Global Cybersecurity, Surveillance, and Privacy: The Obama Administration's Conflicted Legacy

PETER MARGULIES*

ABSTRACT

In the wake of Edward Snowden's disclosures, the United States administration faced a daunting series of challenges on surveillance, cybersecurity, and privacy. Congress was reluctant to enact comprehensive legislation. Moreover, Snowden's revelations had triggered an international trust deficit. To deal with these challenges, the executive branch under President Barack Obama resorted to two alternatives: soft law and agency discretion. Soft law entails the issuance of non-binding policy positions and entry into nonbinding agreements with other stakeholders. In contrast, agency discretion connotes unilateral action by federal agencies.

In the soft law domain, the Obama administration sought to ease the post-Snowden trust deficit with Presidential Policy Directive No. 28, which expressly recognized global privacy rights. In collaboration with the EU, the Obama administration also crafted the Privacy Shield agreement governing U.S.-EU commercial data transfers, which created an ombudsperson in the State Department to address EU complaints about U.S. surveillance. The agency discretion model has also yielded advances on privacy. The Federal Trade Commission, for example, has implemented cybersecurity best practices through settlements with firms whose negligence resulted in data breaches.

While both soft law and agency discretion have marked virtues, they also create risks. In disputes with Microsoft regarding overseas data and with Apple about iPhone encryption, U.S law enforcement prioritized the acquisition of information needed for investigations over engagement with stakeholders. Moreover, soft law often lacks clear norms and enforcement mechanisms. For example, the Privacy Shield

* Professor Law, Roger Williams University School of Law; B.A., Colgate, 1978; J.D., Columbia, 1981.

Indiana Journal of Global Legal Studies Vol. 24 #2 (Summer 2017)
© Indiana University Maurer School of Law

agreement lacks specificity on the ombudsperson's powers, which may blunt the ombudsperson's ability to check the U.S. intelligence community.

To analyze the Obama administration's cyber efforts, this Article proposes a paradigm of stewardship with both discursive and structural dimensions. Discursive stewardship refers to the Executive's openness to dialogue with other stakeholders. Structural stewardship refers to the domestic and transnational distribution of decisional authority, including checks and balances that guard against the excesses of unilateral action. The Article concludes that the Obama administration made substantial progress in each of these realms. However, the outsized role of law enforcement agendas and dearth of clearly articulated checks on transnational surveillance drove headwinds that limited forward movement.

INTRODUCTION

In setting policy on surveillance and cybersecurity, President Barack Obama's administration faced substantial obstacles. The most obvious example was Congress's reluctance to enact comprehensive legislation. The second obstacle, particularly after Edward Snowden's revelations about U.S. surveillance in 2013, was an international trust deficit. Both legislative reluctance and the post-Snowden trust deficit are problems for the United States' global stance, since issues like cybersecurity and surveillance have international ramifications. For example, U.S. surveillance of residents of foreign states can affect privacy rights established by transnational agreements. Moreover, law enforcement agencies' requests for data can affect software and web-related services that are international in their scale and scope. The combination of legislative reluctance and the post-Snowden trust deficit challenged the Obama administration's efforts at every turn.

To deal with these challenges, the executive branch under President Obama often resorted to two alternatives: soft law and agency discretion. Soft law entails the issuance of nonbinding policy positions and entry into nonbinding agreements.[1] Soft law recognizes a spectrum of stakeholders, including foreign states, corporations, and technologists concerned with internet security and governance. In contrast, agency discretion connotes unilateral action by federal agencies, including independent agencies, such as the Federal Trade Commission (FTC), and cabinet departments or components of those departments, such as

1. *See* JEFFREY L. DUNOFF, STEVEN R. RATNER & DAVID WIPPMAN, INTERNATIONAL LAW NORMS, ACTORS, PROCESS: A PROBLEM-ORIENTED APPROACH 89 (4th ed. 2015).

the Federal Bureau of Investigation (FBI) and the Department of Justice (DOJ). Stakeholders tend to have less input into measures driven by agency discretion. Consider a law enforcement agency such as the FBI. While the FBI routinely partners with state or city law enforcement entities, it has rarely engaged in policy dialogue with global non-law-enforcement stakeholders.[2]

While both soft law and agency discretion have marked virtues, they also have liabilities. Unfortunately, because of the post-Snowden trust deficit, transnational governance entities such as the Court of Justice of the European Union (CJEU) have often discounted the virtues for privacy of both the soft law and agency discretion models.[3] Instead, transnational entities have stressed those models' privacy risks.

