in helpful or unhelpful ways.

Germans demonstrate in Berlin against government surveillance. (Markus Winkler/Creative Commons)

Finally, the Snowden disclosures have affected the United States' global internet-freedom agenda. With ever more human activity "mediated through Internet-based technologies," free access to the internet and secure digital communications have "take[n] on an increasingly vital role in political, economic and social life."[39] Under the Bush and Obama administrations, the U.S. government has spent hundreds of millions of dollars to support free access to the internet and secure communications for users around the world, especially those living under authoritarian regimes.[40] The United States has also fought to preserve the multi-stakeholder approach to internet governance and resisted efforts, led by authoritarian regimes, to allow governments to exert greater control over the internet.[41]

High-level government-to-government relationships have largely healed – to some degree out of necessity. Yet there remains what one expert called a "residual trauma" that permeates transatlantic ties on issues related to surveillance and data privacy.

Unfortunately, the Snowden disclosures and the perception that the NSA is engaged in mass online surveillance have dented the United States' credibility as a defender of a free internet. They have also led various countries to enact or consider measures, including "data localization" laws, that if widely adopted would transform the internet from an interconnected global network to a Balkanized mosaic of separate national networks, each tightly controlled by its government.[42]

Effects on the U.S. Technology Sector

The PRISM releases were bad enough – but unfortunately for American technology companies, other damaging leaks were still to come. A Snowden document released in 2014 revealed that NSA had been "interdicting" shipments of U.S.-made computer hardware and implanting beacons that would report back to NSA once installed, raising concerns overseas about the security of U.S. technology products.

In response to the disclosures, various governments, from adversary nations like Russia to friendlier countries like Brazil, have implemented or explored data localization – requiring data about domestic users to be stored on domestic servers. The beneficiaries are local cloud-computing services, which otherwise would struggle to

compete with American market leaders; among the losers would be Silicon Valley startups that could not establish an online presence with global reach without first placing servers in local jurisdictions across the world. In short, public outrage over American surveillance gave some foreign governments political cover to pursue "data protectionism."

This backlash has cost American firms billions and provided "a boon for foreign companies."

This backlash has cost American firms billions and provided "a boon for foreign companies."[43] The blowback affected even non-IT deals; for example, Saab unexpectedly beat out Boeing for a $4.5 billion Brazilian military jet contract after Snowden documents revealed that the NSA had spied on Brazilian President Dilma Rousseff.[44] And the authors heard directly from allied government officials that their IT departments no longer had confidence in the integrity of U.S.-made products for their official systems and had even undertaken efforts to develop indigenous alternatives.

The Information Technology and Innovation Foundation (ITIF) estimated in 2015 that the cost of the Snowden revelations for U.S. tech companies would "far exceed" $35 billion.[45] As the ITIF report explained:

> When historians write about this period in U.S. history it could very well be that one of the themes will be how the United States lost its global technology leadership to other nations. And clearly one of the factors they would point to is the long-standing privileging of U.S. national security interests over U.S. industrial and commercial interests when it comes to U.S. foreign policy.[46]

Some have suggested that the damage to U.S. economic interests from the Snowden disclosures is overhyped or even illusory. While reasonable minds can differ on the precise dollar amount of the losses, this critique overlooks various less obvious ways, beyond lost sales, in which the revelations have affected U.S. companies' business prospects in Europe.

For example, while the *Wall Street Journal* recently reported that American companies continue to dominate the cloud-computing market in Europe, the paper also noted that they have been able to do so only by building "at least a dozen new data centers in Europe in recent years."[47] The additional cost of building new data centers rather than adding capacity at existing facilities in the United States is only one measure of the harm. Digitally enabled services – that is, services that can be delivered remotely over the internet – account for more than half of U.S. exports.[48] And with the rise of cloud computing and big-data analytics, the importance of open data flows will only increase. If the overseas clients of U.S. cloud-storage firms demand that data remain within national borders, U.S. companies will be unable to offer software and analytics services that require data to travel across borders for processing. But the costs are not merely economic; data localization would obstruct the deployment of analytics and smart systems that have the potential to enhance life around the globe.[49]

Data protectionism also poses a fundamental threat to the global business models of many American internet companies. Widespread adoption of data localization could stifle the growth of startups offering innovative, transnational services. Given that the United States is the world leader in such products and services and has the most innovative startup ecosystem, it would be the biggest victim from widespread data localization laws. Even absent data localization mandates, however, some foreign customers are asking U.S. technology companies to store their data within national boundaries.[50] This is technologically suboptimal, for several reasons. But if foreign customers request it, U.S. companies will have little choice but to meet that demand.[51]

Hardware manufacturers have also been harmed by increased suspicion of American technology products. In the post-Snowden era, even when large foreign customers do ultimately choose American products, those orders are routinely preceded by skeptical questions about ties to the NSA and are often coupled with demands for extreme and costly measures to secure the supply chain. In an era of widely distributed global supply chains and on-demand manufacturing, such demands impose significant additional costs on the companies. Finally, American providers have traditionally been able not merely to win orders but also to charge a premium for being the most trusted supplier. To the extent that the Snowden revelations have eroded that trust premium, the full extent of the damage may be hidden by U.S. companies' continued ability to win orders.

Finally, the fact that American technology firms have invested so much in responding to the Snowden revelations and in signaling their independence from the U.S. government is a strong proxy for their assessment of the potential costs of Snowden blowback for their business models. These are sophisticated, for-profit public companies with no incentive to add unnecessary overhead in the form of lawyers, privacy officers, government relations, and so forth. Companies have taken various labor-intensive, expensive steps to shore up trust in their products. These include expanding the use of encryption, adding "trust anchors" and "secure boot" technology to prevent hacking, and even shipping products to anonymized addresses to foil possible government interdiction.[52] Companies would not be expending huge amounts of money, engineering time, and other resources on these efforts unless they sincerely believed that the potential blowback would inflict even greater costs.

Data protectionism poses a fundamental threat to the global business models of many American internet companies.

Three years after the Snowden leaks, the climate of mistrust they created remains damaging. Public skepticism persists. American companies must overcome suspicion that their products and customer data are compromised by government surveillance. And the backlash continues to impede some law enforcement and intelligence activities.

That said, the status quo today is not as bad as it might have been; fortunately, much has already been done to reform U.S. surveillance practices and rebuild trust. The next part of this report reviews these significant post-Snowden reform efforts. Part IV then considers both where policymakers should press for further reforms and how to draw more attention to the important steps already taken.

Post-Snowden Responses and Reforms

This part describes the many reforms already enacted in response to the Snowden leaks. These steps, while by no means the end of the surveillance-reform journey, are a substantial and meaningful beginning.

In fact, more has already been done than is widely appreciated, particularly overseas. Congress and the executive branch have implemented most of the headline recommendations of the major post-Snowden reviews. And President Obama has made historic commitments with respect to the privacy interests of foreigners – commitments matched by no other country.

President's Review Group on Intelligence and Communications Technologies

In the wake of the Snowden disclosures, the president appointed a five-member "Review Group" to consider the issues raised by the leaks and to make recommendations for reform. The Review Group considered both specific programs (including Sections 215 and 702) and broader questions about how to set signals-intelligence priorities and manage and oversee collection. Its December 2013 final report included a wide array of recommendations: general principles for structuring surveillance policy, revisions to specific legal authorities, and significant institutional reforms.[53] The report remains an important touchstone that can still usefully inform the next administration's surveillance-policy decisions.

Many of the Review Group's major recommendations have already been implemented or may be implemented imminently. These include:

- *Telephone metadata*. The Review Group urged that telephone metadata no longer be held by the government, but rather be "held privately for the government to query when necessary for national security purposes."[54] The USA Freedom Act fulfilled this recommendation.
- *Transparency*. The Review Group recommended that the government be required to disclose data about surveillance requests; that private telecommunications providers be permitted to do so; and that Congress authorize "Public Interest Advocates" to represent the public interest before the Foreign Intelligence Surveillance Court.[55] The USA Freedom Act fulfilled these recommendations as well.
- *Principles to govern signals intelligence*. Presidential Policy Directive 28 (PPD-28) adopts as binding policy within the executive branch many of the broad principles endorsed by the Review Group to govern signals intelligence.
- *NSA and Cyber Command leadership*. The Review Group recommended that the head of the military's Cyber Command and the Director of the NSA "should not be a single official" and that civilians be eligible to serve as NSA director.[56] The Obama administration is reportedly considering a plan that would fulfill both of these recommendations.[57]

A number of meritorious and significant Review Group recommendations have yet to be implemented, however. Several of these are addressed in Part IV.

Presidential Policy Directive 28

A month after the Review Group presented its final report, President Obama issued PPD-28, "Signals Intelligence Activities," which "articulates principles to guide why, whether, when, and how the United States conducts signals intelligence activities for authorized foreign intelligence and counterintelligence purposes."[58]

Some of these principles are anodyne; for example, that signals-intelligence collection "shall be authorized by" and "undertaken in accordance with" law.[59] Others elevated existing policy to the level of a binding presidential directive: for example, that agencies may not collect "foreign private commercial information" in order "to afford a competitive advantage to U.S. companies and U.S. business sectors commercially."[60]

Others were more newsworthy, however, and arguably historic. These include:

- Signals-intelligence activities must incorporate safeguards for the personal information of "all individuals, *regardless of … nationality … or where that individual resides.*"[61] The NSA, FBI, and CIA have now published policies and procedures implementing the required safeguards, including minimization procedures limiting how such data can be retained and when it can be disseminated outside the agency.[62]
- Personal information of non-U.S. persons must be purged after five years absent a specific determination by the DNI that it should be retained.[63]
- Data collected in bulk – that is, without targeting based on a specific identifier or selection term – can be used only for specified purposes, including counterterrorism, counterintelligence, countering proliferation of weapons of mass destruction, cybersecurity, and transnational crime.[64]

- The State Department was required to designate, and did designate, a senior official "to serve as a point of contact for foreign governments who wish to raise concerns regarding signals intelligence activities conducted by the United States."[65]
- "[D]eterminations about whether and how to conduct signals intelligence activities" must be subject to a risk-benefit analysis.[66]

PPD-28's commitment to consider the privacy interests of foreign nationals is now being implemented by the intelligence community. Agencies must now "delete non-U.S. person information collected through SIGINT five years after collection unless" certain national-security-related exceptions apply.[67] This five-year limit, while less protective than some would like, outstrips any privacy protection European governments have offered to Americans. PPD-28 should be the starting point for a more robust dialogue with U.S. allies on the protections they are willing to offer one another's citizens in their intelligence practices.

USA Freedom Act

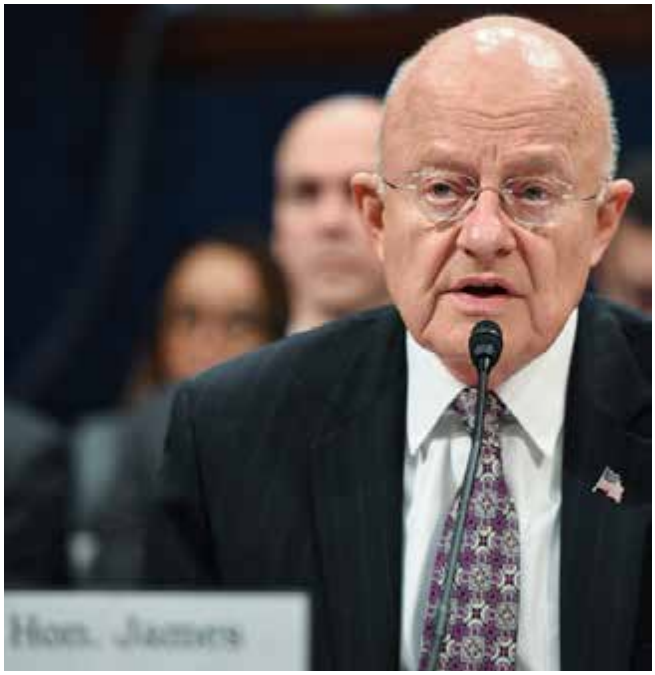
In June 2015, Congress passed and the president signed the USA Freedom Act,[68] which implemented various recommendations from the President's Review Group and the Privacy and Civil Liberties Oversight Board's report on the Section 215 call-records program.[69] The act's most significant reform was prohibiting the government from collecting in bulk telephone call records or other "tangible things" under Section 215. Instead, the new law permits the government to query, on an individualized basis, call records held by telecommunications providers. The government's application for call records must show a "reasonable, articulable suspicion that [a] *specific selection term is associated with … international terrorism*."[70] The government can seek records up to two degrees of separation, colloquially known as "hops," out from the original selection term.[71] The act also prohibited the use of national security letters for bulk collection.[72]

Less widely noted was that the USA Freedom Act contained several major transparency reforms, which are already having a notable and salutary effect. Specifically, the act:

- Permits the Foreign Intelligence Surveillance Court to call upon a select group of cleared advocates to represent the public interest in significant cases. These amici curiae can be appointed to offer "legal arguments that advance the protection of individual privacy and civil liberties" or to provide "information related to intelligence collection or communications technology."[73] The court has already used this provision; experienced national security lawyer Amy Jeffress was appointed last year, and raised several important legal arguments, in the FISC's annual review of the government's certifications for the Section 702 program.[74]
- Requires the DNI and the Attorney General to publish, to the greatest extent practicable, any FISC decision "that includes a significant construction or interpretation of any provision of law."[75]
- Requires the Director of National Intelligence to issue annual reports disclosing the total number of queries under Sections 215, 702, and other surveillance authorities.[76]
- Requires the Administrative Office of the U.S. Courts to issue annual reports disclosing similar data about proceedings before the Foreign Intelligence Surveillance Court.[77]
- Permits private companies to issue periodic reports disclosing, within numerical ranges, the number of surveillance orders of various types that they receive.[78] Since 2013, leading internet companies had battled the government for permission to provide their customers with meaningful disclosure about such requests.[79]

The USA Freedom Act's headline-grabbing changes to the Section 215 call-records program overshadowed this array of transparency and oversight reforms. Importantly, these changes do not materially reduce counterterrorism capability, yet they substantially bolster the public legitimacy and democratic accountability of the programs to which they apply. These reforms embody several important principles of intelligence transparency – principles that point the way for future surveillance-reform efforts.

First, and most fundamentally, domestic surveillance or surveillance of U.S. persons overseas should be based on clear statutory authority, publicly interpreted, with rigorous oversight to ensure that the government stays within the publicly understood confines of its legal authority.[80] This oversight role will often be performed by courts, but also includes close supervision by a fully informed Congress and by a vigorous Privacy and Civil Liberties Oversight Board within the executive branch. The judicial role here need not entail individualized review of every targeting decision; in the context of Section 702, regular programmatic review and supervision are appropriate given that the targets are non-U.S. persons living outside the United States.[81]



Director of National Intelligence James R. Clapper testifies before the House Permanent Select Committee on Intelligence. (Brian Murphy/Office of the Director of National Intelligence Public Affairs)

What is essential, however, is that the available public information permit a well-informed citizen to form a reasonably accurate understanding of the general contours of the government's surveillance powers, allowing meaningful democratic control of the scope of surveillance authority. The goal is to avoid the growth of a substantial discrepancy between what is actually happening and what the public believes to be allowed. As the 2013 leaks (like the Church Committee hearings of the 1970s) demonstrated, such discrepancies can lead to a crisis of public trust when the true scale of government activity is revealed. There are several additional ways to prevent such discrepancies from forming, which are discussed in detail later in this section.

Second, while secret facts are unavoidable in this context, the government should declassify, with as much granularity as is consistent with national security, data about the volume and purposes of surveillance activity. Fortunately, this is already happening to a significant degree – an immensely important and underappreciated change from the pre-2013 status quo. For example, the intelligence community's Statistical Transparency Report for 2015 reports that 94,368 individuals or organizations were targeted for collection under Section 702 in that year,[82] a slight increase from 2014.[83] By way of comparison, the government used "traditional" FISA to obtain domestic national security wiretaps for 1,695 targets in the United States in 2015.[84] Publishing this type of high-level data should not harm national security but can give the public a general sense of the overall scale of surveillance activity and the relative importance of various legal authorities.

Third, secret processes for making significant decisions about the scope and nature of government surveillance should be, if not strictly adversarial, at least designed to consider the interests of all stakeholders. The USA Freedom Act's provision for public-interest advocates is one important application of this principle. Part IV offers other ways to apply it, within both the FISC and other intra-governmental forums.

Privacy and Civil Liberties Oversight Board

The 9/11 Commission recommended that Congress create an independent "board within the executive branch to oversee … the commitment the government makes to defend our civil liberties."[85] Congress adopted that recommendation in the Intelligence Reform and Terrorism Prevention Act of 2004, creating the Privacy and Civil Liberties Oversight Board.[86]

Since 2013, the Board has emerged as a valuable and influential feature of the oversight landscape for counterterrorism and surveillance. Most notably, the Board has issued comprehensive and well-regarded reports on bulk call-records collection under Section 215 and on Section 702. The Board reports that it has received fulsome cooperation from the intelligence community, and its work has spurred the community to declassify many basic facts about the Section 702 program. This enhanced the public's understanding of how the program operates without compromising national security.

As previously noted, the USA Freedom Act implements many of the recommendations from the PCLOB's report on Section 215.[87] The intelligence community has also implemented, in whole or in part, all of the PCLOB's recommendations from its report on Section 702. Among the most notable recommendations were:

- Improving documentation of the foreign-intelligence purpose for individual targeting decisions under Section 702.[88]
- Implementing more rigorous constraints on searches for U.S.-person information incidentally collected under Section 702.
- Giving the Foreign Intelligence Surveillance Court more data on how the government is implementing the broad "authorizations" the court approves under Section 702.[89]

In short, the Board has been a valuable addition to the constellation of oversight entities. Its report on the Section 702 program in particular illustrates how a functioning, well-staffed Board can enhance, in a manner consistent with national security, the public understanding (and thus the democratic legitimacy) of important but controversial signals-intelligence programs. A vigorous Board also strengthens the United States' case to other countries that U.S. signals-intelligence activities operate within a robust oversight framework. For example, in a letter designed to address European concerns related to Privacy Shield, the General Counsel of the Office of the Director of National Intelligence (ODNI) cited the Board and its public reports as evidence of the "rigorous and multi-layered" oversight of U.S. intelligence.[90] Part IV makes several recommendations to ensure that the Board remains a viable and robust presence into the next presidential administration.

Intelligence Community Transparency Agenda

The intelligence community has also moved on its own to increase transparency and public outreach. Last year the Director of National Intelligence publicly committed the community to "appropriate transparency" about its mission and legal authorities, to better public communication and engagement, to "proactive" efforts to declassify and publish relevant information, and to ensuring that classification practices are not excessive or overzealous.[91]

To implement this agenda, ODNI has created "IC on the Record," a website providing "[d]irect access to factual information related to the lawful foreign surveillance activities of the U.S. Intelligence Community."[92] The site provides information about the intelligence budget, periodic transparency and disclosure reports, and many declassified documents related to intelligence programs. IC officials, and particularly NSA officials, have also made a concerted effort to engage publicly with relevant communities.

Diplomatic Efforts

Finally, the State Department has led diplomatic efforts to ameliorate the international repercussions of the 2013 disclosures. In the wake of the revelation that the NSA had been monitoring Chancellor Angela Merkel's cell phone, the United States and Germany initiated a series of meetings to discuss surveillance and rules of the road in cyberspace.[93] (President Obama also ended the monitoring of Chancellor Merkel's communications.[94]) While these meetings produced few concrete outcomes, they allowed for open dialogue between American and German officials at a time when such discussions were politically sensitive in Germany.

More broadly, Secretary of State John Kerry and other State Department officials have attempted to delineate a set of general norms that the United States believes should govern surveillance activities in democratic systems. Specifically, in April 2014, Secretary Kerry laid out four principles that the United States believes are "universally applicable" to surveillance in democratic systems:

1. "Rule of law – democracies must act according to clear, legal authorities, and their intelligence agencies must not exceed those authorities."
2. "Legitimate purpose – democracies should collect and share intelligence only for legitimate national security reasons and never to suppress or burden criticism or dissent."
3. "Oversight – judicial, legislative or other bodies such as independent inspectors general play a key role in ensuring that these activities fall within legal bounds."
4. "Transparency – the principles governing such activities need to be understood so that free people can debate them and play their part in shaping these choices."[95]

Below, we consider how to expand and strengthen these diplomatic efforts; in particular, how to ensure that they result in better global awareness of the reform initiatives the United States has undertaken since 2013 and how to encourage mutual commitments among like-minded nations.

President Barack Obama and German Chancellor Angela Merkel hold a joint news conference. (Chuck Kennedy/Official White House Photo)

As this recounting shows, since the Snowden revelations the U.S. government has undertaken significant reforms to its surveillance programs and oversight mechanisms. Yet while these changes are a strong beginning, they cannot be the end, for several reasons. They are not widely known overseas; indeed, given the technical and bureaucratic nature of many of the changes, they are unknown to most Americans. The focus on the Section 215 call-records program in the immediate post-Snowden period, while understandable, overshadowed other important issues, such as outreach to foreign publics and the challenges facing the U.S. technology sector. Finally, and perhaps most importantly, these successes are fragile. New leaks could rekindle latent skepticism and mistrust. Some changes, such as PPD-28 and the intelligence community's transparency efforts, could be rolled back by a new president. And future terrorist attacks could push public opinion dramatically toward security, as in the period immediately after the 9/11 attacks.

Surveillance reform should be seen as a work in progress rather than a finished product.

For these reasons, surveillance reform should be seen as a work in progress rather than a finished product. The agenda this report proposes would take the next step toward rebuilding trust with the American people, the technology industry, and partners abroad. It would enable the new administration to speak with one voice in support of a pragmatic, privacy-enhancing agenda. It would help persuade allied publics that their countries and the United States share basic values on data privacy and surveillance. It would safeguard the United States' enviable position as the world leader in information technology. And it would help inoculate the new administration against the risk of future unauthorized disclosures. Importantly, however, it would further these aims while preserving needed national security capabilities.

A Pragmatic Agenda for Surveillance Policy

Each new president enters office with a chance to reorient the national agenda and signal that the country is leaving behind the controversies of the previous administration. President Obama, for example, signed on his second day in office an executive order unambiguously banning torture and, less successfully, setting out a plan to close the detention facility at Guantanamo Bay.[96] These moves were intended to signal a clear break with certain controversial post-9/11 counterterrorism policies.

Unfortunately, the Snowden leaks placed the Obama administration in the unenviable position of serving as the face of controversial surveillance practices, even though these practices had spanned administrations. Administration officials have worked hard to dispel the legacy of those revelations, most notably by creating the President's Review Group and implementing many of its recommendations. Notwithstanding these positive steps, however, there was an unavoidable limit to the Obama administration's ability to shed the Snowden legacy, particularly with limited time remaining and many competing priorities.

A new administration will have an opportunity to refresh the narrative surrounding the U.S. government's approach to surveillance and digital privacy – if it acts proactively. But this opportunity is perishable for several reasons. As the new president's term unfolds, other controversies and crises will inevitably arise. Once the administration is forced into a reactive, crisis-management posture it becomes far harder for it to proactively set the policy agenda. Moreover, reforms undertaken in response to a crisis tend to garner less public goodwill than those enacted before a crisis occurs; the public assumes that such reforms, like a forced apology, are grudging and self-interested rather than driven by foresight and conviction. Another benefit of taking reform measures proactively is that if further damaging revelations from the Snowden leaks occur, the president will be a credible reform advocate rather than painted as having silently acquiesced in the disputed practices.

Some might argue that the next president should spend down some of the new administration's post-inaugural political capital to enact an aggressive, controversial surveillance-policy agenda – whether reformist (such as allowing the FISA Amendments Act to sunset) or security-driven (such as pushing for decryption legislation). The authors believe that either course would be impracticable and inadvisable for a new administration. While the inauguration typically produces some reservoir of goodwill for a new president, that resource is quickly exhausted. The new president's first actions will quickly shape public perceptions and, if divisive, consume the president's political capital and harden political opposition. In addition, the public will hold the new administration responsible for any terrorist attacks that occur on its watch.

To avoid this trap, the reform agenda outlined here generally eschews approaches that would require the new administration to simply choose one side of an entrenched dispute over the other. The virtue of this approach is that it is politically realistic and would not require the new administration to expend excessive amounts of political capital on this one issue. In fact, we believe that these recommendations would expand the new president's political capital, earn public support and bipartisan credibility, and to some extent inoculate the president against a backlash should there be future unauthorized disclosures.

Finally, a word on how a new administration should implement a program like that proposed here. Policy experts frequently and understandably treat the issues we discuss here as falling into several distinct spheres: Signals intelligence in one basket, law enforcement in another, diplomacy in a third. The public, however, does not perceive these issues as neatly severable. Snowden-type revelations about NSA signals-intelligence programs and FBI efforts to access encrypted smartphone data both shape the public's perception of whether the government is appropriately reconciling national security needs with digital privacy. Indeed, it is unwise for a new administration to treat these issues as severable, because many of the most significant opportunities to enhance Americans' digital privacy come in areas that do not directly affect counterterrorism capabilities.

For that reason, a new administration would be better served by publicly announcing these measures as part of a unitary reform agenda than by simply farming them out to various parts of the administration for quiet

A new administration will have an opportunity to refresh the narrative surrounding the U.S. government's approach to surveillance and digital privacy – if it acts proactively.

implementation. There are both public-spirited and instrumental reasons to do this. These measures will be more effective as a restorative tonic for past breaches of trust if they are widely known; indeed, one of the reasons that the far-reaching commitments of PPD-28 have not had a significant effect on overseas perceptions of U.S. surveillance practices is that most people simply are not aware of them. Announcing a broad reform agenda, in addition to being sound policy, is also good political practice: A major initiative, publicly promoted by the White House, will more effectively define the new administration in the public mind as caring about Americans' digital privacy than a series of atomized technical changes implemented by the bureaucracy and known only to experts.

Accordingly, these recommendations are organized not by implementing agency but by the particular trust deficit – with the American public, American companies, or foreign governments and publics – that each proposal is aimed at improving.

Strengthening Public Trust

The next president will have a brief window of opportunity in which to signal to the American people that the new administration takes their digital privacy seriously. The next administration will also be confronted with pressing challenges that, depending on how they are resolved, have the potential to muddle that message – in particular, the reauthorization of Section 702 and developments that "could plunge the [Privacy and Civil Liberties Oversight Board] back into obscurity."[97]

This report proposes a series of reforms to enhance Americans' digital privacy, boost transparency, and bolster the credibility of key oversight mechanisms – without compromising important national security authorities.

EMAIL PRIVACY AND GOVERNMENT ACCESS TO OTHER PERSONAL DATA

Many of the issues discussed in this paper are relatively esoteric. While important, they are of interest primarily to subject-matter experts and are not well understood by the general public. Section 702 is a prime example – how many Americans have heard of this statute, not to speak of understanding what it does? That is not to suggest that obscure or esoteric issues are unimportant. But it does mean they are less relevant to the public's overall perception of whether the government respects its digital privacy. And restoring that trust should be a key goal of any surveillance-reform agenda.

That does not mean that a reform agenda should exclude esoteric issues; we cover many here. But it does mean that a reform agenda should *include* those high-visibility, emotionally resonant topics that help shape public opinion on these issues.

One such topic is email privacy – that is, whether the government needs to obtain a warrant based on probable cause to view the content of a U.S. person's email. The Electronic Communications Privacy Act's rules for law enforcement to access the contents of electronic messages are byzantine. If the email is stored on your mobile device, the government almost always needs to get a search warrant before accessing its contents.[98] But if the email is stored in the cloud, whether or not the government needs a warrant to obtain a message depends on how long it has been in storage, whether it has been opened by the user, and what type of communications provider is hosting it.[99]

The historical roots of these distinctions are not relevant here.[100] For present purposes it is enough to note that they have been superseded by technological developments. They are also untethered to Americans' expectations of privacy when they use those platforms.[101] And there is a strong argument that search warrants are constitutionally required, whether because users have a "reasonable expectation of privacy" in the contents of their stored email[102] or because stored emails should be considered "papers" directly protected against unreasonable searches by the text of the Fourth Amendment.[103]

Legislation pending in Congress would replace the statute's anachronistic distinctions with a uniform, nationwide warrant requirement for law-enforcement access to email.[104] The bill, known as the Email Privacy Act, would also end the practice of imposing indefinite gag orders barring providers from notifying customers of government requests for their data. Instead, nondisclosure orders would be limited to 180 days, with the possibility of extensions where needed. To issue a new order or an extension, a judge would have to specifically find that a serious harm would result if the customer were notified.[105]

STRENGTHENING PUBLIC TRUST

Email Privacy and Government Access to Other Personal Data

- If the Email Privacy Act does not pass during the 114th Congress, the next president should, in the first 100 days of the new administration, call for legislation (i) requiring a warrant to obtain the content of email and documents stored in the cloud and (ii) imposing reasonable limits on nondisclosure orders.
- The new administration should launch a White House initiative to propose standards for government access to other types of sensitive data, such as cell-site location data, data generated by "internet of things" devices, license-plate readers, facial recognition systems, and other foreseeable technologies with significant implications for personal privacy.

Intelligence Transparency and Secret Law

- The NSA should expand its efforts to demystify the agency's work in the mind of the general public.
- Senior leaders should not hesitate to defend the many valid purposes of signals intelligence beyond counterterrorism. Limiting the public defense of SIGINT to counterterrorism alone invites a backlash when uses other than counterterrorism are revealed.
- The next president should publicly embrace the principle that all domestic surveillance and surveillance of Americans overseas will be based on clear statutory authority, publicly interpreted, with sufficient oversight to hold the government to its construction of the statute.
- The president should task the general counsels of the Office of the Director of National Intelligence, NSA, FBI, and CIA, and the Assistant Attorney General for National Security, in consultation with the PCLOB, with proposing, within six months, other ways to reduce the amount of classified legal interpretation and programmatic guidance governing electronic surveillance. This could include, where consistent with national security, further declassification of relevant presidential directives, agency procedures, interagency memoranda of understanding, opinions of the Justice Department's Office of Legal Counsel, and classified annexes to legislation.
- Even those documents in these categories that cannot be safely declassified and published should be shared, in a manner consistent with their classification and to the extent permitted by executive privilege, with the congressional intelligence committees.

Section 702

- Section 702 should be reauthorized, but with reforms to enhance public confidence, transparency, and privacy.
- The FBI should publicly explain with greater precision why it needs to search databases containing 702 information for data about U.S. persons.
- The FBI should consider, and explain, whether it would be sufficient for it to continue to query databases containing 702 data for U.S.-person identifiers but, where such a search returns 702 information, to receive only the responsive metadata rather than the content.
- Congress, as a condition of reauthorization, should mandate further transparency about several aspects of the 702 program.

The Privacy and Civil Liberties Oversight Board

- The next president should swiftly appoint new members or reappoint existing members and work with the Senate to ensure that they are promptly confirmed.
- Congress should pass legislation that permits the remaining members to collectively appoint staff in the absence of a chairman.
- Congress should enact legislation exempting the Board from the Government in the Sunshine Act.
- While is appropriate that the Board's activities focus on protecting the privacy rights of U.S. persons, Congress should not expressly restrict the Board's statutory jurisdiction to only the rights of U.S. persons.
- Congress should not require the Board to keep the Director of National Intelligence or other elements of the intelligence community "fully and currently informed" of its activities.

In April 2016, the House passed the Email Privacy Act by a vote of 419-0 – a vanishingly rare demonstration of national consensus on such a consequential issue.[106] The Email Privacy Act unites the left, the right, privacy groups, and the business community. Importantly, it would not harm the Department of Justice's ability to prosecute cases or defend against terrorism; because of a judicial ruling applicable in several states,[107] federal prosecutors and FBI agents nationwide already obtain search warrants for the contents of electronic communications as a matter of policy.[108]

Yet the bill has stalled in the Senate. The principal reason is disagreement over an amendment that would allow the FBI to obtain records about online activity without a judicial order. These records are commonly known as "electronic communications transactional records," or ECTRs, and could include information such as what websites a user visits; the senders, addressees, and time-stamps of a user's emails; and information that can pinpoint the user's location.

The authors understand the perspective of those who sought to add the "ECTR fix" (a shorthand that is itself contested[109]) to the bill. Their aim – ensuring that the FBI is able to fight terrorism effectively – is one we share. But a warrant requirement for accessing the content of stored communications – a rare area of overwhelming bipartisan consensus – should not be further delayed. In addition, the types of records covered by the ECTR amendment raise serious, independent privacy concerns. To its credit, the Justice Department recently provided a thorough set of answers to frequently asked questions about how law enforcement obtains ECTRs, what role they play in investigations, and potential privacy concerns.[110] But the terms on which the government can access various types of sensitive non-content data merit their own debate and deliberation by Congress, independent of the (now largely resolved) debate over access to email content.

The Email Privacy Act unites the left, the right, privacy groups, and the business community.

Another objection comes from the Securities and Exchange Commission and other civil-enforcement agencies, which argue that the act will impede SEC investigations.[111] We understand the SEC's need for email content to perform its duties. But the SEC typically obtains email content directly from the subjects of its investigations rather than from providers; powerful sanctions, including contempt of court, are available if a subject refuses to comply. Indeed, the current SEC Chair has acknowledged that during her three-year tenure the Commission has not once subpoenaed content from a communications provider.[112]

High-tech law-enforcement tools, such as video surveillance paired with powerful analytic software, could have game-changing implications for personal privacy. (Alestivak/Creative Commons)

As of this writing, there remains a chance that the Email Privacy Act will pass during the 114th Congress. But if it does not, the next president should, in the first 100 days of the new administration, call upon Congress to enact legislation requiring a warrant to obtain the content of email and documents stored in the cloud and imposing reasonable limits on nondisclosure orders. This would send a powerful signal that the new administration takes privacy seriously.

The new administration should then build on this call by launching a White House initiative to propose standards for government access to other types of sensitive data. These could include cell-site location data,[113] data generated by "internet of things" devices (from internet-connected cars, to home security systems, to medical devices), license-plate readers, facial recognition systems, and other foreseeable technologies with potentially game-changing implications for personal privacy. The initiative should bring together participants from technology, business, privacy, and national security backgrounds and should culminate in a White House summit highlighting the president's support for legislation addressing these issues.[114]

Congress, to its credit, has already begun considering the privacy implications of many of these technologies.[115] This suggests how salient they are to Americans across the political spectrum. A White House initiative would help earn the new administration political capital and public trust on digital-privacy issues while advancing a critical debate.

INTELLIGENCE TRANSPARENCY AND SECRET LAW

Recently, the government declassified 28 pages from the report of the Congressional Joint Inquiry into the 9/11 attacks. For years, the 28 pages' "secrecy ... made them almost mythical"[116] and spawned various conspiracy theories. Many believed, incorrectly, that the 28 pages contained damning proof that the Saudi government had foreknowledge of the attacks.

When the 28 pages were finally declassified, they turned out to be far less salacious than years of secrecy had led many to suspect. As *The New York Times* reported: "Subsequent investigations into the terror attacks pursued the leads described in the document and found that many had no basis in fact. But the mythology surrounding the document grew with each year it remained classified."[117]

The 28 pages are an object lesson in the risks of excessive secrecy and, simultaneously, an encouraging signal of the public's ability to handle the truth. They illustrate, as one expert told us, that a reflexive anti-disclosure stance has become an "anachronism." While they were secret, the 28 pages fueled years of conspiracy theories and speculation. Once declassified, they made a few days' worth of news and then faded into memory.

It is self-evident that most details of intelligence operations need to remain secret. Fortunately, it is not these details that are most important for democratic accountability, public trust, and political sustainability. The public needs to know and approve of the general contours of what intelligence agencies are empowered by law to do, and why, and have confidence that the agencies are being held to those limits. If unintended disclosures reveal that the scope of government surveillance is qualitatively greater than the public believed, or that oversight is qualitatively less effective, then public trust falters. And, as history shows, it is hard to win back. Important surveillance powers will be politically sustainable only if the public is persuaded that they are necessary, appropriate, and lawful.

In short, the public needs to know the broad strokes of what the government can do, why it needs those powers, and what legal and institutional constraints apply. The U.S. government can provide greater transparency – albeit at this high-altitude level of detail – without compromising the effectiveness of intelligence operations.

What would this mean in practice? Senior leaders should continue and expand efforts to demystify the NSA in the mind of the general public. To their credit, in the wake of the Snowden leaks, NSA leaders have utterly transformed the agency's attitude toward publicity, placing senior leaders in the public eye far more than ever before. Yet few Americans understand *why* the NSA does what it does. The case for robust signals-intelligence capabilities would be persuasive to most Americans if made forthrightly.

Importantly, however, this means making the case for signals intelligence beyond counterterrorism. There are many other valid purposes: Documenting foreign military activity, including in regions like Crimea or eastern Ukraine where the facts are disputed. Unraveling transnational criminal networks. Monitoring proliferation of weapons of mass destruction. Even traditional espionage against foreign governments serves purposes that are not nefarious and that the public would understand. Knowing the intentions and views of foreign governments reduces the risk of miscalculation and escalation. Counterintuitively, surveillance can sometimes help build confidence between countries that do not otherwise trust one another. One illustration of this effect is the Open Skies Treaty, which permits unarmed observation flights over member countries, including the United States and Russia, in order to "enhance mutual understanding and confidence."[118]

It is important to talk about these other purposes of signals intelligence. Limiting the public defense to counterterrorism alone invites a backlash when non-counterterrorism signals-intelligence programs are revealed. The authors repeatedly heard this critique from citizens of allied countries – "you say you use these capabilities for counterterrorism, but why are you spying on our government?" If other uses of signals intelligence are defensible, U.S. leaders should defend them on their own terms, albeit at a high enough level of generality to avoid endangering sources and methods.

Secretary of Defense Ash Carter speaks with NSA Director and U.S. Cyber Command Commander Admiral Michael S. Rogers at NSA headquarters. (Senior Master Sgt. Adrian Cadiz/DoD)

Finally, the next president should announce an administration-wide effort to reduce the amount of what some term "secret law" applicable to surveillance programs.[119] This should include several elements. Most broadly, the next president should publicly embrace the principle that all domestic surveillance or surveillance of U.S. persons overseas will be based on clear statutory authority, publicly interpreted, with sufficient oversight to hold the government to its construction of the statute.[120]

Limiting the public defense to counterterrorism alone invites a backlash when non-counterterrorism signals-intelligence programs are revealed.

The president should then task the General Counsels of the Office of the Director of National Intelligence, NSA, FBI, and CIA, and the Assistant Attorney General for National Security, in consultation with the PCLOB, with proposing, within six months, other ways to reduce the amount of classified legal interpretation and programmatic guidance governing electronic surveillance. This could include, where consistent with national security, further declassification of relevant presidential directives, agency procedures, interagency memoranda of understanding, opinions of the Justice Department's Office of Legal Counsel, and classified annexes to legislation.

Even those documents in these categories that cannot be safely declassified and published, however, should be shared, in a manner consistent with their classification and to the extent permitted by executive privilege, with the congressional intelligence committees.

Finally, assuming that some residuum of secret law will unavoidably remain, this inquiry should consider measures to enhance accountability and public confidence. These might include "public notification of secret law's creation, presumptive sunset and publication dates," and creation of a shared repository of relevant "secret law" available to the responsible cleared officials from each of the three branches of government.[121]

SECTION 702 OF THE FISA AMENDMENTS ACT

Section 702 permits the government to acquire, with the compelled assistance of commercial providers, the communications of non-U.S. persons overseas. The government does not need to obtain individualized judicial orders for each target. However, the Foreign Intelligence Surveillance Court annually reviews the program and must approve a detailed "certification" specifying how the program will be administered and what safeguards are applied, jointly submitted by the Director of National Intelligence and the Attorney General.[122] The functioning of the program's two components, PRISM and "upstream," has been thoroughly described in the Privacy and Civil Liberties Oversight Board's report on Section 702.[123]

Title VII of the Foreign Intelligence Surveillance Act, which includes Section 702, will sunset on December 31, 2017, unless Congress reauthorizes it. This means that the next administration will have no choice but to publicly stake out a position on reauthorization and possible reforms to Section 702. This reauthorization process will be both an opportunity and a potential speed bump for the new administration's efforts to establish credibility on surveillance and digital-privacy issues.

Section 702 should be reauthorized, but with additional reforms to enhance public confidence, transparency, and privacy. Outside observers must rely on proxies in assessing this classified program's effectiveness. That said, the available evidence suggests that the program has become a vital intelligence tool, is legitimate in its basic contours, and is subject to adequate transparency in many, but not all, respects (more on that next page).

Unless Congress reauthorizes Section 702, it will sunset on December 31, 2017. (Architect of the Capitol)

TWO TYPES OF COLLECTION UNDER SECTION 702: PRISM AND UPSTREAM

PRISM collection under Section 702: "The government sends a selector, such as an email address," to a U.S.-based service provider. The provider is then "compelled to give the communications sent to or from that selector to the government." The NSA receives all PRISM data; the CIA and FBI receive some of it.

Upstream collection under Section 702: The NSA filters communications to or from the targeted selector directly from "the telecommunications 'backbone' over which telephone and Internet communications transit." Upstream also collects communications that *mention* the targeted selector in other fields of the message. Only the NSA has access to raw upstream data.

Source: 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)

Most notably, the authors are moved by the Privacy and Civil Liberties Oversight Board's measured but largely positive judgment in its comprehensive review of Section 702:

> Overall, the Board has found that the information the program collects *has been valuable and effective in protecting the nation's security and producing useful foreign intelligence*. The program has operated under a statute that was publicly debated, and the text of the statute outlines the basic structure of the program. Operation of the Section 702 program has been subject to judicial oversight and extensive internal supervision, and the Board has found no evidence of intentional abuse.[124]

What statistics are publicly available suggest that Section 702 has become a central foreign intelligence tool, particularly for counterterrorism. The Board reported that, at the time of its report last year, "*over a quarter* of the NSA's reports concerning international terrorism include information based in whole or in part on Section 702 collection, and this percentage has increased every year since the statute was enacted."[125] Qualitatively, the Board found that "[m]onitoring terrorist networks under Section 702 has enabled the government to learn how they operate, and to understand their priorities, strategies, and tactics"; that it "has led the government to identify previously unknown individuals who are involved in international terrorism"; and that it "has played a key role in discovering and disrupting specific terrorist plots aimed at the United States and other countries."[126] Overall, in 2015, the intelligence community targeted 94,368 overseas individuals, groups, or entities under 702.[127]

Other sources echo the Board's finding that Section 702 is a vital tool for counterterrorism and foreign intelligence more broadly. Matthew Olsen, former General Counsel of NSA and former Director of the National Counterterrorism Center, recently testified that Section 702 "has proven to be a vital authority for the collection of foreign intelligence to guard against terrorism and other threats to our national security" and "has significantly contributed to our ability to prevent terrorist attacks inside the United States and around the world."[128] The NSA has said that "Section 702 is the most significant tool in the NSA collection arsenal for the detection, identification, and disruption of terrorist threats to the U.S. and around the world."[129]

At the same time, Section 702 raises significant domestic civil liberties concerns – in particular, the "incidental" collection of the communications of U.S. persons and the subsequent use of such information. While the government cannot use Section 702 to target U.S. persons, their communications can be collected if they communicated with a target. Communications between two foreign persons may also contain information about a U.S. person.

What the agencies can do with incidentally collected information about U.S. persons is limited by "minimization" rules approved annually by the Foreign Intelligence Surveillance Court.[130] The minimization rules for the NSA, FBI, CIA, and National Counterterrorism Center are available online, with relatively few redactions.[131] Under the USA Freedom Act, significant FISC opinions, including the court's review of the 2015 Section 702 certification by the DNI and Attorney General, have been declassified and published.

Some have noted that, given these safeguards, "the criticism of Section 702 has focused on *hypothetical* rather than actual abuses of Section 702 authorities."[132] This is true, but hypothetical abuses are an appropriate concern where government is granted concentrated and largely secret power. Indeed, the basic design of the U.S. system of government reflects the Framers' fear of hypothetical abuses of centralized power.

President Barack Obama meets with FBI Director James Comey. (Pete Souza/Official White House Photo)

Beyond incidental collection itself, the most sensitive aspect of Section 702's operation is the FBI's ability to use U.S.-person identifiers to query Section 702 data – most controversially, in criminal investigations unrelated to national security. During the course of investigations, FBI agents and analysts typically search the Bureau's databases to see what it already knows about a particular person. One of those databases contains foreign intelligence information, including information from Section 702 and from traditional FISA.[133]

Critics describe such queries as "backdoor searches," arguing that they evade the Fourth Amendment limits that would otherwise apply to government attempts to collect Americans' communications.[134] The Foreign Intelligence Surveillance Court recently held that this practice comports with the Fourth Amendment.[135] Yet even if such searches are constitutional – a complex legal question we do not attempt to resolve here – searching foreign intelligence databases for information about Americans that was collected without a warrant raises serious privacy concerns.

On the other hand, there are also colorable reasons for not prohibiting such queries altogether. The 9/11 Commission found that the government's inability to synthesize pieces of information that different agencies already had – to "connect the dots," in other words – was a key failing that allowed the attacks to occur. If there is a connection between an FBI investigation in the United States and information the government has already collected under 702 – including the communications of known terrorists – it is important to be aware of that.

The limited public information about this practice means that estimates of its national security value are unavoidably conjectural. Additional clarity could help the FBI persuade observers that it is legitimate and necessary. To that end, the FBI should publicly explain with greater precision why it needs the ability to query databases containing 702 information for U.S.-person identifiers to perform its mission, notwithstanding that (i) where investigators lack probable cause (such as early in an investigation), they can use metadata or traditional investigative techniques to identify suspicious connections and thereby establish probable cause to obtain a warrant, and (ii) with a warrant, the Bureau can obtain information equivalent to any content collected under 702, and more, often without notice to the target of the investigation. The Bureau should provide this explanation during the upcoming 702 reauthorization debate.