The biggest cost of the agency discretion model is structural: the model's lack of harmonization with legislatively mandated frameworks. Two clear examples are the Microsoft Ireland dispute[4] and the FBI's

---

2. Technology firms such as Apple believe that the FBI has not engaged in sufficient dialogue on overarching policy issues such as law enforcement access to data on encrypted smartphones. In contrast, then-FBI Director James Comey believed that technology firms' increasing turn toward encryption as a product feature threatened to undermine the criminal justice framework for accountability of wrongdoers. *See* Samuel J. Rascoff, *Presidential Intelligence*, 129 HARV. L. REV. 633, 664–65 (2016). Collaboration on other issues is a mainstay of federal law enforcement. For example, FBI personnel regularly collaborate with private sector stakeholders on issues such as cybersecurity threats. *See* John P. Carlin, *Detect, Disrupt, Deter: A Whole-of-Government Approach to National Security Cyber Threats*, 7 HARV. NAT'L SECURITY J. 391, 417 (2016) (noting that the FBI has a "long history of working with private sector victims of criminal activity" in the cyber arena). Unfortunately, this collaboration has been uneven. Reports indicate that the FBI was not sufficiently proactive in informing the U.S. Democratic National Committee (DNC) about successful hacking efforts that U.S. officials have attributed to Russia in connection with the 2016 U.S. election. *See* Eric Lipton et al., *Hacking the Democrats*, N.Y. TIMES, Dec. 14, 2016, at A1 (reporting that the FBI failed for months to contact senior DNC officials about the hack and instead only sought to inform a low-level DNC information technology contractor).

3. *See* Case C-362/14, Schrems v. Data Protection Comm'r, http://curia.europa.eu/juris/document/document.jsf?text=&docid=168421&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=157889 [hereinafter *Schrems*] (striking down U.S.-EU data transfer agreement because of concerns about scope and operation of U.S. surveillance).

4. *See* Microsoft Corp. v. United States, 829 F.3d 197, 216 (2d Cir. 2016) [hereinafter Microsoft Ireland] (concluding "that Congress did not intend the [Stored Communications Act's] warrant provisions to apply extraterritorially"). *See generally* Jennifer Daskal, *Law Enforcement Access to Data Across Borders: The Evolving Security and Rights Issues*, 8 J. NAT'L SECURITY L. & POL'Y 473 (2016) [hereinafter Daskal, *Law Enforcement*] (exploring the complexities of managing data across international borders). *Compare* Jennifer Daskal, *The Un-Territoriality of Data*, 125 YALE L.J. 326, 331–32 (2015) [hereinafter Daskal, *Un-Territoriality*] (contending that the Internet has displaced venerable notions of jurisdiction and sovereignty), *with* Andrew Keane Woods, *Against Data Exceptionalism*, 68 STAN. L. REV. 729, 735 (2016) (asserting that challenges presented by the Internet can be addressed within established legal frameworks).

dispute with Apple over disabling security features of the iPhone used by one of the shooters in the San Bernardino terrorist attack.[5] In seeking relief under the All Writs Act[6] in the latter case, the government's position unduly discounted the framework of the Communications Assistance for Law Enforcement Act (CALEA).[7] CALEA imposed substantial limits on firms' required assistance, including denying the government the power to force changes in product design. Enlisting the All Writs Act in the effort to force Apple to comply with the government's request circumvented those carefully crafted limits. Moreover, the government's stance alienated a large cohort of technology experts who believed that the government's approach would damage the crucial public good of internet security—the ability of the Internet to support the global exchange of ideas without disruption, inappropriate surveillance, or theft of data.