To be sure, there may be persuasive answers to these questions; such queries may fill an investigatory niche that the posited alternatives would not. For example, it may be impracticably burdensome or unduly invasive of subjects' privacy to replace queries of information the Bureau already holds with additional investigation that gathers new information into the FBI's files. A more granular explanation of the role these queries play in FBI investigations and the suitability of posited alternatives would, if persuasive, help bolster the public legitimacy and sustainability of this practice.

Alternatively, a compromise solution could allow the FBI to continue to use these queries to identify problematic connections but avoid the most serious potential Fourth Amendment concerns. Specifically, during the upcoming authorization debate, Congress should ask the FBI whether it would be sufficient for it to continue to query databases containing 702 data for U.S.-person identifiers but, where such a search returns 702 information, to receive only the responsive metadata rather than the content. Responsive metadata, if it reveals a problematic connection, could then establish probable cause to view the underlying content.

> ***Searching foreign intelligence databases for information about Americans that was collected without a warrant raises serious privacy concerns.***

Congress and the American people would also benefit from additional information about the volume of such queries and the handling of 702 data that they return. It may be that disclosing more information about U.S.-person queries of 702 data would show that the scale of the potential privacy problem is less grave than feared. The FBI receives only a portion of the data collected through PRISM and none of the "upstream" data collected from the internet backbone.[136] It is apparently extremely rare for a query in a non-national-security investigation to return a hit in the FBI's FISA database. The existence of such a connection, while rare, may be a key element in unraveling a terrorist network or other transnational illicit activity. Moreover, only FBI personnel with special training in handling foreign-intelligence information are permitted to *view* responsive information; a query conducted by an agent or analyst without such training returns only a notification that responsive information exists.[137] Analysts without such training must now obtain a supervisor's approval before viewing the responsive information.

Additional information would help inform the public debate about how problematic this practice is from a privacy perspective, and about the scale of incidental collection more broadly. We therefore recommend that Congress, as a condition of reauthorization, mandate further transparency about several various aspects of the 702 program:

Require and enable NSA to fully implement PCLOB Recommendation 9. The Privacy and Civil Liberties Oversight Board recommended in its report on Section 702 that NSA assemble and declassify to the extent practicable several categories of information about the incidental collection, use, and querying of U.S.-person information. For various reasons, that recommendation has been only partially implemented.[138] Congress should incorporate these requirements into reauthorization legislation and, if needed, provide additional funding to enable NSA to comply.

Estimate the overall scale of incidental collection, if a valid and practicable methodology can be found. No one knows how voluminous incidental collection – that is, the collection of data about U.S. persons as an incidental result of permissible targeting of foreigners under Section 702 – actually is. As the PCLOB put it: "[L]awmakers and the public do not have even a rough estimate of how many communications of U.S. persons are acquired under Section 702."[139] The debate about whether Section 702's potential privacy harms outweigh its importance to national security would be better informed if Congress and the public had some idea of how much U.S.-person data is collected.

For obvious reasons, NSA does not review all data collected by the program to identify U.S.-person data. The government argues, reasonably, this would increase the privacy harm to Americans by putting human eyes on data that would otherwise go unreviewed and "age off" its servers after the retention period expires. A representative sample, as some members of Congress and privacy organizations have urged, would be less intrusive.[140] And NSA has conducted analogous statistical reviews before.[141]

That said, while a statistically valid estimate is desirable in theory, it may be difficult to achieve in practice.[142] The principal reason is that communications collected under Section 702 typically lack information that would enable officials to determine whether a U.S person is involved. An email, for example, does not necessarily make clear the nationality of the sender and recipient, much less those discussed in the body text.

These challenges are real, but efforts to surmount them should continue. The intelligence community should persist in seeking to develop an approach that would produce an accurate, statistically valid estimate of incidental collection. If those efforts do not succeed, the next administration and Congress should consider convening a technical working group, perhaps under the auspices of the National Academies of Sciences, Engineering, and Medicine, to consider alternative approaches.

Publish annually the number of instances in which an FBI query in a non-national-security investigation returns 702 information about a U.S. person. The Foreign Intelligence Surveillance Court "now requires the FBI to report to the Court," in detail, every time "FBI personnel view 702 information in response to a query in a non-national-security investigation."[143] While the details of these reports must remain classified, we can identify no national security harm that would result from publishing the overall number of such occurrences.

Estimate the total number of U.S.-person queries of databases containing 702 data conducted by the FBI in non-national-security criminal investigations. The FBI does not currently collect this information.[144] The reason is that its queries "do not distinguish between U.S. persons and others because nationality is not relevant to most criminal investigations."[145] The Bureau need not revamp its entire record-keeping system in order to produce such an estimate, however; a statistically representative sample of cases would suffice.

Provide more detail about which cybersecurity crimes the Department of Justice considers "serious crimes" for which it will use 702-derived information in a criminal proceeding. The General Counsel of the Office of the Director of National Intelligence has stated that the government "will use information acquired under Section 702 as evidence against a person in a criminal case only in cases related to national security or for certain other enumerated serious crimes," and only with approval by the Attorney General.[146] Those "enumerated serious crimes" include, inter alia, "crimes involving … cybersecurity."[147]

This enumeration provides a constructive and basically adequate level of transparency here. That said, some have raised the specific concern that "'crimes involving cybersecurity' are undefined, and could be applied in an overbroad manner."[148] The spectrum of crimes falling under the rubric of "cybersecurity" is broad; for example, a federal appeals court recently held that unauthorized password-sharing can be prosecuted under the Computer Fraud and Abuse Act.[149] Some additional detail about what types of cybersecurity crimes the government will use Section 702 data to prosecute would help address these concerns.

Publish the Justice Department's standard for determining whether evidence introduced in a criminal proceeding is "derived from" 702 information. FISA requires the government to notify criminal defendants when it introduces into evidence information "derived from" 702.[150] The Justice Department has thus far refused to disclose publicly its standard for determining when this phrase is triggered. It is hard to see how national security would be harmed by the Department's further explaining how it interprets this legal obligation.[151]

Mandate the appointment of an amicus curiae in 702 certification proceedings. The USA Freedom Act included important reforms that enhanced the FISC's credibility – most notably, authorizing the court to appoint, from a pool of cleared advocates, amici curiae tasked with representing the public interest. One of these advocates, Amy Jeffress, raised such arguments in the FISC's review of the government's 2015 certifications for the Section 702 program. Her participation appears to have enhanced the rigor, and thus the public credibility, of that proceeding.[152]

Whether to appoint an amicus in a given case is currently up to the court,[153] but there is no apparent reason why an amicus would not have the same beneficial effect on every annual 702 certification proceeding. When Congress reauthorizes the FISA Amendments Act, it should require that one of the FISC amici be appointed to represent the public interest in the annual certification proceedings for Section 702.

Provide to the public as much detail as possible about the national security value of Section 702. The Privacy and Civil Liberties Oversight Board, along with credible current and former officials, have described Section 702's immense value for national security – albeit in general terms. The Office of the Director of National Intelligence should make every possible effort to add to these credible but relatively vague endorsements concrete details that demonstrate the program's value.

Taken together, these reforms will provide Congress and the public with a much stronger public record on which to assess Section 702 and weigh the program's potential privacy harms against its value for national security. Assuming, as seems likely, that the FISA Amendments Act will be again reauthorized with a sunset provision, these measures should bear fruit in time to usefully inform a future reauthorization debate.

THE PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD

The Privacy and Civil Liberties Oversight Board has become a respected and important member of the constellation of oversight entities in this space. The Board's Section 702 report in particular was a landmark; its detailed, unclassified description of the program's basic operation has enabled a much more fact-based public debate about its value and privacy implications.

Importantly, the benefits of a robust Board extend beyond enhancing privacy and civil liberties; it benefits the national security community as well. The Board's judgments can help legitimize controversial programs. Precisely because of its independence, the Board's judgment that the 702 program is "valuable and effective" provides a powerful argument for reauthorization. More broadly, the Board's very existence and its reputation as a vigorous and independent voice strengthen the case that U.S. signals-intelligence programs are subject to robust, multi-layered oversight. This argument is particularly important in Europe, where the Board's existence and independence carry considerable weight.[154]

In short, the Board has been a success – but it is a fragile success. The Board's positive effect on U.S. credibility would evaporate, or even become a negative, if the Board were allowed to fade back into dormancy.

Unfortunately, there is reason to fear that this may happen next year. The Board's chairman resigned this year, and no replacement has been nominated.[155] This alone would be a problem, given that the Board's enabling statute permits only the chairman to hire staff.[156] Yet there are additional

concerns. Another member has been renominated but not reconfirmed; his extended term will expire when the Senate adjourns *sine die* in January.[157] A third member's term will expire in January and can be extended for only 60 days unless the new president nominates a replacement.[158] In sum, by early next year, the Board could be down to as few as two members – less than the quorum it needs to operate.

Accordingly, it is essential that the next president swiftly appoint new board members or reappoint existing members and work with the Senate to ensure that they are promptly confirmed. The Board's inherent bipartisanship means that there should not be a strong partisan valence here. And to ensure that the Board is not paralyzed in situations where it lacks a chairman, Congress should enact legislation permitting the remaining members to collectively appoint staff in the absence of a chairman, as the Senate Select Committee on Intelligence has proposed.[159]

The Privacy and Civil Liberties Oversight Board has been a success – but it is a fragile success.

In addition, in order to enhance the Board's ability to deliberate effectively, Congress should enact legislation exempting the Board from the Government in the Sunshine Act. The act requires that all Board meetings – vaguely defined as "deliberations" involving more than two members that "result in the joint conduct or disposition of official agency business" – take place in public.[160] To be sure, it is important that the Board involve the public in its work and reach official decisions in a transparent and accountable manner. But the Board's organic statute already provides for significant transparency, requiring the Board to make its meetings and reports "available to the public to the greatest extent that is consistent with the protection of classified information."[161]

The added requirements of the Sunshine Act impede effective collaboration and are a poor fit for the Board's work, for several reasons. First, unlike the regulatory bodies the act was designed to hold accountable, the Board exercises no regulatory authority – it can only perform oversight and offer nonbinding advice. In this context, the benefits of informal collaboration far outweigh any possible concern about opaque decisionmaking. Second, because the Board's work is overwhelmingly classified, it must expend inordinate time and energy following the act's cumbersome procedures for closing its many meetings covering classified subject matter.[162] Finally, since four of the Board's five members are part-time and have conflicting outside commitments, it is especially important that they be permitted to collaborate flexibly outside of formal meetings. The act makes informal collaboration unduly difficult.

Congress should remove this nuisance, which adds little and prevents the Board from being as effective as it might be. Alternatively, Congress should consider making all five Board members full-time, enabling them to devote themselves fully to the job.

Another concern is that legislation circumscribing the Board's authority could undermine its public credibility. Section 603 of the Senate's FY 2017 Intelligence Authorization Act would expressly limit the Board's jurisdiction to activities affecting the privacy and civil liberties "of United States persons."[163] To be clear, it is appropriate that the Board's activities focus on protecting the privacy rights of U.S. persons. But Section 603's express limitation to that effect is a solution in search of problem – and it risks creating several additional headaches. First, it would prevent the Board from responding to requests from the president, the intelligence community, or Congress to look into issues affecting the privacy interests of non-U.S. persons.[164] Second, and most importantly, it would unnecessarily suggest to European audiences that their privacy is not protected by the U.S. oversight infrastructure – a damaging prospect given that the survival of the Privacy Shield agreement will likely turn on just such perceptions.[165] Absent some future development that illustrates a compelling need for such a restriction, the Board's jurisdiction should not be expressly limited to considering the privacy rights of only U.S. persons.

Finally, Congress should not require the Board to keep the Director of National Intelligence or other elements of the intelligence community "fully and currently informed" of its activities.[166] Reporting to Congress is entirely appropriate and indeed essential – the Board, like other executive branch agencies, is subject to Congress' laws and funded by its appropriations. But a requirement to report to the agencies that the Board is meant to oversee impinges upon its independence, and thus its credibility. The Board's reliance on information provided by the intelligence community suffices to ensure that adequate working communication is maintained.

UPDATE WHISTLEBLOWER LAWS

Update Whistleblower Laws In the wake of Edward Snowden's leaks, many debated whether he would or would not have been protected by existing whistleblower laws.[167] Without wading into that debate here, the uncertainty surrounding the question was itself undesirable.

The law should clearly allow civil servants and contractors working in the intelligence community to report potential abuses within cleared channels – specifically, to their supervisors, to inspectors general, and ultimately to the congressional intelligence committees. On the other hand, it should not encourage those entrusted with classified information to take the law into their own hands and publish information that the people's democratically elected representatives have decided must be kept secret for reasons of national security.

Under current law, employees of the intelligence community who report abuses to their agency's inspector general or to the Intelligence Community Inspector General, and from there to the congressional intelligence committees, are protected against retaliatory personnel actions, including retaliatory revocation of their security clearances.[168] However, the statutory term "employee" likely does not apply to the many contractors working within the intelligence community. Presidential Policy Directive 19 (PPD-19), issued by President Obama in 2012, contains many similar protections, and administration officials have suggested that they view PPD-19 as at least partially applicable to contractors.[169] But that protection is at best unclear and could easily be rescinded by a future president.

To ensure that the scope of whistleblower protections is clear, the next president should issue an executive order making PPD-19's protections binding within the executive branch and clarifying that they extend to contractors working at all intelligence community components. Ultimately, Congress should extend the full panoply of statutory whistleblower protections to contractors working in the intelligence community.

The FBI, which is subject to its own agency-specific whistleblower regime, has had various struggles with whistleblower protection over the years.[170] In April, the Senate Judiciary Committee approved bipartisan legislation, co-sponsored by Chairman Charles Grassley and Ranking Member Patrick Leahy, to update the Bureau's whistleblower regime.[171] Among other changes, the bill would extend whistleblower protection to employees who report abuses to their supervisors as well as to the Inspector General and other officials designated by the Attorney General – an uncontroversial change endorsed by Attorney General Loretta Lynch and FBI Director James Comey.[172] The bill also clarifies that FBI employees can report alleged malfeasance to members of Congress[173] and to the Office of Special Counsel.[174] If this bill is not enacted during the 114th Congress, the next Attorney General should support legislation updating the FBI's whistleblower process in the next Congress.

The law should clearly allow civil servants and contractors working in the intelligence community to report potential abuses within cleared channels.

Protecting a Flourishing Technology Industry

The aftermath of the Snowden disclosures illustrated the severe repercussions that surveillance decisions can have for the American technology industry. This is not merely a concern for those companies' shareholders; it is also a national security concern. Economic strength and technological sophistication are fundamental pillars of national power. The United States' leadership in information technology is an important source of employment, wealth creation, and global influence. Information-technology companies create hundreds of thousands of high-paying American jobs. Tech is a leading export industry. And it produces immense advantages for the defense industrial base.

Less obviously, however, it is also an enormous advantage for the U.S. intelligence community and law enforcement that the world's leading internet companies are based in the United States and store much of their data here. For example, Section 702, NSA's "most significant" tool for collecting counterterrorism intelligence, works only because so much relevant data is held by U.S.-based companies or transmitted across internet cables that pass through the United States. In short, there are many reasons – including national security reasons – to ensure that surveillance policy does not endanger this golden goose.

> ***The aftermath of the Snowden disclosures illustrated the severe repercussions that surveillance decisions can have for the American technology industry.***

Surveillance decisions that harm the U.S. technology sector also drive a wedge between firms and the government. The Snowden disclosures "created an overall fear among U.S. companies that there is 'guilt by association' from which they need to proactively distance themselves."[175] Technology executives, understandably focused on retaining their customers' trust, recoiled from contact with the government and even took highly visible steps to enable their clients to prevent government surveillance. This harms intelligence and law enforcement efforts by making quiet cooperation between industry and government more difficult.

ENCRYPTION

The most prominent example of this backlash is the rapid adoption of strong encryption technologies across a range of widely used consumer products. The accelerated shift toward user-controlled encryption was largely a response to the Snowden leaks. For example, in the immediate wake of the disclosures, Eric Schmidt – whose company's overseas internal server-to-server links the NSA had reportedly accessed without the company's consent or knowledge[176] – said that "[t]he solution to government surveillance is to encrypt everything."[177] Later, in response to Director Comey's concerns about encrypted mobile devices, Schmidt responded: "The people who are criticizing this are the ones who should have expected this."[178]

Since then, leading companies have significantly expanded the use of encryption in their products – both with respect to "data at rest" on mobile devices and "data in motion" between end users. Most prominently, Apple devices running iOS 8 or later now feature full-disk encryption keyed only to the user's passcode. This makes it extremely difficult for law-enforcement officers to access data stored on a suspect's phone – for example, a phone taken from an arrestee or captured in a raid on a terrorist safehouse – unless the data is backed up to the cloud, the police learn the passcode, or officers seize the device while it is unlocked.

This means that these phones are inaccessible even if law enforcement has obtained a search warrant to access their contents.[179] Apple's privacy policy explains:

> For all devices running iOS 8 and later versions, Apple will not perform iOS data extractions in response to government search warrants because the files to be extracted are protected by an encryption key that is tied to the user's passcode, which Apple does not possess.[180]

The FBI's struggles to access the iPhone used by one of the San Bernardino shooters brought worldwide attention to the challenges device encryption poses for law enforcement – although it did not produce agreement on the severity of that problem or how to address it.

Meanwhile, Apple's iMessage, Facebook's WhatsApp, and other messaging services have introduced end-to-end encryption for data in motion across their services. This means that only the end users can read the content of messages in decrypted cleartext. As with device encryption, the end result is that providers cannot give law enforcement decrypted content, even in response to a warrant.

PROTECTING A FLOURISHING TECHNOLOGY INDUSTRY

Encryption

- Given the impasse over decryption legislation, and given that the debate itself has damaged relations between the government and the technology industry, the next administration should de-escalate the public debate over encryption.
- The FBI should support its argument for an encryption mandate by publishing more data about the precise contours of the technical challenge posed by encryption.
- To help the FBI cope with the status quo, Congress should scale up the FBI's resources for gaining access to encrypted devices and communications without compelled assistance from providers.
- This scaling up should also include resources to enable the FBI to create a centralized repository of expertise and technical assistance for the 15,000 state and local law enforcement agencies in the United States.

Risk Management in SIGINT Decisions

- Operations that, if exposed, would pose a significant risk to an American company or business sector should be approved by senior political appointees after a process that incorporates, to the greatest extent possible, external input about the scale of the risk.
- The government should create regularized channels for candid communication between NSA and the technology industry, such as creating an industry advisory board of corporate officials who hold security clearances.
- To the extent that a dialogue would, for some companies, raise concerns about appearing complicit in NSA practices, NSA should also establish a formalized one-way channel for receiving comment from American companies about the risks that signals-intelligence practices pose to their businesses and other issues of concern.
- Where the U.S. government wishes to obtain data held by a U.S. company, it should generally seek to access the data through the "front door" provided by U.S. domestic law rather than through overseas intelligence operations or liaison relationships.
- To the extent that the government contemplates operations that involve tampering with or introducing vulnerabilities into an American company's product before it reaches its end customer, any such operations should be approved by the National Security Advisor with input, where appropriate, from the Deputy National Security Advisor for International Economic Affairs, or another senior official with analogous responsibilities.
- The government should not, as a rule, pressure American technology companies to compromise their own products or hand over their source code.
- The government should not pressure American companies that sell to the government to disclose to it vulnerabilities that the company discovers before the company discloses them to other customers.
- The Vulnerabilities Equities Process should be formalized in an executive order.
- The executive order should, to the maximum extent consistent with national security, list all agencies that have a say in the process and should specifically state which agencies have a vote on whether to retain or disclose a vulnerability.
- In order to ensure that the process takes account of the broader interests of the U.S. technology sector, the Department of Commerce should have a regular seat at the table.
- The executive order should also describe the process to be followed in deciding whether to retain or disclose a vulnerability. In particular, it should clearly state the government's substantive standard for deciding whether a vulnerability's potential national security benefits outweigh the risks of retaining it.
- The executive order should also require that there be periodic review of whether a retained vulnerability should be disclosed.
- The executive order should provide for public annual reports containing as much detail about the process's operation as is consistent with national security, along with a classified annex for the relevant congressional committees.

iPhones protected by full-disk encryption have frustrated law enforcement. (Adrian Ilie/Creative Commons)

Encryption is becoming a serious challenge for law enforcement and counterterrorism. Law-enforcement agencies across the United States are accumulating piles of devices for which they have obtained or could obtain search warrants but which cannot be unlocked because of encryption. In Senate testimony last year, Manhattan District Attorney Cyrus Vance Jr. offered several specific examples of investigations thwarted by unbreakable encryption.[181] Government hacking, like the FBI's purchase of a "gray market" exploit in the San Bernardino case, may be an option in a few high-value cases. But it is difficult to scale and is not a realistic option for most of the 15,000 police departments across the country, which do not have the financial or technical resources of the FBI.

This is not just a law-enforcement problem; international terrorists are consciously using encrypted communications to enhance their operational security. Both ISIS and al Qaeda have made heavy use of Telegram, a Berlin-based app that touts its end-to-end encrypted "[s]ecret chats ... meant for people who want more secrecy than the average fella."[182] An ISIS operational-security manual specifically recommends that operatives use Telegram and other encrypted apps,[183] and ISIS recruiters commonly move to an encrypted platform after establishing contact with a potential recruit on social media.[184] The chief planner of last year's Paris attacks reportedly gave each operative "an email address to reach him on and a USB stick with an encryption key he was to download on his computer."[185] And those involved in the Paris plot reportedly used encrypted services, including WhatsApp and Skype, to communicate with operatives in Syria while they laid low between the Paris attacks and the subsequent attacks in Brussels.[186]

European allies, facing a wave of attacks planned or inspired by ISIS, are increasingly faulting encryption for obstructing terrorism investigations. For example, European officials blamed the failure to find those who planned the Paris attacks before they struck again on encrypted communications: "Everyone was trying to find these guys. ... They were able to elude us. But they were able to elude the Americans, too, and that shows you what a problem encryption is."[187] In the wake of repeated attacks in both countries, the interior ministers of France and Germany recently called for legislation requiring encryption providers to assist law enforcement in terrorism investigations.[188]

One common response is that law enforcement can use metadata, content stored in the cloud, or other information like geolocation data as a substitute for content made inaccessible by encryption.[189] Some even argue that these alternatives have created a "golden age of surveillance."[190] Government officials respond, however, that these are incomplete solutions. Metadata is often not as probative as content. Cloud backup may be unavailable or incomplete.[191] And government access to other forms of user data presents its own privacy challenges, which are only beginning to be confronted.

On the other hand, some of the solutions being proposed raise their own concerns. First, there is the risk that a decryption mandate would reduce the security of Americans' data. Requiring that companies retain the ability to decrypt data encrypted by their products would introduce a certain (albeit unquantified) degree of additional insecurity into those products. Adding complexity to software necessarily increases the risk that it will contain bugs for attackers to exploit. And requiring manufacturers to hold keys to devices they manufacture would create some risk of key theft – although an attacker would have to have both the key and physical possession of the device to capitalize on this.[192]

> ***There is the risk that a decryption mandate would reduce the security of Americans' data.***

It also bears noting that strong encryption's benefits are not limited to cybersecurity; it can also enhance *national* security, by shielding key U.S. government data and that of strategically important private actors from skilled adversaries. As Secretary of Defense Ash Carter has noted, the Department of Defense "is the largest user of encryption in the world, principally because our

troops need it. It helps keep our fighter jets and our sensor networks from getting hacked, it allows us to surprise our adversaries and it lets our people deployed around the world communicate securely with their families back home, from sailors aboard aircraft carriers to soldiers in Afghanistan."[193] In the private sector, strong encryption can help protect the intellectual property of defense contractors and other strategically important industries.[194] At the same time, it is unclear whether these national security needs call for encryption *that only the end user can unlock* – the feature most challenging for domestic law enforcement.

There are also serious concerns about the effect a decryption mandate would have on international human rights. Technologically advanced authoritarian states like Russia and China have powerful indigenous capabilities for surveilling their citizens and controlling the flow of information on the internet. Increasingly, however, technologically unsophisticated governments are also in on the game, as they can purchase high-tech monitoring systems and hacking tools from private companies.[195] These developments challenge a longstanding principle of U.S. foreign policy: internet freedom, including secure communications for dissidents and journalists living in authoritarian countries. Each year, the State Department's Bureau of Democracy, Human Rights, and Labor (DRL) funds the development of secure communications technologies for use by dissidents overseas.[196] American companies and foundations have also supported the internet freedom agenda by funding technologies to enable secure internet browsing and communications.[197]

A U.S. decryption mandate would, to some hard-to-quantify extent, reduce the ability of vulnerable people living under authoritarian governments to communicate and browse the internet securely. U.S. companies are responsible for many, albeit not all, of the most secure communications technologies that are widely available to consumers. If the United States requires U.S. companies to retain the ability to decrypt data, it seems safe to assume that authoritarian governments would allow only iPhones with that exceptional-access mechanism into their markets.[198] On the other hand, powerful countries with large internal markets, such as Russia and China, appear intent on having access to their citizens' data regardless of what the United States does.[199]

This is not an artificial debate in which one side is completely wrong and the other is completely right; it is an authentically difficult policy conundrum in which various legitimate interests are in tension with one another. Unfortunately, some of the most prominent arguments in this debate have implied otherwise.

For example, senior law-enforcement officials have contended that the Fourth Amendment's "balance" requires that all evidence be amenable to search once police get a warrant.[200] The Fourth Amendment, however, merely *limits* the terms on which police can conduct searches; it does not require citizens to preserve evidence to facilitate those searches.

Meanwhile, opponents of a decryption mandate frequently argue that it is "mathematically impossible" to design a perfectly secure system for government access – or, as one put it, that a secure lawful-access mechanism is a "magic rainbow unicorn."[201] That may be true, but it mischaracterizes the argument. Supporters of such a law do not contend that a lawful-access mechanism would be perfectly secure; rather, they argue that any reduction in security would be manageable and justified by the benefits for public safety.[202] That is debatable, but it is not impossible. It would be informative to know how often comparable existing platforms have been penetrated in the past and what security flaws led to those breaches. Technologists should also undertake forward-looking, practical assessments of how great the reduction in security would be if a given approach to mandatory decryption were adopted.

This is not an artificial debate in which one side is completely wrong and the other is completely right; it is an authentically difficult policy conundrum in which various legitimate interests are in tension with one another.

Similarly, strong-encryption advocates frequently argue that any decryption mandate will be toothless because the truly "bad guys" would simply switch to non-U.S. products.[203] This would surely be true of terrorists, child pornographers, and other sophisticated criminals. But most Americans, including ordinary criminals who are not tech-savvy, would stick with the most convenient, user-friendly, and widely accessible products. In that scenario, unsophisticated or impulsive criminals would no longer benefit from unbreakable encryption. This would not eliminate the set of hard targets for law enforcement but would likely reduce it

A decryption mandate would make devices less secure, but law-enforcement officials contend that the benefits for public safety would outweigh that harm. (Yuri Samoilov/Flickr)

dramatically. And with a much smaller set of high-value targets, one-off solutions like placing malware on a suspect's computer or using zero-day exploits to hack a device[204] – which are too costly or labor-intensive to be used for a large number of routine cases – might be an adequate alternative.

Ideally, both sides would focus on developing the factual record to support their assertions. A pragmatic, factually oriented debate would be far more useful to most observers and members of Congress, who come to this debate willing to consider the arguments and legitimate concerns of both sides.

For now, there appears to be little prospect of a decisive resolution either way. Legislation like the Senate's Burr-Feinstein bill seems unlikely to pass absent a major terrorist attack or some other event that dramatically alters the political balance. The Obama administration declined to seek such legislation; indeed, a leaked National Security Council options memorandum on encryption did not even include "seek legislation" among the three options considered.[205]

Given this impasse, and given that the debate itself has damaged relations between the government and the technology industry, the authors recommend that the next administration, even if it maintains the Obama administration's wait-and-see posture, de-escalate the public debate over encryption. Deciding not to decide is a rational approach given that the relevant facts are not fully known and public opinion is not fully formed. That means taking steps to ensure that the entire government acts consistent with that approach. There is little sense in declining to seek decryption legislation yet simultaneously antagonizing industry by seeking to use existing laws to achieve the same ends. In a world of widespread strong encryption and no compelled-decryption law, government will need a collaborative relationship with industry to identify alternatives to encrypted data – for example, making optimal use of available cloud backups and metadata.[206] Government will also need industry's support to combat the use of social-media platforms to spread terrorist propaganda.[207] De-escalating this debate can create breathing room for quiet industry-government discussions.

As long as the present impasse prevails, policymakers should focus on developing the factual record and exploring the pros and cons of various courses of actions. A working group recently launched by the National Academies of Sciences, Engineering, and Medicine, made up of leading experts from academia, industry, and civil society, should help.[208] Another promising option would be a commission to study the issue and develop the factual record, as U.S. Rep. Michael McCaul and Sen. Mark Warner have proposed.[209] If Congress creates such a commission, its mandate should be limited to studying the scope of the problem, exploring the various technical alternatives, and considering possible harms to data security, privacy, human rights, U.S. technological leadership, and other important interests. Weighing those values against each other, on the other hand, calls for the type of sensitive value judgments that should be made by the people's elected representatives, as members of the House Energy and Commerce and Judiciary Committees have argued.[210]

> ***Government will need a collaborative relationship with industry to identify alternatives to encrypted data.***

Whether or not a commission is created, however, the FBI should support its argument for an encryption mandate by publishing more data about the precise contours of the technical challenge posed by encryption. Specifically, it should document the specific technical obstacles (e.g., device and operating-system versions) and surrounding circumstances (e.g., whether cloud backups and/or metadata were viable alternatives) encountered in cases where investigations have reportedly been impeded by encryption. The record that preceded the enactment of the Communications Assistance for Law Enforcement Act (CALEA) in 1994, which was far more quantitatively detailed than anything that has been produced on the encryption issue, is illustrative.[211]

Finally, the new administration and Congress should work to help the FBI and state and local law enforcement cope with the status quo. Among other things, this means scaling up the FBI's resources for gaining access to encrypted devices and communications without compelled assistance from providers. Germany, which has thus far not sought a decryption mandate, recently took similar steps: The government recently announced that it will create a new agency to help law enforcement and the domestic intelligence services break encryption and otherwise ensure that it is technically possible to carry out lawful surveillance.[212] In a world of widespread strong encryption, the most likely alternative to "back doors" or some other kind of decryption mandate is "lawful hacking" authorized by search warrants.[213] It may be an imperfect solution from a law-enforcement perspective, but it is the only solution that is feasible in the current political climate.

> ***In a world of widespread strong encryption, the most likely alternative to "back doors" or some other kind of decryption mandate is "lawful hacking" authorized by search warrants.***

This scaling up should also include resources to enable the FBI to create a centralized repository of expertise and technical assistance for state and local law enforcement. There are more than 15,000 law enforcement agencies in the United States – many of them small state or local departments without the resources to circumvent sophisticated encryption technologies or purchase vulnerabilities like that used to access the San Bernardino shooter's phone. The FBI's Criminal Justice Information Center serves as a national center of excellence and knowledge repository for fingerprint analysis; the Justice Department should explore and report to Congress how the Bureau could perform a similar role for communications technologies, and what resources it would need.

RISK MANAGEMENT IN SIGINT DECISIONS

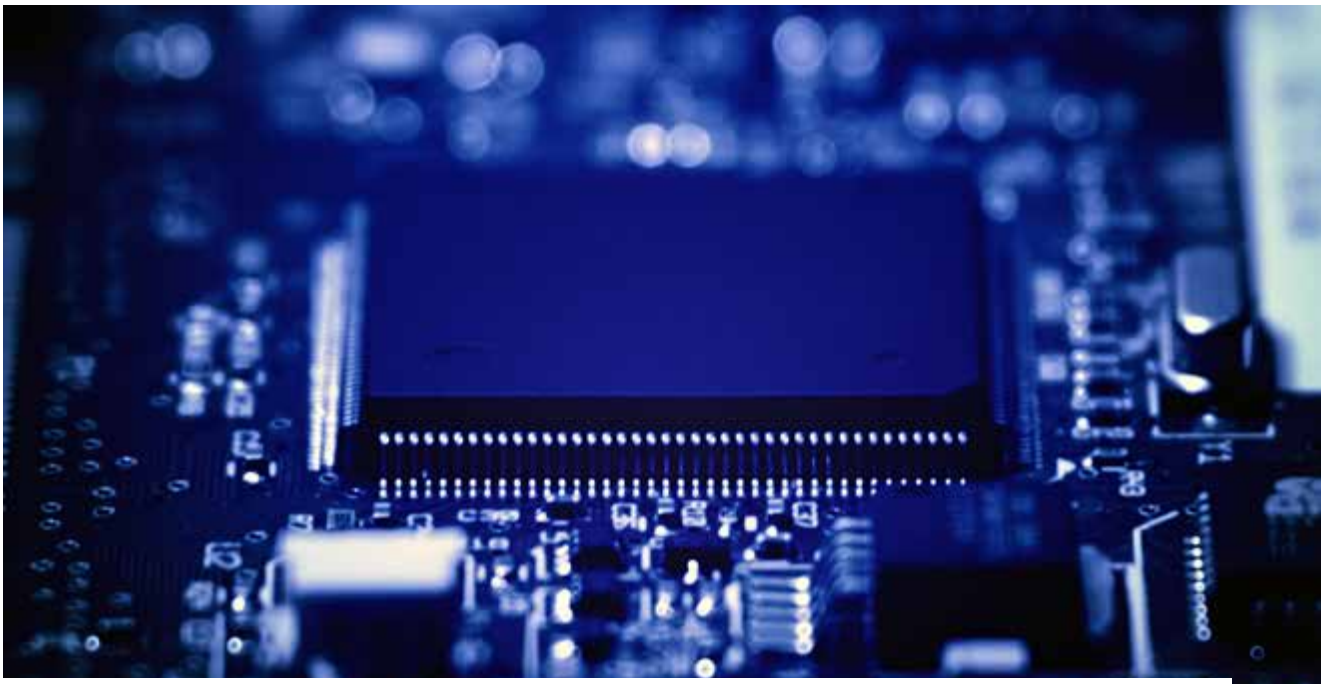
One of the indelible lessons of the post-Snowden period is that surveillance practices can pose a grave danger to the global business prospects of important American companies. In particular, surveillance practices that call into question the integrity or security of U.S. products endanger the technology industry's global competitiveness and give ammunition to foreign competitors, who may exploit NSA surveillance as a marketing tool.

Given the ubiquity of American technology, it is impossible to forbid altogether surveillance practices that implicate American products. But at a minimum, the government should do everything possible to ensure that (i) such operations are undertaken only where the national security ends justify the potential harms and (ii) the potential risks to American companies are accurately incorporated into the decisionmaking process. In the words of the President's Review Group, managing risk, including "risks to trade and commerce," is a "central task" of surveillance policy.[214]

There have been some positive steps in this direction. NSA Director Michael Rogers "determined one of the answers to" the NSA's reputational crisis "was to focus on strengthening and formalizing risk management."[215] NSA now has a "Chief Risk Officer" and has built an internal risk model that considers "disclosure, risk to U.S. foreign policy, risk to the U.S. technology sector, civil liberties and privacy."[216] (The model itself, and the weighting it assigns to each factor, are classified.) The Privacy and Civil Liberties Oversight Board recommended, and the intelligence community is reportedly developing, "a comprehensive methodology for assessing the efficacy and relative value of counterterrorism programs."[217] And the executive branch has reenergized the interagency Vulnerabilities Equities Process (VEP), which decides whether to exploit or disclose software vulnerabilities.[218]

While these steps are a promising beginning, more can and should be done to ensure that signals-intelligence practices collect needed information without creating unnecessary risks to the American technology industry. A good guiding principle is that operations that, if exposed, would pose a significant risk to an American company or business sector should be approved by senior political appointees after a process that incorporates, to the greatest extent possible, external input about the scale of the risk. The same is true of operations that, if revealed, pose strategic risks for U.S. foreign policy – a recognition embodied in President Obama's post-Snowden restrictions on surveilling foreign leaders.[219]

Unfortunately, such risk management appears to have fallen short in the pre-Snowden era. "While the



The Snowden disclosures undermined international confidence in the integrity of American hardware products. (Yuri Samoilov/Flickr)

NSA excels at performing ... cost-benefit analysis at the tactical level," it does not seem to have adequately weighed "the risks of those efforts becoming front-page news."[220] Indeed, even when undertaking highly sensitive espionage on allied leaders, the intelligence community reportedly conducted no cost-benefit analysis that considered the risk that the operation could be exposed.[221] Senior administration officials with a broader political view and wider experience are better positioned to weigh economic and political risks than NSA officials focused on that agency's mission.

Industry is also understandably skeptical that the NSA has adequate information to accurately gauge risk to the U.S. technology sector, and to particular companies, when deciding whether an operation's overall costs exceed its benefits. Because the new risk model is classified, it is not publicly known how it assesses the risk to American companies' businesses and reputations or how much weight it assigns to that risk in the overall calculus. Companies worry that the NSA, given its institutional interests and limited understanding of their businesses, will give overriding weight to intelligence value while underestimating the risks to the technology industry and that sector's importance to the broader national interest.

To address this, the government should create regularized channels for candid communication between NSA and the technology industry. In addition to enhancing the government's understanding of risks to the industry, this channel could provide a forum for an ongoing exchange of views on issues of mutual concern, enhancing the quality and stability of public-private contacts on signals-intelligence issues. One way to do this would be to create an industry advisory board, potentially comprising corporate officials who hold security clearances.

To the extent that a dialogue would, for some companies, raise concerns about appearing complicit in NSA practices, NSA could also establish a formalized one-way channel for receiving comment from American companies about the risks that signals-intelligence practices pose to their businesses and other issues of concern.

Reports that the NSA had accessed data held by U.S. companies through clandestine intelligence operations overseas rather than the mechanisms provided by domestic law were a particularly significant source of post-Snowden friction.[222] It should be a selling point for U.S. companies that the data they hold is protected by the United States' legal regime for access by law enforcement and the intelligence community. That argument is undermined if the government collects such data in overseas operations not covered by the statutes and constitutional provisions that apply at home. Accordingly, where the U.S. government seeks data held by a U.S. company, it should generally seek to access the data through the "front door" provided by U.S. domestic law rather than through overseas intelligence operations or liaison relationships.[223]

Britain's Government Communications Headquarters, which reportedly cooperated with the NSA to access communications links between U.S. companies' overseas data centers. (GCHQ | Crown Copyright)

To the extent that the government contemplates operations that involve tampering with an American company's product without the company's consent, any such operations would pose a significant potential risk to the U.S. technology industry.[224] The backlash that followed the release of the infamous photo depicting a Cisco box illustrates how damaging the perception of NSA tampering can be, both for particular companies and for confidence in American technology more broadly.[225] If American technology products are less trusted abroad, American technological leadership and American workers will ultimately suffer.

To ensure that such operations are undertaken only when strictly necessary, we recommend that operations that involve tampering with or introducing vulnerabilities into an American company's product before it reaches its end customer, to the extent that the government contemplates such operations, should be approved by the National Security Advisor, with input, where appropriate, from the Deputy National Security Advisor for International Economic Affairs or another senior official with analogous responsibilities.

While it is hard to define with precision what operations should be subject to this requirement, the basic principle is the front-page test: If disclosure of the operation would undermine trust in the security and integrity of an American company's product, the operation should undergo high-level review and be formally approved by politically accountable officials who take into account the nation's security and economic interests. Unlike most recommendations in this report, this should probably be implemented quietly, without public fanfare, as the harm of reminding foreign customers that the government may occasionally undertake such operations may outweigh any remedial effect. As such, this change is probably best viewed as prophylaxis against future disclosures rather than remediating past harms.

More broadly, the government should not, as a rule, pressure American technology companies to compromise their own products or hand over their source code. Many foreigners believe that the U.S. government routinely obtains American companies' source code or that American technology products are pervasively compromised by the NSA. Non-U.S. companies have exploited the resulting skepticism to gain an advantage over their American competitors. Some hardened skeptics will never be persuaded, but frequent repetition by high-level officials that this is not U.S. policy can help make this belief less widespread.

Similarly, the government should not pressure American companies that sell to the government to disclose to it vulnerabilities that the company discovers before the company discloses them to other customers. This practice, which would allow the government to exploit vulnerabilities before they are patched by the company's other customers, would similarly undermine foreign customers' faith in American products.

THE VULNERABILITIES EQUITIES PROCESS

Some cyber operations exploit vulnerabilities that already exist but are not known to the company – which means that they cannot be patched.[226] These are known as "zero days" because the developer has had zero days to address them. Such offensive operations do not create new vulnerabilities, but the decision to exploit existing vulnerabilities rather than disclose them to the manufacturer necessarily allows them to persist, leaving ordinary users of the flawed product at risk.[227] One prominent example is the recent leak of a trove exploit code, believed by some analysts to have been exfiltrated from the NSA, by a group calling itself the Shadow Brokers.[228] The exploits reportedly incorporate zero-day vulnerabilities in networking products made by several American companies, including Cisco and Juniper – products "used by both private and government organizations around the world."[229]

On the other hand, there are instances in which the benefits of retaining a vulnerability outweigh the security costs of allowing it to persist. For example, the FBI's takedown of the notorious child-pornography

site "Playpen," which rescued "at least 26 child victims" from ongoing abuse, relied on a vulnerability in the Tor browser, although it is not known whether that flaw was a zero-day or was previously known.[230] Law enforcement and counterterrorism will only become more reliant on vulnerabilities as user-controlled strong encryption spreads.[231] If providers cannot access the content of encrypted messages, "the only way for law enforcement to read them is on the device, by essentially placing itself in the position of the end user."[232] And that will sometimes mean exploiting a vulnerability to gain access to the device.

There are instances in which the benefits of retaining a vulnerability outweigh the security costs of allowing it to persist.

In short, there is no way around the need for a case-by-case weighing of the interests at stake. In theory, the Vulnerabilities Equities Process created and later reenergized by the Obama administration reflects that need.[233] With the caveat that "there are no hard and fast rules," the White House Cybersecurity Coordinator laid out in a widely cited blog post nine factors relevant to the decision whether to disclose or retain a vulnerability.[234] That post also said that the process "is biased toward responsibly disclosing" software bugs, which accords with a recommendation of the President's Review Group.[235] NSA has said that it discloses 91 percent of the vulnerabilities it finds, although this fact alone is relatively uninformative absent more information about whether that 91 percent includes the most significant vulnerabilities and how long the NSA holds on to them before disclosing them.[236] A document declassified earlier this year provides substantial additional information about how the process is structured, albeit with extensive redactions.[237]

In practice, however, the process is widely perceived as insufficiently transparent and as likely to overvalue government interests relative to those of users and manufacturers. Most notably, the composition of the interagency Equities Review Board that decides by majority whether to withhold or disclose vulnerabilities remains classified.[238]

It is vital, as the White House Cyber Coordinator has noted, that Americans and the companies whose products are affected "have confidence in the integrity of the process" that the government "use[s] to make these decisions."[239] Today, however, "there is insufficient public information to evaluate whether the process is fairly designed ... and a lack of clarity regarding who and what is governed by it."[240]

A reform agenda for the VEP should aim to "generate public legitimacy through transparency and accountability."[241] The first step in enhancing the VEP's credibility would be formalizing the process in an executive order as part of a broader reset of the government's approach to commercial technology and risk management. As former White House cybersecurity officials Ari Schwartz and Rob Knake have explained, the current interagency agreement "does not carry the weight of an executive order signed by the president," so "there are few consequences for agencies that choose not to participate in the process."[242]

The executive order should, to the maximum extent consistent with national security, list all agencies that have a say in the process and should specifically state which agencies have a vote on whether to retain or disclose a vulnerability. To ensure that the process takes account of the broader interests of the U.S. technology sector, the Department of Commerce should have a regular seat at the table.

The executive order should also describe the "process to be followed in making a disclosure decision."[243] In particular, it should clearly state the government's substantive standard for deciding whether a vulnerability's potential national security benefits outweigh the risks of retaining it. Of course, those who apply this standard

In some instances, the benefits of retaining a vulnerability for law enforcement, foreign intelligence, or military uses will outweigh the cybersecurity risks of allowing it to remain unpatched. (Yuri Samoilov/Flickr)

will have to apply their own judgment to determine the ultimate outcome in any given case. But short of an outright ban on retaining vulnerabilities – which would endanger national security and public safety – there is no way to structure this process that avoids relying on the case-by-case discretion of those at the table.

The executive order should also require that there be periodic review of whether a retained vulnerability should be disclosed.[244] We do not believe, however, that there must be a prescribed period after which every retention decision is reviewed, other than perhaps a presumptive outer limit. As with the retention decision itself, the facts of the case – namely, the intended use and the nature of the vulnerability – may themselves suggest what a natural period for reviewing a given decision would be. When the VEP decides that a vulnerability should be retained, the agencies involved should also agree to a period after which the decision will be reviewed.

Public reports, even at a high level of generality, will enhance democratic accountability and public oversight, and thus the credibility of the process.

Finally, the executive order should provide for public annual reports containing as much detail about the process's operation as is consistent with national security, along with a classified annex for the relevant congressional committees. Under the existing process, the program's executive secretariat (at NSA) prepares and disseminates what appear to be quite detailed annual reports, but these are distributed only to the participating agencies.[245] Public reports, even at a high level of generality, will enhance democratic accountability and public oversight, and thus the credibility of the process.

These changes will not satisfy those who believe that retaining vulnerabilities is never, or almost never, appropriate. If, however, it remains government policy to retain some number of useful vulnerabilities for intelligence and law-enforcement purposes, these recommendations will do much to ensure that the process for making those decisions is relatively transparent and as credible as possible.