In the Microsoft Ireland case,[8] the structural issues with the government's contentions had an even more marked effect on foreign affairs. The government argued that the Stored Communications Act (SCA)[9] gave the government the ability to obtain a warrant for data stored abroad. In making this argument, the government failed to acknowledge the legal backdrop for the Act, which treated warrants as only available domestically absent an express congressional provision for extraterritorial reach. The government's gambit also ignored the structure of mutual legal assistance treaties (MLATs), which are treaties entered into bilaterally to facilitate exchanges of data and other matters relevant to criminal prosecutions. While MLATs are cumbersome, the remedy for this inefficiency is new legislation and/or

---

5. *See* Danny Yadron, *San Bernardino iPhone: US Ends Apple Case After Accessing Data Without Assistance*, THE GUARDIAN (Mar. 29, 2016, 2:24 PM), https://www.theguardian.com/technology/2016/mar/28/apple-fbi-case-dropped-san-bernardino-iphone. A U.S. magistrate in New York analyzed a similar issue as the San Bernardino dispute was pending. *See In re* Apple, Inc., 149 F. Supp. 3d 341, 344 (E.D.N.Y. 2016).

6. 28 U.S.C. § 1651(a) (2012).

7. 47 U.S.C. §§ 1001–1010 (2012). This Article's principal concern with the Apple case is the government's choice of legal arguments. The government did not seek to unilaterally force Apple to comply with its request. Instead, the government sought a court order. In this sense, the government's position did not raise the structural concerns regarding the separation of powers that a unilateral executive action would have engendered. However, in the broader structural sense used in this Article, the government's choice of litigating positions was still problematic.

8. *Microsoft*, 829 F.3d at 197.

9. *See* 18 U.S.C. §§ 2701–2712 (2012). For a guide on how to properly construe the SCA, see Orin S. Kerr, *A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It*, 72 GEO. WASH. L. REV. 1208, 1215–16 (2004).

reform of the MLAT process, not an end run around a long-established course of dealing.[10]

In the soft law area, the government's biggest international innovation has been the new Privacy Shield agreement,[11] which replaced the Safe Harbor agreement struck down by the CJEU on privacy grounds in *Schrems v. Data Protection Commissioner*.[12] In governing commercial data transfer between the United States and European Union, the Privacy Shield agreement commits the United States to set up an office of the ombudsperson in the State Department to address EU complaints about U.S. surveillance's impacts on EU residents. However, the Privacy Shield agreement lacks specificity on the ombudsperson's powers and responsibilities. That lack of binding rules, a characteristic of soft law, may impede the ombudsperson's ability to check the U.S. intelligence community.

The trust deficit prompted by Edward Snowden's revelations has exacerbated the problems of both the agency discretion and soft law paradigms. This trust deficit drove the CJEU's decision in *Schrems*. Because of the post-Snowden trust deficit, the CJEU failed to adequately acknowledge checks on U.S. surveillance. The CJEU also failed to accord appropriate deference—what the European Court of Human Rights (ECHR) has called a "margin of appreciation"[13]—to the combined judgment of EU member states and the United States that the Safe Harbor data-transfer agreement contained sufficient safeguards.[14] In addition, the post-Snowden trust deficit set the stage

10. To its credit, the Justice Department has proposed reform legislation. *See* Jennifer Daskal & Andrew K. Woods, *Congress Should Embrace the DOJ's Cross-Border Data Fix*, JUST SECURITY (Aug. 31, 2016, 8:03 AM), https://www.justsecurity.org/32213/congress-embrace-dojs-cross-border-data-fix/.

11. *See* Commission Implementing Decision (EU) No. 2016/1250 of 12 July 2016, 2016 O.J. (L 207) 1 [hereinafter EC Adequacy Decision].

12. *Schrems*, *supra* note 3. *See also* Case C-203/15, Tele2 Sverige AB v. Post –och Telestyrelsen, http://curia.europa.eu/juris/document/document.jsf?text=&docid=186492&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=82797 [hereinafter *Tele2 Sverige*] (invalidating United Kingdom and Swedish data retention laws on grounds that these measures violated EU privacy laws by requiring telecommunications firms to retain all call-record data for specific period).

13. *See* Handyside v. United Kingdom, 24 Eur. Ct. H.R. (ser. A) at 21–22 (1976) (regulating public dissemination of information about human sexuality to protect children); *see also* Robert D. Sloane, *Human Rights for Hedgehogs?: Global Value Pluralism, International Law, and Some Reservations of the Fox*, 90 B.U. L. REV. 975, 983 (2010) (observing that the ECHR grants states "a 'margin of appreciation' within which to implement or interpret human rights in ways that may be sensitive or responsive to prevailing social, cultural, and other norms within their polities").