Mitigating the International Consequences of Surveillance Policy

The recommendations in this section address the international effects of U.S. surveillance policy. That includes diplomatic consequences, harms to the American technology sector's international prospects and preeminence, and effects on U.S. "soft power" and global influence.

The Snowden revelations triggered immediate repercussions in each of these areas. Surveillance against foreign leaders, including Germany's Angela Merkel and Brazil's Dilma Rousseff, strained diplomatic ties with affected countries.[246] U.S. companies encountered newfound skepticism from foreign customers.[247] The European Court of Justice's decision invalidating the U.S.-EU Safe Harbor agreement plunged transatlantic data transfers, and the billions of dollars in commerce dependent on them, into uncertainty.[248] Public trust of the United States declined in important allied countries.[249] Authoritarian states seized the opportunity to suggest a false moral equivalency between the United States' surveillance practices and their own.

The Obama administration took a number of important steps to attempt to repair the international consequences of the leaks: It created a new "protected list" placing certain allied leaders' private communications off-limits for the NSA.[250] It created a bilateral Cyber Dialogue with Germany, providing a forum to work through major post-Snowden disagreements.[251] It negotiated the new Privacy Shield agreement to replace Safe Harbor. Most importantly, Presidential Policy Directive 28 recognized that surveillance policy should respect the privacy interests of non-U.S. persons and required intelligence community elements to adopt policies and procedures to do so. This is a historic commitment – one matched, as far as we are aware, by no other country.

With these reforms on the books, the United States has a comparatively good story to tell on legal and institutional control over its intelligence community. Unfortunately, the actions the United States took in reaction to the post-Snowden blowback are not widely known among European publics. And European institutions have continued to pressure the United States over surveillance despite the fact that U.S. law and policy governing electronic surveillance and government access to data are stronger than analogous European restrictions. To some extent, this reflects European governing institutions' separation between national security and data privacy, both at the European and national levels. Data privacy and cross-border data transfers are subject to European Union regulation, while national security is the exclusive province of national governments. On the

MITIGATING THE INTERNATIONAL CONSEQUENCES OF SURVEILLANCE POLICY

Surveillance Diplomacy and PPD-28

- The next administration should offer to hold a political dialogue, among willing allies with similar rule-of-law cultures, on norms to govern surveillance of one another's citizens and institutions.
- This dialogue should seek to exchange high-level, public, political (rather than legal) commitments analogous to the public commitments the United States has already made, most notably in PPD-28.
- These discussions should also include mutual, public, high-level commitments about the purposes and boundaries of "liaison" cooperation between one another's intelligence services – in particular, the circumstances in which they will exchange information about one another's citizens.
- In order to encourage allied governments to enter into such discussions and extend appropriate privacy protections to the American people, the United States should make clear to allied publics and their governments that while it is prepared to commit itself to protect their privacy, the American people's privacy deserves equivalent respect and it expects such protections to be reciprocated.
- The next administration should reaffirm that PPD-28's basic recognition that signals-intelligence activities must consider the basic dignity and privacy of all people, and the fundamental commitments of Section 1 of PPD-28 (signals-intelligence activities must be be authorized by law; no use for discrimination or suppressing dissent; no espionage for commercial advantage of U.S. companies; narrow tailoring), will remain applicable to all countries and their citizens without regard to their own governments' policies.
- The new administration should announce that after one year, the heightened commitments in PPD-28 Sections 2 and 4 will be guaranteed only to citizens of countries that agree to extend comparable protection to Americans. There is no reason why other countries, and particularly U.S. allies, should resist extending to Americans the same consideration that the U.S. government grants to their citizens.
- The next administration should also offer to elevate these commitments to an executive order for countries that make credible reciprocal promises.
- The United States should insist that European Union member states grant to Americans the same judicial-redress rights and access to a surveillance "ombudsperson" that the United States extended to Europeans under Privacy Shield.
- The United States should demand that allied countries publicly commit not to spy on one another's nationals for the economic benefit of domestic companies – a practice the United States has long forsworn but some close allies have not.
- The next administration should also make clear that it will consider excluding from any list of allied leaders whose personal communications are off-limits from surveillance the leaders of any country that refuses to publicly renounce economic espionage against American companies.
- The next administration and Congress should establish regularized, formal exchanges between congressional, judicial, and executive branch compliance and oversight bodies, including the Privacy and Civil Liberties Oversight Board, and their foreign counterparts.

Public Diplomacy

- The United States should explain, in a modest and factual manner, the many ways in which the U.S. intelligence community supports Europe in its fight against terrorism.
- The intelligence community should, with as much specificity as is consistent with national security, offer greater detail about how much and what kind of counterterrorism data the United States shares with European partners, as well as the types of information it receives from them.
- The next administration should also consider raising the profile of joint counterterrorism efforts by making American ambassadors and senior national security officials available to discuss them with local media, and asking European counterparts to publicly acknowledge the cooperation.

Privacy Shield

- While legal challenges are pending, U.S. officials should seek to foster a climate conducive to ensuring that Privacy Shield passes judicial muster.
- This includes continuing to make the case that U.S. and European privacy protections are, at a minimum, "essentially equivalent."

- U.S. officials should also seek to publicly reinforce the significance of the new ombudsperson mechanism and the Judicial Redress Act.
- Consumer-protection officials should work to publicly demonstrate that Privacy Shield's consumer protections are being rigorously enforced.
- American ambassadors in Europe and visiting U.S. government principals should be encouraged to highlight U.S. privacy protections and emphasize that in the United States, as in Europe, the right to privacy is a fundamental right.
- The next administration should begin to consider what the United States' response will be, other than further concessions, if Privacy Shield is struck down.
- It should also begin communicating quietly to European partners that while the United States respects their legal institutions, shares their values, and has taken every reasonable measure to help European partners satisfy the Court of Justice, the United States has a "Plan B" and will not respond to another flawed, Schrems-like decision with more unilateral concessions.
- To amplify this message, Congress should consider legislation providing that if a judicial decision restricts data transfers from Europe to the United States, the same limitations will apply to data transfers from the United States to Europe by European companies.

Cross-Border Data Requests

- If the Justice Department's proposal does not pass during the current Congress, the next administration should seek, and Congress should enact, similar legislation authorizing executive agreements on cross-border data requests.
- Once the enabling legislation is enacted, the executive branch should move quickly to conclude executive agreements with countries with similar human-rights and rule-of-law standards.
- Legislation creating an alternative to the Mutual Legal Assistance system should be accompanied by parallel efforts to streamline the existing system.

national level, data-protection authorities are politically independent but lack authority over their own governments' national security practices.

The upshot is that the European institutions that criticize the U.S. government's surveillance practices and penalize American companies have no official responsibility to reconcile their criticisms with their own governments' comparable practices. Indeed, under European and national law, they often have no legal *authority* to do so. Even more frustrating for U.S. national security officials is that European security agencies quietly ask their American counterparts for intelligence produced by U.S. surveillance practices even as the privacy officials of the same governments are publicly blasting those practices – sometimes, we have heard, on the same day. Put simply, in many European governments, one hand does not know, or does not wish to know, what the other hand is doing.

This dissonance between European privacy policy and national security policy has hurt U.S. national interests – most notably, in the disruptive Safe Harbor decision. U.S. policy should seek to alter this status quo in three ways. First, it should seek to encourage, in an appropriate and amicable way, what should be a favorable comparison between U.S. and European legal restrictions applicable to electronic surveillance. Second, it should incentivize European governments to reconcile their own interest in preserving transatlantic data flows and U.S. investment in Europe with their data-protection authorities' and courts' apparent urge to use commerce in data as leverage to pressure the United States over surveillance. And third, it should seek to raise awareness among European publics of the ways in which the U.S. intelligence community supports their security from terrorist attacks and other threats.

Importantly, this does not mean limitless apologies or one-sided concessions. To the extent that reasonable *mutual* concessions would help further these aims, the next President should seek them. But the next administration will also be called, respectfully but firmly, to defend the United States' record and identify appropriate ways to ensure that important national interests are not imperiled by the decisions of European institutions.

SURVEILLANCE DIPLOMACY AND PPD-28

President Obama's Presidential Policy Directive 28 makes broader commitments to protect the privacy interests of foreigners in signals-intelligence collection than the policy or law of any other country of which we are aware. The closest comparable statement we have found is in Germany's recent law regulating domestic collection of foreign-foreign communications. That law

contains special protections for EU institutions, EU member states, and EU citizens, but no heightened protection for Americans.

The United States' legal and oversight regime governing domestic intelligence collection – including domestic collection against foreigners – is also equivalent to or stronger than the systems in place in leading European countries.[252] For example, only two of the leading EU member states surveyed in a review by the law firm Sidley Austin "require judicial authorization for intelligence surveillance, and most place such authorization in the hands of government ministers."[253] France, Germany, the United Kingdom, and the Netherlands all "explicitly permit certain types of surveillance that are not targeted at identified suspected individuals"[254] – that is, arguably, the type of "generalized" collection to which the Court of Justice objected in the *Schrems* decision. None of these countries' laws explicitly require minimization, and retention limits apply only to a few narrow categories of data.[255]

By contrast, in the United States all intelligence surveillance under Title I of the Foreign Intelligence Surveillance Act and criminal surveillance under the Wiretap Act (Title III) requires an individualized judicial order based on probable cause. Domestic surveillance of non-U.S. persons overseas under Section 702 requires individualized targeting, is subject to annualized judicial oversight by the Foreign Intelligence Surveillance Court, and is governed by minimization procedures that must be submitted by each participating agency and approved by the court. Even data on foreigners collected overseas is subject to a presumptive five-year retention period.[256] The United States also has robust congressional intelligence committees, "significant internal compliance and auditing mechanisms" within the executive branch, "embedded privacy and civil liberties officials and powerful and autonomous inspectors general," and the independent Privacy and Civil Liberties Oversight Board.[257]

American national security experts frequently lament that European privacy advocates criticize U.S. practices while being unaware of, or overlooking, the fact that their own intelligence agencies do similar things but are subject to fewer legal constraints and less oversight than their American counterparts. In the recent Privacy Shield negotiations, for example, EU negotiators demanded and obtained expanded rights of judicial redress in the United States for EU citizens and the creation of a State Department ombudsperson to receive Europeans' complaints about U.S. intelligence practices. Yet Americans receive none of these protections in the European Union – indeed, to the authors' knowledge, they were not offered.

Even more troubling, the United States' existing, unreciprocated concessions are not widely known abroad and have generated little goodwill for the United States. For example, one German expert told us that most Germans are "totally unaware" of PPD-28 – arguably the most significant commitment ever made by a major power to the privacy interests of foreigners. The United States should welcome a comparison between its legal and oversight regime and that of its European allies.

Fortunately, this should be an opportune time for a more mature, two-way transatlantic dialogue about surveillance. The political dynamics surrounding surveillance issues in Europe have been subtly changing, even before recent terrorist attacks. In Germany, a leader on data-privacy issues, a parliamentary committee created to investigate the NSA's activities ended up uncovering an array of controversial activities by Germany's own foreign intelligence service, the *Bundesnachrichtendienst*. This has triggered an unprecedented period of public debate and reflection about espionage and oversight. Meanwhile, in the wake of repeated terrorist attacks, public opinion in key European countries has swung dramatically toward expanded surveillance powers. France has been under a state of emergency for almost a year. In July, the United Kingdom's House of Commons passed the Investigatory Powers Bill, which gives authorities significant new surveillance powers and requires companies to help authorities break encryption in some situations.[258] Most recently, in the wake of several terrorist attacks, Germany's governing coalition has proposed a tough new set of counterterrorism measures.[259] In a Europe under regular attack by ISIS, governments are likely to conduct more surveillance and share information more widely.

The United States' legal and oversight regime governing domestic intelligence collection – including domestic collection against foreigners – is equivalent to or stronger than the systems in place in leading European countries.

Changing dynamics in Europe provide an opening for a more honest, less adversarial transatlantic dialogue on surveillance policy. (Pete Souza/Official White House Photo)

These developments have created an opportunity for a more productive, less adversarial transatlantic discussion on surveillance policy – including an honest comparison of legal and oversight regimes. The question for the next administration is how to encourage this comparison and raise awareness of the United States' record in a manner that is seen as productive and collegial rather than boastful and adversarial. One reason the commitments in PPD-28 are not widely appreciated is that they were offered as unilateral concessions rather than reciprocal exchanges between partners. Put differently, these concessions may well be more widely valued and known in Europe if Europeans were asked to give something in return.

To that end, the next administration should offer to hold a political dialogue, among willing allies with similar rule-of-law cultures, on norms to govern surveillance of one another's citizens and institutions. This differs from the recommendation of the President's Review Group that the United States seek to enter into a "very few new" bilateral "understandings or arrangements regarding intelligence collection guidelines and practices with respect to each other's citizens," analogous to the so-called Five Eyes arrangement among the United States, the U.K., Canada, Australia, and New Zealand.[260] The discussions proposed here would entail neither the detailed commitments nor the intensive intelligence coordination of the Five Eyes arrangement. Nor would they result in the type of "no-spy" agreement that Germany reportedly sought after the Snowden disclosures.

Rather, these would be high-level, public, political (rather than legal) commitments analogous to the public commitments the United States has already made, most notably in PPD-28.[261] For example, the United States should ask partners to mutually agree:

- To incorporate in their signals-intelligence practices protections for the privacy interests of one another's citizens.[262]
- To publish, with the maximum detail consistent with national security, agency procedures implementing such protections, including minimization requirements limiting the dissemination and retention of personal information of one another's citizens.[263]
- To establish a presumptive time limit for retaining the personal information of one another's citizens.[264]
- To agree to limitations on the use of signals intelligence collected in bulk.[265]
- To designate a senior official to serve as a point of contact for implementation of these commitments and other concerns related to signals-intelligence practices.[266]

- To require individualized judicial approval for electronic surveillance of one another's citizens when on the other country's territory.[267]

These negotiations would be an opportunity for the United States to demonstrate its good faith and strong bona fides on these issues, but also to subtly invite a comparison between its own practices and those of its allies. If U.S. allies are as committed to privacy as they contend, they should be eager to sign on to these commitments. If not, they should explain to their publics and the world why they refuse to.

These discussions should also include mutual, public, high-level commitments about the purposes and boundaries of "liaison" cooperation between one another's intelligence services – in particular, the circumstances in which they will exchange information about one another's citizens. While cross-border spying receives the most attention, people ultimately have the most to fear from their own governments, who after all wield direct coercive power over their lives, liberty, and property. Limits on such cooperation exist, but most are classified. More transparency would increase the democratic legitimacy of such cooperation and help dispel suspicions that services use liaison cooperation to evade their own domestic legal restrictions.

It is possible that other governments will be reluctant to enter into the type of discussions we envision here. To ensure that allied governments are adequately motivated to enter into such discussions and extend appropriate privacy protections to the American people, the United States should make clear to allied publics and their governments that while it is prepared to commit itself to protect their privacy, the American people's privacy deserves equivalent respect and it expects such protections to be reciprocated.

The new president's review of PPD-28 will provide an opportunity to give effect to this demand for reciprocity. PPD-28's basic recognition that signals-intelligence activities must consider the basic dignity and privacy of all people, and the fundamental commitments of Section 1 of PPD-28 (signals-intelligence activities must be be authorized by law; no use for discrimination or suppressing dissent; no espionage for commercial advantage of U.S. companies; narrow tailoring), should remain applicable to all countries and their citizens.

As for the heightened commitments in PPD-28 Sections 2 and 4 – for example, limits on how long intelligence agencies can retain non-U.S. persons' data – the new administration should announce that after one year, these protections will be conditioned on other governments' extending comparable protection

Joint U.K.-U.S. signals-intelligence facility at Menwith Hill, North Yorkshire, England. (Matt Crypto/Wikimedia)

to Americans. There is no reason why other countries, particularly U.S. allies, should resist extending to Americans the same consideration that the United States grants to their citizens. Indeed, the desire to retain PPD-28's protections should help stimulate in allied countries the political will to do so. The next administration should also offer to elevate PPD-28's commitments to an executive order for countries that make credible reciprocal promises.

Some might argue that adding conditionality to PPD-28 would be damaging for privacy standards globally. We understand this argument and appreciate the importance of PPD-28 for the United States' global moral authority on surveillance practices. Our hope, however, is that if this proposal were adopted, there would not be any rollback of PPD-28 because other countries would choose to retain the protection of all of its provisions by making reciprocal commitments to the American people.

Indeed, making these commitments reciprocal would substantially *enhance* privacy, for several reasons. If, as we expect, a significant number of countries accept this reciprocity and make the necessary commitments, it would be a substantial victory for privacy and surveillance under law around the world. Americans would gain new privacy protections from other governments. Citizens of other countries would gain new insights about their own governments' surveillance practices. Elevating PPD-28 to an executive order (at least for reciprocating countries) would also add a degree of permanence, enhancing its public credibility. Finally, one might argue that it would inappropriately disserve Americans' privacy to preserve these concessions for foreign citizens without using the leverage they provide to elicit equivalent protections for Americans.

There are other commitments that the authors do not believe can be made conditional, but which the United States should nonetheless make clear to its allies that it expects them to reciprocate. First, the United States should insist that EU member states grant to Americans the same judicial-redress rights and access to a surveillance ombudsperson that the United States extended to Europeans under Privacy Shield. There is no defensible ground for granting these protections to Europeans but not Americans. If the European Union wishes to deny Americans the same protections it has demanded for its own citizens, the United States should at least ensure that it is forced to publicly defend this inequity.

Second, as part of the bilateral and potentially multilateral discussions we envision, the United States should demand that allied countries publicly commit not to spy on one another's nationals for the economic benefit of domestic companies – a practice the United States has long forsworn but that some close allies have not. For example, former Secretary of Defense Robert Gates has "singled out France as particularly aggressive in its use of economic espionage."[268] The United States should not be harangued into unilateral privacy concessions by countries whose surveillance practices include "stealing American defense technology" and "bugging American business executives."[269] The next administration should also make clear that it will consider excluding from any list of allied leaders whose personal communications are off-limits from surveillance the leader of any country that refuses to publicly renounce such economic espionage against American companies. Even China has publicly promised not to conduct economic espionage for commercial advantage. It is not unreasonable to ask the same of U.S. allies.

Finally, it is not realistic or practical for the reciprocal commitments we envision to be legally binding or enforced by judicial review. For the type of high-level political commitments envisioned here, equivalently high-level political safeguards should be adequate to hold countries to their commitments, broadly speaking. The most basic protection is that such reciprocal commitments should only be made with countries that have rule-of-law and governance cultures in which such commitments are taken seriously and internally enforced. However, to reassure participating countries' publics that both countries are implementing their commitments, the next administration and Congress should establish regularized, formal exchanges between congressional, judicial, and executive branch compliance and oversight bodies, including the Privacy and Civil Liberties Oversight Board, and their foreign counterparts.

PUBLIC DIPLOMACY

Another persistent frustration we encountered among American national security officials is the discrepancy between their European counterparts' view of U.S. signals-intelligence and counterterrorism practices and European *publics'* view. European counterterrorism efforts rely heavily on data provided by the U.S. intelligence community: The United States reportedly sends to Europe vastly more counterterrorism intelligence than Europe sends back. Yet European publics hear an account of U.S. surveillance practices, including from their government officials, that is almost relentlessly negative. One senior European security official told the authors that her country's citizens do not understand the scale of American counterterrorism intelligence sharing "at all."

This has produced a warped understanding of the consequences of U.S. intelligence practices, in which privacy costs are highlighted and security gains largely ignored. Yet with jihadist attacks striking at Europe's heart, the political dynamics are changing. European leaders who three years ago felt the need to distance themselves from U.S. intelligence practices are now willing to publicly highlight enhanced intelligence sharing with the United States.[270] The United States should take this opportunity to explain, in a modest and factual manner, the many ways in which the U.S. intelligence community supports Europe in its fight against terrorism. For example, after the terrorist attacks in Paris in November 2015, the White House deployed American counterterrorism experts to European capitals "to help Western European allies shore up their defenses and borders."[271] The Brussels attacks in March and subsequent attacks in France and Germany illustrate how vital this support remains. Unfortunately, this assistance was, as *The New York Times* wrote, "little-noticed."[272]

This support is the right thing to do and should persist regardless of whether it is publicly appreciated. Yet it is in the U.S. national interest that European publics become aware of how U.S. intelligence cooperation – including intelligence generated by the NSA's electronic surveillance – helps protect them from terrorism. Skepticism about U.S. intelligence practices continues to harm the United States, as the invalidation of the Safe Harbor agreement demonstrates. Greater European public awareness of these benefits can help reduce that damaging skepticism.

Of course, a public relations tour trumpeting U.S. counterterrorism assistance would be distasteful and counterproductive. And the United States should not imply that counterterrorism is the *only* purpose of U.S.

signals-intelligence collection. That is not true, and U.S. officials would lose credibility by suggesting it. That said, counterterrorism is a central purpose, and there are ways to raise European publics' awareness of how U.S. intelligence supports their security without boasting or overstating the case. At a minimum, the intelligence community should, with as much specificity as is consistent with national security, offer greater detail about how much and what kind of counterterrorism data the United States shares with European partners, as well as the types of information it receives from them.

awareness of the relative strength of the legal restrictions on intelligence activities in the United States and Europe. The effect on the legal proceedings involving Privacy Shield would be another important benefit of such an initiative.

U.S. officials should also seek to publicly reinforce the significance of the new ombudsperson mechanism and the Judicial Redress Act, which extends to Europeans the rights Americans enjoy under the 1974 Privacy Act.[276] Consumer-protection officials should work to publicly demonstrate that Privacy Shield's consumer protections are being rigorously enforced.[277] And American ambassadors in Europe and

It is in the U.S. national interest that European publics become aware of how U.S. intelligence cooperation – including intelligence generated by the NSA's electronic surveillance – helps protect them from terrorism.

The next administration should also consider raising the profile of joint counterterrorism efforts by making American ambassadors and senior national security officials available to discuss them with local media, and asking their European counterparts to publicly acknowledge the cooperation. Public commitments regarding the purposes of intelligence cooperation and exchanges between data-protection authorities and oversight officials, both recommended elsewhere in this section, should help mitigate potential civil-liberties concerns arising from this cooperation.

PRIVACY SHIELD

Earlier this year, the United States and the European Union concluded the new Privacy Shield agreement to replace Safe Harbor. It is to be hoped that Privacy Shield will survive the European judicial review process that is now underway.[273] Billions of dollars in transatlantic commerce depend on transatlantic data transfers, and operating without the safety of Safe Harbor has proved disruptive and costly for U.S. companies. Data-protection authorities in various European companies have leapt at the opportunity to pursue enforcement actions against American companies. Some are now attacking companies' ability to use a fallback tool, standard contractual clauses, to comply with European regulations.[274]

During this period, U.S. officials should seek to foster a climate conducive to ensuring that Privacy Shield passes judicial muster. This means continuing to make the case, as government officials such as the General Counsel of the Office of the Director of National Intelligence and private actors including Peter Swire and Sidley Austin have done, that U.S. and European privacy protections are, at a minimum, "essentially equivalent," as EU law requires.[275] The diplomatic initiatives outlined here would help raise visiting U.S. principals should be encouraged to highlight U.S. privacy protections and emphasize that in the United States, as in Europe, "the right to privacy is a personal and fundamental right."[278]

Unfortunately, however, even with the best efforts of U.S. officials there remains a real prospect that Privacy Shield, like Safe Harbor, will be invalidated by the Court of Justice of the European Union. The Article 29 Working Party of European data-protection authorities, for example, has expressed concern about various aspects of the final agreement.[279] The next administration should begin to consider what the United States' response will be, other than further concessions, if Privacy Shield is struck down. The administration should also begin communicating quietly to European partners that while the United States respects their legal institutions, shares their values, and has taken every reasonable measure to help European partners satisfy the Court of Justice, the United States has a "Plan B" and will not respond to another flawed, *Schrems*-like decision with more unilateral concessions.

To amplify this message, Congress should consider legislation providing that if a judicial decision restricts data transfers from Europe to the United States, the same limitations will apply to data transfers from the United States to Europe by European companies. Traditionally, American companies have been far more data-driven – and thus more dependent on such transfers – than European companies. But as traditional industrial companies increasingly become data companies as well, this imbalance is waning. European companies such as Daimler, Mercedes, Audi, Airbus, and Siemens will be increasingly reliant on data flowing back from their products in the United States to Europe. U.S. law should reflect the fact that both sides have a strong incentive to ensure continued data flows.

CROSS-BORDER DATA REQUESTS

A final key issue is how law-enforcement agencies access data stored outside of their home country when needed for criminal investigations. There are two sides to this issue: how foreign governments access data held in the United States, and how the U.S. government accesses data stored abroad.

The question of foreign-government access to data stored in the U.S. has been percolating for several years as foreign governments have grown progressively more dissatisfied with the status quo. There are several reasons for this frustration. First, because American companies are so predominant in digital communications and social networking, they hold a huge amount of data about foreign nationals – much of which is stored in the United States. Second, U.S. law prohibits service providers from disclosing the contents of their customers' communications directly to a foreign government, even if served with valid legal process from that government.[280] (Providers are allowed to respond to foreign-government requests for stored metadata, although they are not obligated to do so.) Rather, foreign governments are told that they must make a diplomatic request for this information, employing what is known as the Mutual Legal Assistance (MLA) process. Unfortunately, that process is notoriously slow and bureaucratic.[281] The President's Review Group reported that MLA requests "appear to average approximately 10 months to fulfill, with some requests taking considerably longer."[282]

Foreign governments are naturally dissatisfied with a status quo that frustrates their time-sensitive investigations, particularly when they are investigating their own residents in connection with local crime and the only U.S. link to the data is that it happens to be stored here. As the President's Review Group noted, lengthy Mutual Legal Assistance "delays provide a rationale for new laws that require e-mail and other records to be held in the other country," "contributing to the harmful trend of [data] localization laws."[283] Alternatively, foreign governments can simply insist that U.S. companies comply with their laws even if those laws conflict directly with the companies' obligations in the United States. This leaves companies in an untenable bind. For example, when Microsoft "refused to violate U.S. law by complying with unilateral and extraterritorial Brazilian orders, government authorities in Brazil have levied fines against [Microsoft's] local subsidiary and in one case even arrested and criminally charged a local employee" of the company.[284] These delays also give foreign governments an incentive to go outside the legal system and take data surreptitiously – for example, by hacking.

To address these problems, the Justice Department recently proposed amending the Electronic Communications Privacy Act to allow American companies to respond directly to certain requests "to disclose electronic data [to] foreign governments investigating serious crime, including terrorism."[285] The legislation would permit eligible foreign governments to take these requests directly to providers rather than using the MLA process. This proposal contains several important privacy-protective limitations. It applies only to non-U.S. persons abroad; requests must be reviewed by a judge or other independent overseer; and requests must be targeted and of limited duration (that is, it forbids bulk collection).[286] Perhaps most important, however, is that to be eligible to benefit from the legislation, a foreign government will have to (i) be certified by the Attorney General and Secretary of State as satisfying various human-rights and rule-of-law standards, (ii) enter into an executive agreement with the United States, (iii) adopt privacy-protective minimization procedures limiting how data acquired through the agreement can be used, and (iv) agree to periodic compliance reviews by the United States.[287] The agreements will also be reciprocal, meaning that U.S. law enforcement would be able to make direct requests for data held by providers based in the other country, subject to analogous privacy restrictions.

The United States and the United Kingdom have reportedly been negotiating an executive agreement allowing U.K. authorities to request data from U.S. companies in qualifying investigations.[288] The legislation recently proposed by the Department of Justice is a necessary prerequisite for that agreement and others like it.

As academics Jennifer Daskal and Andrew Woods have argued, this legislation and the system of executive agreements it would permit would be significantly more privacy-protective than the status quo, particularly over the long term.[289] If foreign governments continue to be denied data that they reasonably seek for legitimate law-enforcement investigations, the inexorable result will be widespread data-localization laws and stepped-up efforts to surreptitiously access data outside of legal channels. That is, foreign governments will gain direct access to this data without any of the privacy commitments required by the draft legislation – and in a manner that is destructive for an open and free internet and for American technology companies with cross-border business models (virtually all of them).

If the Justice Department's proposal does not pass during the current Congress, the next administration should seek, and Congress should enact, similar

legislation authorizing executive agreements on cross-border data requests. Once the enabling legislation is enacted, the executive branch should move quickly to conclude executive agreements with countries with similar human-rights and rule-of-law standards.

Even with those agreements in place, however, many requests will still have to go through the traditional Mutual Legal Assistance process – and the number of MLA requests from foreign governments has been steadily rising in recent years. Accordingly, legislation creating an alternative to the Mutual Legal Assistance system should be accompanied by parallel efforts to streamline the existing system. These could include increased funding for the MLA process, an online portal and docket for MLA requests, and annual reports on the volume of MLA requests and how long they take to process.[290]

The other key issue is U.S. law enforcement's ability to access data stored outside the United States. In a widely followed case involving customer emails Microsoft had stored in Ireland, the U.S. Court of Appeals for the Second Circuit held that the government cannot force U.S.-based companies to produce customer communications stored outside the United States – even if they can access the data from the United States and the request is supported by probable cause, the standard for a search warrant under the Fourth Amendment.[291] The effect is that the U.S. government now has to use the cumbersome MLA process to obtain customer data stored overseas. In some cases, law enforcement may not be able to access the data at all – either because the relevant country does not have a functioning MLA system, or because that country does not have jurisdiction over the person or entity that can actually access the data.[292]

The Justice Department is seeking review of the *Microsoft* decision but has already announced that it intends to seek legislation addressing the decision's consequences. The parallel timing of the two issues – foreign governments' access to data held in the United States, and the U.S. government's access to data held abroad – provides an opportunity for a broader rationalization of the legal regime governing cross-border access to data. Among countries with comparable rule-of-law standards, law-enforcement access to data should turn on the location and nationality of the subject of the investigation rather than where the data happens to be stored. That principle would align access to data with real-world law-enforcement responsibilities.[293] And it would avoid creating incentives for individuals, companies, and governments to redirect data flows in ways that harm performance, functionality, and the integrity of stored data.

In practice, this could mean combining the Justice Department's proposed cross-border-data-sharing legislation with a measure giving U.S. law-enforcement agencies qualified authority to obtain warrants for data stored abroad. And because both of these measures would amend the Electronic Communications Privacy Act, they could be packaged with long-delayed legislation requiring a warrant to access the contents of Americans' stored communications and imposing reasonable limits on nondisclosure orders, which prevent companies from notifying their customers that the government is seeking their data.[294] That package should be able to pass even today's polarized Congress and would yield benefits for international comity, the U.S. technology sector, and individual privacy.

The parallel timing of the two issues – foreign governments' access to data held in the United States, and the U.S. government's access to data held abroad – provides an opportunity for a broader rationalization of the legal regime governing cross-border access to data.

Conclusion

The reform agenda outlined in this report would strengthen privacy and civil liberties, improve oversight, and enhance transparency and democratic accountability. At the same time, the authors have consciously dubbed this a *pragmatic* agenda for surveillance policy. With the United States and its allies facing a grave terrorist threat and many other pressing international challenges, it is not realistic or responsible to eliminate lawful intelligence tools that are critical to U.S. national security.

On the international front, this agenda leads with good faith efforts to find mutual agreement on controversial surveillance-policy issues. This should help rebuild diplomatic capital damaged by the Snowden leaks and protect the U.S. technology industry's ability to do business abroad. Yet this approach also recognizes the need to firmly defend U.S. interests if other powers reject these overtures or prefer to leverage surveillance disputes to serve their own interests.

The next president will take office at a time of serious terrorist threat *and* substantial public and international skepticism about U.S. surveillance practices. An approach to surveillance policy that does not adequately account for both of these factors would, at a minimum, require a heavy expenditure of the new president's scarce political capital. By contrast, a principal virtue of our approach is that instead of expending political capital, it would expand it by helping the new president establish trust and credibility with the American people, international partners, and the U.S. technology industry. And it would do so without endangering important national security capabilities.

There is a one final reason why the next president would be wise to proactively undertake a pragmatic surveillance-reform agenda like that proposed here. The Snowden disclosures were the most significant national security leaks of the digital age, but they were neither the first nor the last of their kind. The recent "Shadow Brokers" leak is yet more evidence that nothing – not even the most highly classified program – is truly secret anymore.[295] If the new administration is hit with a wave of unexpected revelations, having launched a pragmatic but forward-leaning push for surveillance reform will to some extent help protect the president from any backlash. For the good of the country – and to protect itself – the new administration should act swiftly to demonstrate its commitment to pragmatic surveillance reform.

The next president will take office at a time of serious terrorist threat* and *substantial public and international skepticism about U.S. surveillance practices.

Endnotes

1. Bruce Schneier, "Cisco Shipping Equipment to Fake Addresses to Foil NSA Interception," Schneier on Security blog on Schneier.com, March 20, 2015, https://www.schneier.com/blog/archives/2015/03/cisco_shipping_.html.

2. President Barack Obama, "Remarks by the President on Review of Signals Intelligence" (Department of Justice, Washington, Jan. 17, 2014), https://www.whitehouse.gov/the-press-office/2014/01/17/remarks-president-review-signals-intelligence.

3. Review Group on Intelligence and Communications Technologies, *Liberty and Security in a Changing World: Report and Recommendations of The President's Review Group on Intelligence and Communications Technologies (December 12, 2013), 75, https://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf.*

4. Ibid., 31–32. Internal NSA audits publicized in 2013 uncovered "a couple" instances "in the past decade" in which officers had misused agency systems to surveil former love interests – a practice colloquially known as "LOVINT." Siobhan Gorman, "NSA Officers Spy on Love Interests," *The Wall Street Journal,* August 23, 2013, http://blogs.wsj.com/washwire/2013/08/23/nsa-officers-sometimes-spy-on-love-interests/?cb=logged0.17765718392901975. Each of the miscreants "was punished either with an administrative action or termination." Ibid.

5. Yochai Benkler, "We cannot trust our government, so we must trust the technology," *The Guardian*, February 22, 2016, https://www.theguardian.com/us-news/2016/feb/22/snowden-government-trust-encryption-apple-fbi.

6. Review Group on Intelligence and Communications Technologies, *Liberty and Security in a Changing World: Report and Recommendations of The President's Review Group on Intelligence and Communications Technologies,* 6.

7. See, for example, Dena Levitz, "It's harder to build a new 'Silicon Valley' than cities think," *The Washington Post*, August 12, 2015, https://www.washingtonpost.com/posteverything/wp/2015/08/12/every-city-wants-to-create-its-own-silicon-valley-this-is-bad-for-innovation/; Carles .Buzz [sic], "We All Live in Silicon Somewhere," Motherboard.Vice.com, March 4, 2016, http://motherboard.vice.com/read/we-all-live-in-silicon-somewhere; and Shane Dingman, "What Israel's startup scene can teach the world," *The Globe and Mail*, January 22, 2016, http://www.theglobeandmail.com/report-on-business/small-business/startups/what-israels-startup-scene-can-teach-the-world/article28329835/. ("There is immense, enormous curiosity about this phenomen[on] ... this mania of creating startups.")

8. See, for example, Ben FitzGerald et al., "Open Source Software and the Department of Defense" (Center for a New American Security, August 2016), https://www.cnas.org/publications/reports/open-source-software-and-the-department-of-defense.

9. Eric Jhonsa, "Amazon, Microsoft and Google Are Breaking Away From the Pack in Cloud Infrastructure," TheStreet.com, August 6, 2016, https://www.thestreet.com/story/13667086/1/amazon-microsoft-and-google-are-breaking-away-from-the-pack-in-cloud-infrastructure.html.

10. Frank Konkel, "CIA Official: 'Cloud Has Been a Godsend,'" Nextgov.com, August 12, 2016, http://www.nextgov.com/cloud-computing/2016/08/cia-official-cloud-has-been-godsend/130716/.

11. Ibid.

12. Frank Konkel, "Amazon Launches Cloud Marketplace for Spy Agencies," Nextgov.com, April 27, 2016, http://www.nextgov.com/cloud-computing/2016/04/amazon-launches-cloud-marketplace-spy-agencies/127833/; *cf.* AWS Marketplace, https://aws.amazon.com/marketplace.

13. Ibid.

14. Christopher Stewart and Mark Maremont, "Twitter Bars Intelligence Agencies From Using Analytics Service," *The Wall Street Journal*, May 8, 2016, http://www.wsj.com/articles/twitter-bars-intelligence-agencies-from-using-analytics-service-1462751682.

15. Ibid.

16. Ibid.

17. Ryan Browne, "Top intelligence official: ISIS to attempt U.S. attacks this year," CNN.com, February 9, 2016, http://www.cnn.com/2016/02/09/politics/james-clapper-isis-syrian-refugees/; and Mark Landler, "North Korea Nuclear Threat Cited by James Clapper, Intelligence Chief," *The New York Times*, February 9, 2016, http://www.nytimes.com/2016/02/10/world/asia/north-korea-nuclear-effort-seen-as-a-top-threat-to-the-us.html.

18. See Part IV.B.

19. Review Group on Intelligence and Communications Technologies, *Liberty and Security in a Changing World: Report and Recommendations of The President's Review Group on Intelligence and Communications Technologies*, 45 ("reject[ing]" the view that society must "choose between" these values).

20. See, for example, text accompanying notes 97–112.

21. James Risen and Eric Lichtblau, "Bush Lets U.S. Spy on Callers Without Courts," *The New York Times*, December 16, 2005, http://www.nytimes.com/2005/12/16/politics/bush-lets-us-spy-on-callers-without-courts.html.

22. Public Law 110-55, *Protect America Act of 2007*, August 5, 2007; and Public Law 110-261, *FISA Amendments Act of 2008*, July 10, 2008.

23. *ACLU v. Clapper*, No. 14-42-cv, slip op. at 54 (2d Circuit, May 7, 2015) (quoting 50 U.S.C. § 1861(b)(2)(A)).

24. Ibid.

25. Ibid., *59.*

26. Ellen Nakashima, "Top spy bemoans loss of key information-gathering program," *The Washington Post*, September 9, 2015, https://www.washingtonpost.com/world/national-security/top-spy-bemoans-loss-of-key-intelligence-program/2015/09/09/a214bda4-5717-11e5-abe9-27d53f250b11_story.html.

27. Schneier, "Cisco Shipping Equipment to Fake Addresses" and text accompanying endnote 52.

28. Barton Gellman and Ashkan Soltani, "NSA infiltrates links to Yahoo, Google data centers worldwide, Snowden documents say," *The Washington Post*, October 30, 2013, 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.

29. See, for example, Brad Smith, General Counsel, Microsoft, "Protecting customer data from government snooping," December 4, 2013, http://blogs.microsoft.com/blog/2013/12/04/protecting-customer-data-from-government-snooping/; and Robert Weber, General Counsel, IBM, "A Letter to Our Clients About Government Access to Data," March 14, 2014, http://asmarterplanet.com/blog/2014/03/open-letter-data.html.

30. Google, "Transparency Report: Legal Process," https://www.google.com/transparencyreport/userdatarequests/legalprocess/; Apple, "Privacy: Government Information Requests," https://www.apple.com/privacy/government-information-requests ("When we receive information requests, we require that it be accompanied by the appropriate legal documents such as a subpoena or search warrant."); Facebook, "Information for Law Enforcement Authorities," https://www.facebook.com/safety/groups/law/guidelines/ ("We disclose account records solely in accordance with our terms of service and applicable law, including the federal Stored Communications Act. ..."); and Microsoft, *Principles, Policies and Practices FAQ,* https://www.microsoft.com/about/csr/transparencyhub/pppfaq/. ("If a government wants customer data, it needs to follow applicable legal process – meaning, it must serve us with a warrant or court order for content or a subpoena for subscriber information or other non-content data.")

31. *Microsoft v. United States*, No. 14-2985 (2d Circuit, July 14, 2016).

32. Apple, "Legal Process Guidelines: U.S. Law Enforcement" (September 29, 2015), 9, http://www.apple.com/legal/privacy/law-enforcement-guidelines-us.pdf.

33. "German Trust in United States Plummets," Spiegel.de, November 8, 2013, http://www.spiegel.de/international/germany/nsa-spying-fallout-majority-of-germans-mistrust-united-states-a-932492.html.

34. William Jordan, "World's Most Admired 2015: Angelina Jolie and Bill Gates," YouGov.co.uk, January 30, 2015, https://yougov.co.uk/news/2015/01/30/most-admired-2015/.

35. Ben Scott, "Transatlantic Digital Dialogue: Rebuilding Trust through Cooperative Reform" (The German Marshall Fund of the United States, November 5, 2015), http://www.gmfus.org/publications/transatlantic-digital-dialogue-rebuilding-trust-through-cooperative-reform.

36. See, for example, Robert Litt, "Europe's court should know the truth about US intelligence," *Financial Times,* October 5, 2015, http://www.ft.com/cms/s/0/90be63f4-6863-11e5-a57f-21b88f7d973f.html.

37. See Part IV.C.

38. Julia Fioretti and Dustin Volz, "Privacy group launches legal challenge against EU-U.S. data pact," Reuters, October 27, 2016, http://mobile.reuters.com/article/idUSKCN12Q-2JK.

39. Richard Fontaine, "Bringing Liberty Online: Reenergizing the Internet Freedom Agenda in the Post-Snowden Era" (Center for a New American Security, September 2014), https://www.cnas.org/publications/reports/bringing-liberty-online-reenergizing-the-internet-freedom-agenda-in-a-post-snowden-era.

40. Ibid.; and Adam Klein, "Decryption Mandates and Global Internet Freedom: Toward a Pragmatic Approach," Aegis Paper Series No. 1608 (Hoover Institution, September 2016), https://www.scribd.com/document/325067103/Decryption-Mandates-and-Global-Internet-Freedom-Toward-a-Pragmatic-Approach#from_embed.

41. Fontaine, "Bringing Liberty Online: Reenergizing the Internet Freedom Agenda in the Post-Snowden Era," 3.

42. Ibid., 4.

43. Claire Cain Miller, "Revelations of N.S.A. Spying Cost U.S. Tech Companies," *The New York Times*, March 21, 2014, http://www.nytimes.com/2014/03/22/business/fallout-from-snowden-hurting-bottom-line-of-tech-companies.html; and Danielle Kehl et al., "Surveillance Costs: The NSA's Impact on the Economy, Internet Freedom & Cybersecurity" (New America's Open Technology Institute, July 2014), https://static.newamerica.

org/attachments/534-surveillance-costs-the-nsas-impact-on-the-economy-internet-freedom-cybersecurity/Surveilance_Costs_Final.pdf.

44. Ibid., 10; and Alonso Soto and Brian Winter, "Saab wins Brazil jet deal after NSA spying sours Boeing bid," Reuters, December 18, 2003, http://www.reuters.com/article/brazil-jets-idUSL2N0JX17W20131219#DeFikOkt1LmAZOQG.97. #of 27 icy LandscaeAngela Merke'alogous electronic messagesto localize ata before it is encrypted or after it is decrypt

45. Daniel Castro and Alan McQuinn, "Beyond the USA Freedom Act: How U.S. Surveillance Still Subverts U.S. Competitiveness" (Information Technology & Innovation Foundation, June 2015), http://www2.itif.org/2015-beyond-usa-freedom-act.pdf?_ga=1.114044933.369159037.1433787396.

46. Ibid., 7.

47. Sam Schechner, "U.S. Tech Firms Dominate Cloud Services in Western Europe," *The Wall Street Journal*, August 4, 2016, http://www.wsj.com/articles/u-s-tech-firms-dominate-cloud-services-in-western-europe-1470303004.

48. U.S. Department of Commerce Economics & Statistics Administration, *New BEA Estimates of International Trade in Digitally Enabled Services* (May 24, 2016), http://www.esa.doc.gov/economic-briefings/new-bea-estimates-international-trade-digitally-enabled-services.

49. See, for example, Ginni Rometty, "Competitive Advantage in an Era of Innovation" (Lisbon Council, Brussels, December 7, 2013) (listing examples), 2-4, http://www.lisboncouncil.net/news-a-events/495-ibms-rometty-on-competitive-advantage-in-an-era-of-innovation.html.

50. See, for example, Deutsche Telekom, "Deutsche Telekom to act as Data Trustee for Microsoft Cloud in Germany," November 11, 2015, https://www.telekom.com/media/company/293260.

51. See, for example, Jeremy Kahn, "Amazon's Pitch to Europe: Your Data Is Safe From American Spies," Bloomberg Technology, January 7, 2016, https://www.bloomberg.com/news/articles/2016-01-07/amazon-s-pitch-to-europe-your-data-is-safe-from-american-spies.

52. Schneier, "Cisco Shipping Equipment to Fake Addresses."

53. Review Group on Intelligence and Communications Technologies, *Liberty and Security in a Changing World: Report and Recommendations of The President's Review Group on Intelligence and Communications Technologies.*

54. Ibid., 17.

55. Ibid., 36.

56. Ibid., 21.

57. Warren Strobel, "Obama prepares to boost U.S. military's cyber role: sources," Reuters, August 7, 2016, http://www.reuters.com/article/us-usa-cyber-idUSKCN10G254.

58. Available at http://fas.org/irp/offdocs/ppd/ppd-28.pdf.

59. PPD-28 § 1(a).

60. PPD-28 § 1(c).

61. PPD-28 § 4 (emphasis added).

62. Lauren Bateman, "NSA, CIA, and FBI Implementation of PPD-28," Lawfare, February 9, 2015, https://www.lawfareblog.com/nsa-cia-and-fbi-implementation-ppd-28.

63. PPD-28 § 4.

64. PPD-28 § 2.

65. PPD-28 § 4(d); and "Designation of the Senior Coordinator for International Information Technology Diplomacy," U.S. Department of State, press release, March 5, 2014, http://www.state.gov/r/pa/prs/ps/2014/03/223001.htm.

66. PPD-28 § 3.

67. Office of the Director of National Intelligence, *Signals Intelligence Reform: 2015 Anniversary Report*, http://icontherecord.tumblr.com/ppd-28/2015/privacy-civil-liberties#p-pd-28.

68. Public Law 114-23, *USA FREEDOM Act of 2015*, June 2, 2015.

69. Privacy and Civil Liberties Oversight Board, *Recommendations Assessment Report* (January 29, 2015), https://pclob.gov/library/Recommendations_Assessment-Report.pdf.

70. 50 U.S.C. § 1861(b)(2)(C), "Access to certain business records for foreign intelligence and international terrorism investigations" (emphasis added).

71. Ibid.; 50 U.S.C. § 1861(c)(2)(F)(iii)-(iv).

72. The act also prohibited the use of FISA's pen register/trap-and-trace provisions for bulk collection. Public Law 114-23, Sections 201, 501.

73. 50 U.S.C. § 1803(i), "Designation of judges."

74. United States Foreign Intelligence Surveillance Court, *Memorandum Opinion and Order (November 6, 2015)*, https://www.dni.gov/files/documents/20151106-702Mem_Opinion_Order_for_Public_Release.pdf.

75. 50 U.S.C. § 1872(a), "Declassification of significant decisions, orders, and opinions."

76. Public Law 114-23, Section 602, codified at 50 U.S.C. § 1873(b), "Annual reports."

77. Public Law 114-23, Section 602, codified at 50 U.S.C. § 1873(a).

78. Public Law 114-23, Section 603, codified at 50 U.S.C. § 1874, "Public reporting by persons subject to orders."

79. See, for example, *In re Motion for Declaratory Judgment to Disclose Aggregate Data Regarding FISA Orders and Directives*, No. 13-06, Motion of Facebook, Inc. (FISC, Sept. 9, 2013) , http://www.fisc.uscourts.gov/sites/default/files/Misc%2013-06%20Motion-3.pdf. ("Despite Facebook's efforts to push for more transparency, which have included extensive discussions with government officials, the U.S. government has taken the position that Facebook is prohibited from disclosing the specific number and type of any such requests as well as even aggregate numbers of any national security requests within ranges.")

80. *Cf.* "The Global Principles on National Security and the Right to Information (Tshwane Principles)," Paragraph 10E (June 12, 2013), https://www.opensocietyfoundations.org/sites/default/files/global-principles-national-security-10232013.pdf. ("The overall legal framework concerning surveillance of all kinds, as well as the procedures to be followed for authorizing surveillance, selecting targets of surveillance, and using, sharing, storing, and destroying intercepted material, should be accessible to the public.")

81. 50 U.S.C. § 1881a, "Procedures for targeting certain persons outside the United States other than United States persons."

82. Office of the Director of National Intelligence, *Statistical Transparency Report Regarding Use of National Security Authorities - Annual Statistics for Calendar Year 2015* (May 2, 2016), https://icontherecord.tumblr.com/transparency/odni_transparencyreport_cy2015.

83. Office of the Director of National Intelligence, *Statistical Transparency Report Regarding Use of National Security Authorities - Annual Statistics for Calendar Year 2014* (April 22, 2015), https://icontherecord.tumblr.com/transparency/odni_transparencyreport_cy2014 (92,707 targets under Section 702).

84. Office of the Director of National Intelligence, *Statistical Transparency Report Regarding Use of National Security Authorities - Annual Statistics for Calendar Year 2015*.

85. National Commission on Terrorist Attacks Upon the United States, *The 9/11 Commission Report* (2004), 395.

86. Congress later revised the board's organic statute in the implementing recommendations of the 9/11 Commission Act of 2007.

87. Privacy and Civil Liberties Oversight Board, *Recommendations Assessment Report*.

88. Privacy and Civil Liberties Oversight Board, *Recommendations Assessment Report*, 15; and Rachel L. Brand, Member, Privacy and Civil Liberties Oversight Board, testimony to the Committee on the Judiciary, U.S. Senate, May 10, 2016, 7.

89. Privacy and Civil Liberties Oversight Board, *Recommendations Assessment Report*, 20.

90. Letter from Robert Litt to Justin Antonipillai, Counselor, Department of Commerce, and Ted Dean, Deputy Assistant Secretary, International Trade Administration (February 22, 2016), 7, http://ec.europa.eu/justice/data-protection/files/privacy-shield-adequacy-decision-annex-6_en.pdf.

91. Office of the Director of National Intelligence, *Principles of Intelligence Transparency for the Intelligence Community* (February 2015), http://www.dni.gov/index.php/intelligence-community/intelligence-transparency-principles.

92. At http://icontherecord.tumblr.com/.

93. See, for example, "Joint Statement on U.S.-Germany Cyber Bilateral Meeting," U.S. Department of State, press release, March 24, 2016, https://www.state.gov/r/pa/prs/ps/2016/03/255082.htm.

94. Adam Entous and Danny Yadron, "Some Senior U.S. Officials Not Comfortable With Obama's Curbs on NSA Spying on Leaders," *The Wall Street Journal*, December 30, 2015, http://www.wsj.com/articles/some-senior-u-s-officials-not-comfortable-with-obamas-curbs-on-nsa-spying-on-leaders-1451506801.

95. John Kerry, "Remarks to the Freedom Online Coalition Conference" (via teleconference, April 28, 2014), http://www.state.gov/secretary/remarks/2014/04/225290.htm; and Scott Busby, Deputy Assistant Secretary for Democracy, Human Rights, and Labor, "Remarks on Internet Freedom" (RightsCon, San Francisco, March 4, 2014), http://www.humanrights.gov/dyn/state-department-on-internet-freedom-at-rightscon.html.

96. Joby Warrick and Karen DeYoung, "Obama Reverses Bush Policies On Detention and Interrogation," *The Washington Post*, January 23, 2009, http://www.washingtonpost.com/wp-dyn/content/article/2009/01/22/AR2009012201527.html.

97. Julian Hattem, "Surprise resignation threatens to hobble privacy watchdog," *The Hill*, April 8, 2016, http://thehill.com/policy/national-security/275545-surprise-vacancy-threatens-privacy-watchdog.

98. *Riley v. California*, 134 S. Ct. 2473 (2014).

99. 18 U.S.C. § 2703, "Required disclosure of customer communications or records"; and Richard M. Thompson II and Jared P. Cole, "Stored Communications Act: Reform of the Electronic Communications Privacy Act (ECPA)," R44036 (Congressional Research Service, May 19, 2015), https://www.fas.org/sgp/crs/misc/R44036.pdf.

100. Peter J. Henning, "The Fight Over Privacy and Secrecy in Government Investigations," *The New York Times*, May 16, 2016, http://www.nytimes.com/2016/05/17/business/

dealbook/the-fight-over-privacy-and-secrecy-in-government-investigations.html ("Why the different level of protections based on the age of the communications? Thirty years ago, Congress considered any messages over 180 days old to be abandoned, and therefore subject to reduced protection. This distinction does not make much sense now. ... ").

101. *Cf.* Digital Due Process, "ECPA Reform: Why Now?," http://www.digitaldueprocess.org. ("A particular kind of information (for example, the content of private communications) should receive the same level of protection regardless of the technology, platform or business model used to create, communicate or store it" and "regardless of how old the communication is and whether it has been 'opened' or not.")

102. *United States v. Warshak*, 631 F.3d 266 (6th Circuit, 2010).

103. *Cf. Kyllo* v. United States, 533 U.S. 27 (2001) (use of remote thermal imager to gather information about interior of a home constitutes a Fourth Amendment search).

104. H.R. 699, 114th Congress.

105 Ibid., § 4.

106. Roll Call 167, 114th Congress, 2d Session, http://clerk.house.gov/evs/2016/roll167.xml.

107. *United States v. Warshak*.

108. House Committee on the Judiciary, Report Accompanying the Email Privacy Act, H.R. Rep. No. 114-528 (2016), 9. ("Soon after the [*Warshak]* decision, the Department of Justice began using warrants for email in all criminal cases. That practice became Department policy in 2013.")

109. See, for example, Center for Democracy & Technology, "Correcting the Record: The ECTR 'Fix,'" June 27, 2016, https://cdt.org/insight/correcting-the-record-the-ectr-fix/.

110. Susan Hennessey, "DOJ Responses to FAQs on Use of National Security Letters to Obtain Electronic Communication Transaction Records," Lawfare, October 28, 2016, https://www.lawfareblog.com/doj-responses-faqs-use-national-security-letters-obtain-electronic-communication-transaction-records.

111. Letter from SEC Commissioners to Sen. Charles Grassley (May 11, 2016), http://src.bna.com/eXr.

112. Julie Brill, "It's time to update the Electronic Communications Privacy Act (ECPA)," *The Hill*, May 25, 2016, http://thehill.com/blogs/congress-blog/technology/281106-its-time-to-update-the-electronic-communications-privacy-act.

113. Chase Gunter, "Lawmakers seek controls for access to geolocation data," *FCW* (March 2, 2016), https://fcw.com/articles/2016/03/02/oversight-geolocation.aspx.

114. *Cf.* Executive Office of the President, *Big Data: Seizing Opportunities, Preserving Values (May 2014),* https://www.whitehouse.gov/sites/default/files/docs/big_data_privacy_report_may_1_2014.pdf/.

115. See, for example, *Gunte*r, "Lawmakers seek controls for access to geolocation data."

116. Mark Mazzetti and Scott Shane, "A Saudi Imam, 2 Hijackers and Lingering 9/11 Mystery," *The New York Times*, June 17, 2016, http://www.nytimes.com/2016/06/18/world/middleeast/saudi-arabia-sept11-classified-28-pages.html.

117. Mark Mazzetti, "In 9/11 Document, View of a Saudi Effort to Thwart U.S. Action on Al Qaeda," *The New York Times*, July 15, 2016, http://www.nytimes.com/2016/07/16/us/28-pages-saudi-arabia-september-11.html.

118. U.S. Department of State, *Treaty on Open Skies,* http://www.state.gov/t/avc/trty/102337.htm.

119. See generally Elizabeth Goitein, "The New Era of Secret Law" (Brennan Center for Justice, 2016), https://www.brennancenter.org/sites/default/files/publications/The_New_Era_of_Secret_Law.pdf.

120. "The Global Principles on National Security and the Right to Information (Tshwane Principles)."

121. Dakota Rudesill, "Coming to Terms with Secret Law," *Harvard National Security Journal*, 7 no. 1 (2015), 241, http://harvardnsj.org/wp-content/uploads/2016/05/Rudesill-Secret-Law.pdf.

122. 50 U.S.C. § 1881a.

123. 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), https://www.pclob.gov/library/702-Report.pdf.

124. bid., 2 (emphasis added).

125. Ibid., 10 (emphasis added).

126. Privacy and Civil Liberties Oversight Board, *Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act*, 10.

127. Office of the Director of National Intelligence, *Statistical Transparency Report Regarding Use of National Security Authorities - Annual Statistics for Calendar Year 2015*.

128. Matthew G. Olsen, Former Director of the National Counterterrorism Center, testimony to the Committee on the Judiciary, U.S. Senate, May 10, 2016, https://www.judiciary.senate.gov/imo/media/doc/05-10-16%20Olsen%20Testimony.pdf.

129. "The National Security Agency: Missions, Authorities, Oversight and Partnerships," National Security Agency, press room statement, August 9, 2013, https://www.nsa.gov/

news-features/press-room/statements/2013-08-09-the-nsa-story.shtml.

130. See, for example, United States Foreign Intelligence Surveillance Court, *Memorandum Opinion and Order.*

131. Office of the Director of National Intelligence, *Release of 2015 Section 702 Minimization Procedures* (August 11, 2016), https://icontherecord.tumblr.com/tagged/section-702.

132. Chris Inglis and Jeff Kosseff, "In Defense of FAA Section 702," Aegis Paper Series No. 1604, (Hoover Institution, 2016), 16, http://www.hoover.org/sites/default/files/research/docs/ingliskosseff_defenseof702_final_v3_digital.pdf.

133. Privacy and Civil Liberties Oversight Board, *Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act*, 59.

134. See, for example, Elizabeth Goitein, "The FBI's War. rantless Surveillance Back Door Just Opened a Little Wider," JustSecurity.org, April 21, 2016, https://www.justsecurity.org/30699/fbis-warrantless-surveillance-door-opened-wider/.

135. United States Foreign Intelligence Surveillance Court, *Memorandum Opinion and Order.*

136. Brand, testimony to the Committee on the Judiciary, 9.

137. Privacy and Civil Liberties Oversight Board, *Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act*, 56.

138. Privacy and Civil Liberties Oversight Board, *Recommendations Assessment Report*, 23–26.

139. Privacy and Civil Liberties Oversight Board, *Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act*, 147.

140. Letter from House Judiciary Committee Members to DNI James Clapper (April 22, 2016), https://assets.documentcloud.org/documents/2811050/Letter-to-Director-Clapper-4-22.pdf; and letter from privacy groups to DNI James Clapper (October 29, 2015), https://www.brennancenter.org/sites/default/files/analysis/Coalition_Letter_DNI_Clapper_102915.pdf.

141. Foreign Intelligence Surveillance Court, 2011 702 Certification Op. 34 n.32 (October 3, 2011) (per Bates, J.).

142. Letter from I. Charles McCullough III, Inspector General of the Intelligence Community, to Sens. Ron Wyden and Mark Udall (June 15, 2012), https://www.wired.com/images_blogs/dangerroom/2012/06/IC-IG-Letter.pdf.

143. Brand, testimony to the Committee on the Judiciary, 10; and United States Foreign Intelligence Surveillance Court, *Memorandum Opinion and Order*, 78.

144. Ibid., 59 (FBI records "do not identify whether the query terms are U.S. person identifiers").

145. Brand, testimony to the Committee on the Judiciary, 9.

146. "ODNI General Counsel Robert Litt Speaks on Intelligence Surveillance Reform at the Brookings Institute" (February 4, 2015), https://icontherecord.tumblr.com/post/110099240063/video-odni-general-counsel-robert-litt-speaks-on.

147. Ibid., note *.

148. Jake Laperruque, "Updates to Section 702 Minimization Rules Still Leave Loopholes," Center for Democracy & Technology, February 9, 2015, https://cdt.org/blog/updates-to-section-702-minimization-rules-still-leave-loopholes/.

149. *United States v. Nosal,* Nos. 14-10037, 10275 (9th Circuit, July 5, 2016).

150. 50 U.S.C. § 1806(c), "Use of information"; and 50 U.S.C. § 1881e(a).

151. Patrick C. Toomey, "Why Aren't Criminal Defendants Getting Notice of Section 702 Surveillance — Again?," JustSecurity.org, December 11, 2015, https://www.justsecurity.org/28256/arent-criminal-defendants-notice-section-702-surveillance-again/.

152. United States Foreign Intelligence Surveillance Court, *Memorandum Opinion and Order*; and accompanying text.

153. 50 U.S.C. § 1803(i)(2).

154. Letter from Litt to Antonipillai *and accompanying text*.

155. See, for example, Hattem, "Surprise resignation threatens to hobble privacy watchdog"; and David Medine, "The Right New Agency at the Right Time," *The Hill,* June 29, 2016, http://thehill.com/blogs/congress-blog/judicial/285184-the-right-new-agency-at-the-right-time.

156. 42 U.S.C. § 2000ee(j)(1), "Privacy and Civil Liberties Oversight Board."

157. Privacy and Civil Liberties Oversight Board, "James X. Dempsey," https://www.pclob.gov/about-us/board/dempsey.html.

158. Privacy and Civil Liberties Oversight Board, "Rachel L. Brand," https://www.pclob.gov/about-us/board/brand.html; and 42 U.S.C. § 2000ee(h)(4).

159. S. 3017, Intelligence Authorization Act for Fiscal Year 2017, 114th Cong., § 602.

160. 5 U.S.C. § 552b, "Open meetings."

161. 42 U.S.C. § 2000ee(f).

162. Patricia Wald, *Senator Chuck Grassley: Questions for the Record, 5,* https://www.judiciary.senate.gov/imo/media/doc/Wald-Reappoint-Responses-to-Grassley.pdf.

163. S. 3017 § 603, "Protection of the privacy and civil liberties of United States persons" (emphasis added).

164. See, for example, PPD-28 §5(b).

165. Center for Democracy & Technology et al., "Coalition Letter Opposing Provision of Intelligence Authorization Act on PCLOB" *(June 24, 2016)*, https://cdt.org/insight/coalition-letter-opposing-provision-of-intelligence-authorization-act-on-pclob/.

166. *Cf.* S. 3017, Intelligence Authorization Act for Fiscal Year 2017, § 601.

167. See, for example, Glenn Kessler, "Edward Snowden's claim that he had 'no proper channels' for protection as a whistleblower," *The Washington Post*, March 12, 2014, https://www.washingtonpost.com/news/fact-checker/wp/2014/03/12/edward-snowdens-claim-that-as-a-contractor-he-had-no-proper-channels-for-protection-as-a-whistleblower/.

168. Public Law 105-272, *Intelligence Authorization Act for Fiscal Year 1999*, October 20, 1998, Title VII; 50 U.S.C. § 3033, "Inspector general of the intelligence community"; and 50 U.S.C. §3234, "Prohibited personnel practices in the intelligence community."

169. The White House, *Presidential Policy Directive 19: Protecting Whistleblowers with Access to Classified Information* (October 10, 2012), http://fas.org/irp/offdocs/ppd/ppd-19.pdf; and Kessler, "Edward Snowden's claim that he had 'no proper channels' for protection as a whistleblower" (quoting Dan Meyer, Executive Director for Intelligence Community Whistleblowing and Source Protection; Office of the Intelligence Community Inspector General).

170. Joe Davidson, "Senate report hits 'inferior' FBI whistleblower procedures, citing 'numerous deficiencies,'" *The Washington Post*, June 2, 2016, https://www.washingtonpost.com/news/powerpost/wp/2016/06/02/senate-report-hits-inferior-fbi-whistleblower-procedures-citing-numerous-deficiencies/.

171. S. 2390, 114th Congress.

172. Senate Report 114-261, (May 25, 2016), 8, https://www.congress.gov/114/crpt/srpt261/CRPT-114srpt261.pdf.

173. 5 U.S.C. § 7211, "Employees' right to petition Congress."

174. 5 U.S.C. § 1213, "Provisions relating to disclosures of violations of law, gross mismanagement, and certain other matters."

175. Steven Titch, "Has the NSA Poisoned the Cloud?," Policy Study No. 17 (R Street Institute, January 2014), http://www.rstreet.org/wp-content/uploads/2014/01/RSTREET17.pdf.

176. Nicholas Weaver, "Band-Aids Can't Fix Bullet Holes: Silicon Valley and the NSA," Lawfare, September 30, 2015, https://www.lawfareblog.com/band-aids-cant-fix-bullet-holes-silicon-valley-and-nsa. ("The NSA committed at least three major acts: the battle over FISA orders against Yahoo, sabotaging US products in transit, and the bulk surveillance of Yahoo and Google's internal networks, that all represent not just attacks on Silicon Valley companies, but attacks on the very business models these companies operate on.")

177. Nathan Ingraham, "Google's Eric Schmidt: 'the solution to government surveillance is to encrypt everything,'" TheVerge.com, November 21, 2013, http://www.theverge.com/2013/11/21/5130472/googles-eric-schmidt-encrypt-everything-to-prevent-government-surveillance.

178. Danny Yadron, "Google's Schmidt Fires Back Over Encryption," *The Wall Street Journal*, October 8, 2014, http://www.wsj.com/articles/googles-schmidt-says-encrypted-phones-wont-thwart-police-1412812180.

179. Under *Riley v. California*, 134 S. Ct. 2473 (2014), law enforcement officers must obtain a search warrant to access data stored on an arrestee's cellphone.

180. Apple, "Privacy: Government Information Requests."

181. Cyrus R. Vance Jr., New York County District Attorney, "Going Dark: Encryption, Technology, and the Balance Between Public Safety and Privacy," Written Testimony to the Committee on the Judiciary, U.S. Senate, July 8, 2015, http://www.judiciary.senate.gov/imo/media/doc/07-08-15%20Vance%20Testimony.pdf; and Manhattan District Attorney's Office, *Report on Smartphone Encryption and Public Safety* (November 2015), http://manhattanda.org/sites/default/files/11.18.15%20Report%20on%20Smartphone%20Encryption%20and%20Public%20Safety.pdf.

182. Telegram FAQ, https://telegram.org/faq#q-what-is-telegram-what-do-i-do-here.

183. Kim Zetter, "Security Manual Reveals the OPSEC Advice ISIS Gives Recruits," *Wired* (November 19, 2015), http://www.wired.com/2015/11/isis-opsec-encryption-manuals-reveal-terrorist-group-security-protocols/.

184. See, for example, Warren Richey, "Terror on Twitter: How Islamic State uses social media to draw recruits," *The Christian Science Monitor*, June 3, 2015, http://www.csmonitor.com/USA/Justice/2015/0603/Terror-on-Twitter-How-Islamic-State-uses-social-media-to-draw-recruits-video.

185. Rukmini Callimachi et al., "How the Paris Attackers Honed Their Assault Through Trial and Error," *The New York Times*, November 30, 2015, http://www.nytimes.com/2015/12/01/world/europe/how-the-paris-attackers-honed-their-assault-through-trial-and-error.html.

186. Sebastian Rotella, "ISIS via WhatsApp: 'Blow Yourself Up, O Lion,'" ProPublica, July 11, 2016, https://www.propublica.org/article/isis-via-whatsapp-blow-yourself-up-o-lion.

187. Ibid.

188. "Paris, Berlin want access to encrypted apps to fight terror," Deutsche Welle, August 23, 2016, http://www.dw.com/en/paris-berlin-want-access-to-encrypted-apps-to-fight-terror/a-19495759.

189. Urs Gasser et al., "Don't Panic. Making Progress on the 'Going Dark' Debate" (Harvard University's Berkman Center for Internet & Society, February 2016), https://cyber.harvard.edu/pubrelease/dont-panic/Dont_Panic_Making_Progress_on_Going_Dark_Debate.pdf.

190. See, for example, Peter Swire, Huang Professor of Law and Ethics, Scheller College of Business, Georgia Institute of Technology, testimony to the Committee on the Judiciary, U.S. Senate, July 8, 2015, 2, https://www.judiciary.senate.gov/imo/media/doc/07-08-15%20Swire%20Testimony.pdf.

191. Vance, "Going Dark: Encryption, Technology, and the Balance Between Public Safety and Privacy."

192. See, for example, Daniel J. Weitzner, "Warning Signs: A Checklist for Recognizing Flaws of Proposed 'Exceptional Access' Systems," Lawfare, May 11, 2016, https://www.lawfareblog.com/warning-signs-checklist-recognizing-flaws-proposed-exceptional-access-systems ("History shows that even keys from governments and major companies can be stolen." (citing examples)); see generally Harold Abelson et al., "Keys Under Doormats: Mandating insecurity by requiring government access to all data and communications," MIT-CSAIL-TR-2015-026 (Massachusetts Institute of Technology's Computer Science and Artificial Intelligence Laboratory, July 6, 2015), 10, https://dspace.mit.edu/bitstream/handle/1721.1/97690/MIT-CSAIL-TR-2015-026.pdf.

193. Defense Secretary Ash Carter, "Remarks by Secretary Carter" (Commonwealth Club, San Francisco, March 1, 2016), http://www.defense.gov/News/Transcripts/Transcript-View/Article/683775/remarks-by-secretary-carter-at-the-commonwealth-club-san-francisco-california.

194. Mike McConnell, Michael Chertoff, and William Lynn, "Why the fear over ubiquitous data encryption is overblown," *The Washington Post*, July 28, 2015, https://www.washingtonpost.com/opinions/the-need-for-ubiquitous-data-encryption/2015/07/28/3d145952-324e-11e5-8353-1215475949f4_story.html.

195. Klein, "Decryption Mandates and Global Internet Freedom: Toward a Pragmatic Approach"; Frank Bajak and Jack Gillum, "Snapping up cheap spy tools, nations 'monitoring everyone,'" The Associated Press, August 2, 2016, http://bigstory.ap.org/article/f799cfd080b04b93a34df61fc007b096/snapping-cheap-spy-tools-nations-monitoring-everyone; and Andy Greenberg, "Hacking Team Breach Shows a Global Spying Firm Run Amok," *Wired* (July 6, 2015), https://www.wired.com/2015/07/hacking-team-breach-shows-global-spying-firm-run-amok/.

196. U.S. Department of State, Bureau of Democracy, Human Rights and Labor, *Request for Statements of Interest: DRL Internet Freedom Annual Program Statement* (June 13, 2016), http://www.state.gov/j/drl/p/258418.htm.

197. See, for example, Shane Huntley and Jonathan Pevarnek, "The Most Important Gmail Update You'll Hopefully Never See," Medium.com, March 24, 2016, https://medium.com/jigsaw/the-most-important-gmail-update-you-ll-hopefully-never-see-673b8ffe539e#.avh643kb1; Tor Project, "Tor: Sponsors," https://www.torproject.org/about/sponsors.html.en; and Electronic Frontier Foundation, "HTTPS Everywhere," https://www.eff.org/https-everywhere.

198. Ron Wyden, "This Isn't about One iPhone. It's About Millions of Them.," Backchannel.com, February 19, 2016, https://backchannel.com/this-isn-t-about-one-iphone-it-s-about-millions-of-them-3958bc619ea4#.dltm7ruqi. ("[I]f the FBI can force Apple to build a key, you can be sure authoritarian regimes like China and Russia will turn around and force Apple to hand it over to them.")

199. Patrick H. O'Neill, "Russian bill requires encryption backdoors in all messenger apps," The Daily Dot, June 20, 2016, http://www.dailydot.com/layer8/encryption-backdoor-russia-fsb/; Matthew Bodner, "What Russia's New Draconian Data Laws Mean for Users," *The Moscow Times*, July 12, 2016, https://themoscowtimes.com/articles/what-russias-new-draconian-data-laws-mean-for-users-54552; and Paul Mozur and Jane Perlez, "China Quietly Targets U.S. Tech Companies in Security Reviews," *The New York Times*, May 16, 2016, http://www.nytimes.com/2016/05/17/technology/china-quietly-targets-us-tech-companies-in-security-reviews.html. ("Chinese authorities are quietly scrutinizing technology products sold in China by Apple and other big foreign companies, focusing on whether they pose potential security threats to the country.")

200. See, for example, Sally Quillian Yates, Deputy Attorney General, testimony to the Committee on the Judiciary, U.S. Senate, July 8, 2015.

201. Riana Pfefferkorn, "Here's What the Burr-Feinstein Anti-Crypto Bill Gets Wrong," JustSecurity.org, April 15, 2016, https://www.justsecurity.org/30606/burr-feinstein-crypto-bill-terrible/.

202. Susan Hennessey, "Encryption Legislation: Critics Blinded by Outrage are Blinded to the Lessons," Lawfar, April 21, 2016 (emphasis added), https://www.lawfareblog.com/encryption-legislation-critics-blinded-outrage-are-blinded-lessons.

203. McConnell, Chertoff, and Lynn, "Why the fear over ubiquitous data encryption is overblown."

204. Cyrus Farivar, "FBI paid at least $1.3M for zero-day to get into San Bernardino iPhone," ArsTechnica.com, April 21, 2016, http://arstechnica.com/tech-policy/2016/04/fbi-paid-at-least-1-3m-for-zero-day-to-get-into-san-bernardino-iphone/.

205. "Read the NSC draft options paper on strategic approaches to encryption," *The Washington Post*, http://apps.washingtonpost.com/g/documents/national/read-the-nsc-draft-options-paper-on-strategic-approaches-to-encryption/1742/.

206. See, for example, *Cecilia Kang and Eric Lichtblau, "*F.B.I. Error Locked San Bernardino Attacker's iPhone," *The New York Times*, March 1, 2016 (noting that but for FBI error, Apple would have helped FBI recover shooter's data from cloud backup).

207. See, for example, Editorial Board, "The government wants social media sites to take down terrorist propaganda. Maybe they shouldn't.," *The Washington Post*, September 16, 2016, https://www.washingtonpost.com/pb/opinions/the-government-wants-social-media-sites-to-take-down-terrorist-propaganda-maybe-they-shouldnt/2016/09/16/148d75cc-7b77-11e6-ac8e-cf8e0dd91dc7_story.html.

208. National Academies, "Committee Membership Information: Law Enforcement and Intelligence Access to Plaintext Information in an Era of Widespread Strong Encryption: Options and Tradeoffs," September 7, 2016, https://www8.nationalacademies.org/cp/CommitteeView.aspx?key=49806.

209. H.R. 4651, 114th Congress (2016), https://homeland.house.gov/wp-content/uploads/2016/03/2016.03.03_HR-4651-Commission.pdf; and *"Hillary Clinton's Initiative on Technology & Innovation," HillaryClinton.com,* https://www.hillaryclinton.com/briefing/factsheets/2016/06/28/hillary-clintons-initiative-on-technology-innovation-2/.

210. Brendan Sasso, "The Hill's Newest Encryption Fight -- Over Committee Turf," GovExec.com, March 23, 2016, http://www.govexec.com/oversight/2016/03/hills-newest-encryption-fight-over-committee-turf/126895/ ("'I think the chairmen and ranking members of the two committees of jurisdiction did not feel comfortable punting on it, in their opinion, by going with the commission.'").

211. House Report 103-827, 103d Congress (1994), 16–17.

212. Computerwoche, "De Maizière plant neue Behörde für Überwachung, " June 24, 2016, http://www.computerwoche.de/a/de-maiziere-plant-neue-behoerde-fuer-ueberwachung,3312792.

213. See generally Steven Bellovin et al., "Lawful Hacking: Using Existing Vulnerabilities for Wiretapping on the Internet," *Northwestern Journal of Technology and Intellectual Property*, 12 no. 1 (2014), http://scholarlycommons.law.northwestern.edu/cgi/viewcontent.cgi?article=1209&context=njtip.

214. Review Group on Intelligence and Communications Technologies, *Liberty and Security in a Changing World: Report and Recommendations of The President's Review Group on Intelligence and Communications Technologies,* 15.

215. Hilary Tuttle, "How the NSA's First CRO is Integrating Risk Management Into National Security," *Risk Management (December 1, 2015),* http://www.rmmagazine.com/2015/12/01/mission-critical-how-the-nsas-first-cro-is-integrating-risk-management-into-national-security/.

216. "NSA Director Names New Chief Risk Officer," National Security Agency, press release, September 24, 2014, https://www.nsa.gov/news-features/press-room/press-releases/2014/new-chief-risk-officer.shtml; and Tuttle, "How the NSA's First CRO is Integrating Risk Management Into National Security."

217. Privacy and Civil Liberties Oversight Board, *Recommendations Assessment Report*, 26.

218. Michael Daniel, White House Cybersecurity Coordinator, "Heartbleed: Understanding When We Disclose Cyber Vulnerabilities" (April 28, 2014), https://www.whitehouse.gov/blog/2014/04/28/heartbleed-understanding-when-we-disclose-cyber-vulnerabilities.

219. Obama, "Remarks by the President on Review of Signals Intelligence"; and Entous and Yadron, "Some Senior U.S. Officials Not Comfortable With Obama's Curbs on NSA Spying on Leaders."

220. Bruce Schneier, "The NSA's New Risk Analysis," Schneier on Security blog on Schneier.com, October 9, 2013, https://www.schneier.com/blog/archives/2013/10/the_nsas_new_ri.html.

221. *Editorial Board,"Spying on allied leaders carries big risks: Our view," USA Today, October 24, 2013,* http://www.usatoday.com/story/opinion/2013/10/24/nsa-eavesdropping-foreign-leaders-angela-merkel-editorials-debates/3183277/.

222. For example, Barton Gellman and Ashkan Soltani, "NSA infiltrates links to Yahoo, Google data centers worldwide, Snowden documents say," *The Washington Post*, October 30, 2013, 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.

223. *Cf.* Mieke Eoyang, "Beyond Privacy and Security: The Role of the Telecommunications Industry in Electronic Surveillance," Aegis Paper Series No. 1603 (Hoover Institution, April 2016), 13, http://www.hoover.org/sites/default/files/research/docs/eoyang_privacysecurity_final_v3_digital.pdf.

224. Schneier, "Cisco Shipping Equipment to Fake Addresses."

225. Ibid.

226. Dave Aitel and Matt Tait, "Everything You Know About the Vulnerability Equities Process Is Wrong," Lawfare, August 18, 2016, https://lawfareblog.com/everything-you-know-about-vulnerability-equities-process-wrong#.

227. Daniel, "Heartbleed."

228. Andy Greenberg, "The Shadow Brokers Mess is What Happens When the NSA Hoards Zero-Days," *Wired* (August 17, 2016), https://www.wired.com/2016/08/shadow-brokers-mess-happens-nsa-hoards-zero-days/.

229. Bruce Schneier, "The NSA Is Hoarding Vulnerabilities," Schneier on Security blog on Schneier.com, August 26, 2016, https://www.schneier.com/blog/archives/2016/08/the_nsa_is_hoar.html; and Omar Santos, "The Shadow Brokers EPICBANANA and EXTRABACON Exploits," Security blog on Cisco.com, August 17, 2016, https://blogs.cisco.com/security/shadow-brokers. ("There are no workarounds for this vulnerability.")

230. Susan Hennessey and Nicholas Weaver, "A Judicial Framework for Evaluating Network Investigative Techniques," Lawfare, July 28, 2016, https://www.lawfareblog.com/judicial-framework-evaluating-network-investigative-techniques; and *Joseph Cox, "*The FBI's 'Unprecedented' Hacking Campaign Targeted Over a Thousand Computers," Motherboard.Vice.com, January 5, 2016, https://motherboard.vice.com/read/the-fbis-unprecedented-hacking-campaign-targeted-over-a-thousand-computers.

231. Aitel and t Tait, "Everything You Know About the Vulnerability Equities Process."

232. Klein, "Decryption Mandates and Global Internet Freedom: Toward a Pragmatic Approach," 6.

233. Daniel, "Heartbleed: Understanding When We Disclose Cyber Vulnerabilities"; see generally Jason Healey, "The U.S. Government and Zero-Day Vulnerabilities: From Pre-Heartbleed to Shadow Brokers," *Columbia SIPA Journal of International Affairs* (November 2016), https://jia.sipa.columbia.edu/sites/default/files/attachments/Healey%20VEP.pdf.

234. Daniel, "Heartbleed: Understanding When We Disclose Cyber Vulnerabilities."

235. Ibid.; and Review Group on Intelligence and Communications Technologies, *Liberty and Security in a Changing World: Report and Recommendations of The President's Review Group on Intelligence and Communications Technologies*, 37.

236. Don Reisinger, "NSA: We Disclose 91 Percent of Security Bugs We Find," *PC Magazine* (November 9, 2015), http://www.pcmag.com/article2/0,2817,2494740,00.asp.

237. Commercial and Government Information Technology and Industrial Control Product or System Vulnerabilities Equities Policy and Process (February 16, 2010), https://www.eff.org/document/vulnerabilities-equities-process-january-2016.

238. Ibid., 8, § 6.7(c).

239. Daniel, "Heartbleed: Understanding When We Disclose Cyber Vulnerabilities."

240. Susan Hennessey, "Vulnerabilities Equities Reform That Makes Everyone (and No One) Happy," Lawfare, July 8, 2016, https://www.lawfareblog.com/vulnerabilities-equities-reform-makes-everyone-and-no-one-happy.

241. Ibid.

242. Ari Schwartz and Rob Knake, "Government's Role in Vulnerability Disclosure: Creating a Permanent and Accountable Vulnerability Equities Process" (Belfer Center for Science and International Affairs, June 2016), http://belfercenter.ksg.harvard.edu/files/vulnerability-disclosure-web-final3.pdf.

243. Ibid., 13–14.

244. *Cf.* ibid., 15–16.

245. Commercial and Government Information Technology and Industrial Control Product or System Vulnerabilities Equities Policy and Process, 8–9.

246. See text accompanying notes 31, 42.

247. See Part II.

248. See text accompanying notes 34–35.

249. Scott Wilson and Ann Gearan, "Obama didn't know about surveillance of U.S.-allied world leaders until summer, officials say," *The Washington Post*, October 28, 2013, https://www.washingtonpost.com/politics/obama-didnt-know-about-surveillance-of-us-allied-world-leaders-until-summer-officials-say/2013/10/28/0cbacefa-4009-11e3-a751-f032898f2dbc_story.html (describing backlash in France and Spain).

250. Entous and Yadron, "Some Senior U.S. Officials Not Comfortable With Obama's Curbs on NSA Spying on Leaders"; and Review Group on Intelligence and Communications Technologies, *Liberty and Security in a Changing World: Report and Recommendations of The President's Review Group on Intelligence and Communications Technologies*, 20.

251. "Joint Statement on U.S.-Germany Cyber Bilateral Meeting"; and accompanying text.

252. Peter Swire, "US Surveillance Law, Safe Harbor, and Reforms Since 2013" (Future of Privacy Forum, December 17, 2015), Chapter 1, https://fpf.org/wp-content/uploads/2015/12/White-Paper-Swire-US-EU-Surveillance.pdf; and Jacques Bourgeois et al., "Essentially Equivalent: A comparison of the legal orders for privacy and data protection in the European Union and United States" (Sidley Austin LLP, January 2016), http://www.sidley.com/~/media/publications/essentially-equivalent---final.pdf.

253. Bourgeois et al., "Essentially Equivalent: A comparison of the legal orders for privacy and data protection in the European Union and United States," 5. The review covered Belgium, France, Germany, Italy, Ireland, the Netherlands, Poland, and the U.K. Ibid., *35.*

254. Ibid., 37.

255. Ibid., 51.

256. PPD-28, § 4.

257. Bourgeois et al., "Essentially Equivalent: A comparison of the legal orders for privacy and data protection in the European Union and United States," 6.

258. Kelly Fiveash, "Investigatory Powers Bill passes through Commons after Labour backs Tory spy law," ArsTechnica.co.uk, July 6, 2016, http://arstechnica.co.uk/tech-policy/2016/06/labour-backs-principle-of-investigatory-powers-bill/.

259. Alison Smale, "Germany Proposes Tougher Measures to Combat Terrorism," *The New York Times*, August 11, 2016, http://www.nytimes.com/2016/08/12/world/europe/germany-antiterrorism-measures.html.

260. Review Group on Intelligence and Communications Technologies, *Liberty and Security in a Changing World: Report and Recommendations of The President's Review Group on Intelligence and Communications Technologies, 20.*

261. Fontaine, "Bringing Liberty Online: Reenergizing the Internet Freedom Agenda in the Post-Snowden Era," 7. ("[T]he United States should call on other governments toembrace similar principles, or to explain why they are unwilling to do so.")

262. *Cf.* PPD-28 § 4.

263. *Cf.* IC on the Record, *Intelligence Community's Implementation of Section 4 of Presidential Policy Directive / PPD-28, Signals Intelligence Activities* (2016), https://icontherecord.tumblr.com/ppd-28/2016.

264. *Cf.* PPD-28 § 4.

265. *Cf.* PPD-28 § 2.

266 *Cf.* PPD-28 § 4(d); and "Designation of the Senior Coordinator for International Information Technology Diplomacy," U.S. Department of State, press release, March 5, 2014, http://www.state.gov/r/pa/prs/ps/2014/03/223001.htm.

267. *Cf.* 50 U.S.C. § 36, Subchapter I, "Electronic Surveillance."

268. Zachary Keck, "Robert Gates: Most Countries Conduct Economic Espionage," *The Diplomat* (May 23, 2014), http://thediplomat.com/2014/05/robert-gates-most-countries-conduct-economic-espionage/.

269. Adam Rawnsley, "Espionage? Moi?," *Foreign Policy* (July 2, 2013), http://foreignpolicy.com/2013/07/02/espionage-moi/.

270. For example, German Missions in the United States, "Interior Minister de Maizière in DC for Talks on Combatting Terrorism" (May 19, 2016), http://www.germany.info/Vertretung/usa/en/__pr/P__Wash/2016/05/19-deMaiziere-DC.html.

271. Eric Schmitt, "U.S. Officials Met With Belgians on Security Concerns Before Attacks," *The New York Times,* April 4, 2016, http://www.nytimes.com/2016/04/05/world/europe/us-security-brussels-attacks.html?_r=0.

272. Ibid.

273. Fioretti and Volz, "Privacy group launches legal challenge against EU-U.S. data pact."

274. Catherine Muyl, "EU-US Data Transfers: An update on actions taken by European DPAs," Foley Hoag Security, Privacy and the Law blog on SecurityPrivacyandtheLaw.com, June 18, 2016, http://www.securityprivacyandthelaw.com/2016/06/eu-us-data-transfers%E2%80%8E-an-update-on-actions-taken-by-european-dpas/.

275. Letter from Litt to Antonipillai and Dean; Swire, "US Surveillance Law, Safe Harbor, and Reforms Since 2013"; and Bourgeois et al., "Essentially Equivalent: A comparison of the legal orders for privacy and data protection in the European Union and United States."

276. "EU-U.S. Privacy Shield: Frequently Asked Questions," European Commission, press release, February 29, 2016, http://europa.eu/rapid/press-release_MEMO-16-434_en.htm.

277. Ibid.

278. Public Law 93-579, *The Privacy Act of 1974 (As Amended),* Section 2(a)(4).

279. Article 29 Working Party Statement on the decision of the European Commission on the EU-U.S. Privacy Shield, http://ec.europa.eu/justice/data-protection/article-29/press-material/press-release/art29_press_material/2016/20160726_wp29_wp_statement_eu_us_privacy_shield_en.pdf.

280. 18 U.S.C. § 121, "Stored Wire and Electronic Communications and Transactional Records Access."

281. Jonah Force Hill, "Problematic Alternatives: MLAT Reform for the Digital Age," *Harvard Law School National Security Journal* (January 28, 2015), http://harvardnsj.org/2015/01/problematic-alternatives-mlat-reform-for-the-digital-age/. ("The MLAT system today is deeply dysfunctional. Responses to MLAT requests for information are often abysmally slow; many of the requests are denied or only partially satisfied due to confusion over the rules governing data.")

282. Review Group on Intelligence and Communications Technologies, *Liberty and Security in a Changing World: Report and Recommendations of The President's Review Group on Intelligence and Communications Technologies*, 227.

283. Ibid.

284. Brad Smith, President and Chief Legal Officer, Microsoft Corporation, written testimony to the Judiciary Committee, U.S. House of Representatives, February 25, 2016, 3, https://judiciary.house.gov/wp-content/uploads/2016/02/brad-smith-testimony.pdf.

285. Letter from Assistant Attorney General Peter J. Kadzik to the Honorable Joseph R. Biden, President of the Senate (July 15, 2016), https://www.documentcloud.org/documents/2994379-2016-7-15-US-UK-Biden-With-Enclosures.html.

286. David Kris, "U.S. Government Presents Draft Legislation for Cross-Border Data Requests," Lawfare, July 16, 2016, https://www.lawfareblog.com/us-government-presents-draft-legislation-cross-border-data-requests.

287. U.S. Department of Justice section-by-section analysis of legislation, 3, https://www.documentcloud.org/documents/2994379-2016-7-15-US-UK-Biden-With-Enclosures.html.

288. Jennifer Daskal and Andrew Woods, "A New US-UK Data Sharing Treaty?," JustSecurity.org, June 23, 2015, https://www.justsecurity.org/24145/u-s-u-k-data-sharing-treaty/.

289. Jennifer Daskal and Andrew Keane Woods, "Congress Should Embrace the DOJ's Cross-Border Data Fix," Lawfare, August 1, 2016, https://www.lawfareblog.com/congress-should-embrace-dojs-cross-border-data-fix-0.

290. Review Group on Intelligence and Communications Technologies, *Liberty and Security in a Changing World: Report and Recommendations of The President's Review Group on Intelligence and Communications Technologies*, 227–229; LEADS Act, S. 512, 114th Congress; U.S. Department of Justice Criminal Division, *FY 2016 Budget Request, 20–29,* https://www.justice.gov/sites/default/files/jmd/pages/attachments/2015/02/02/10._criminal_division_crm.pdf; and Bryan Cunningham, "Measuring MLAT," *The Hill, June 19, 2015,* http://thehill.com/blogs/congress-blog/foreign-policy/245454-measuring-mlat.

291. *Microsoft v. United States*, No. 14-2985 (2d Cir. July 14, 2016).

292. Jennifer Daskal, "The Dangerous Implications of the Microsoft Ireland Case," JustSecurity.org, October 14, 2016, https://www.justsecurity.org/33577/dangerous-implications-microsoft-ireland-case/.

293. Andrew Keane Woods, "Reactions to the Microsoft Warrant Case," Lawfare, July 15, 2016, https://www.lawfareblog.com/reactions-microsoft-warrant-case.

294. See text accompanying notes 9–110; and Jennifer Daskal, "A New Lawsuit from Microsoft: No More Gag Orders!," JustSecurity.org, April 14, 2016, https://www.justsecurity.org/30583/challenge-microsoft-gag-orders/.

295. Greenberg, "The Shadow Brokers Mess is What Happens When the NSA Hoards Zero-Days,"; Schneier, "The NSA Is Hoarding Vulnerabilities."

About the Center for a New American Security

The mission of the Center for a New American Security (CNAS) is to develop strong, pragmatic and principled national security and defense policies. Building on the expertise and experience of its staff and advisors, CNAS engages policymakers, experts and the public with innovative, fact-based research, ideas and analysis to shape and elevate the national security debate. A key part of our mission is to inform and prepare the national security leaders of today and tomorrow.

CNAS is located in Washington, and was established in February 2007 by co-founders Kurt M. Campbell and Michèle A. Flournoy.

CNAS is a 501(c)3 tax-exempt nonprofit organization. Its research is independent and non-partisan. CNAS does not take institutional positions on policy issues. Accordingly, all views, positions, and conclusions expressed in this publication should be understood to be solely those of the authors.

1152 15th Street, NW Suite 950 Washington, DC 20005

t. **202.457.9400** | f. **202.457.9401** | **info@cnas.org** | **cnas.org**

Bold. Innovative. Bipartisan.