14. The CJEU also failed to exhibit a measure of difference in its opinion in Tele2 Sverige v. Post –och telestyrelsen. *See Tele2 Sverige*, *supra* note 12 (striking down UK and Swedish data retention laws).

for the confrontations between U.S. law enforcement and technology firms in the Apple and Microsoft Ireland cases.

One solution is a new stewardship approach.[15] Stewardship of the Internet is an old idea. Historically, Internet stewardship has referred largely to strengthening the technical aspects of internet operation and governance. On this view of stewardship, the ease of communication and access to information engendered by the Internet embody a global public good, which states should nurture. Concern for maintaining the Internet's virtues should prompt opposition to regimes that stifle or erode these virtues in the absence of compelling reasons. Maintaining the Internet's virtues also requires ensuring a threshold level of privacy safeguards to ensure that the chill posed by public exposure or state retaliation does not inhibit communication.

Despite its strengths, this notion of internet stewardship fails to adequately acknowledge that the Internet is subject to a range of threats, including state and nonstate actors who use the Internet's tools to promote more parochial agendas, such as identity theft, extortion, and political influence.[16] A renewed vision of stewardship must accommodate reasonable state and transnational action to address these threats. However, that vision should not sacrifice the Internet's virtues.

The public-good account of Internet stewardship would benefit from integration with broader legal and political notions of governance. For example, technical stewardship of the Internet overlaps with legal grounds for U.S. surveillance in the domestic and transnational realms. Similarly, the public-good account of internet stewardship must reckon with law enforcement access to transnational encrypted data. In each of these contexts, issues of the separation of powers and human rights are also salient. The CJEU in *Schrems v. Data Commissioner* asserted that EU privacy guarantees clashed with an EU-U.S. commercial data transfer agreement that allowed U.S. surveillance.[17] An adequate conception of stewardship should address the CJEU's concerns about the scope and reviewability of U.S. surveillance. It should also fashion

---

15. *See generally* Peter Margulies, *Taking Care of Immigration Law: Presidential Stewardship, Prosecutorial Discretion, and the Separation of Powers*, 94 B.U. L. REV. 105 (2014) (analyzing the scope and derivation of the President's provisional power—specifically as it relates to Barack Obama's initiative Deferred Action for Childhood Arrivals (DACA)—by building on the stewardship theory advanced by Theodore Roosevelt).

16. *See generally* David E. Pozen, *Privacy-Privacy Tradeoffs*, 83 U. CHI. L. REV. 221 (2016) (exploring the conflicts between privacy and itself by introducing the phenomenon of privacy-privacy tradeoffs, with particular attention to their role in NSA surveillance).

17. *See Schrems*, *supra* note 3, at ¶¶ 28, 30.

appropriate limits on the authority of transnational tribunals such as the CJEU.

The new stewardship envisioned here supplements the technical aspect of the traditional model with a discursive and structural dimension. Discursive stewardship refers to the Executive's openness to dialogue with other stakeholders, such as foreign states, transnational organizations like the United Nations and the European Union, private firms, and scholars. Structural stewardship refers to the domestic and transnational distribution of decisional authority, including checks and balances that guard against unilateral action by any one stakeholder.

Viewed from the stewardship standpoint, the Obama administration's record has been mixed. The administration made substantial strides in the discursive realm through soft law initiatives. That record includes the post-Snowden issuance of Presidential Policy Directive Number 28[18] with its recognition of global privacy rights and unprecedented transparency about intelligence collection. It also includes the Obama administration's use of the Commerce Department's National Institute for Standards and Technology (NIST) to develop consensus on cybersecurity best practices[19] and its establishment of a Vulnerabilities Equities Process (VEP)[20] to weigh the security and law enforcement benefits of exploiting flaws in internet software against the virtues of disclosure of such flaws to manufacturers.

However, the Obama administration's record on discursive and structural stewardship is imperfect. In the discursive realm, the FBI's conspicuous cavils about encryption and "going dark" have injected a dissonant note. In the realm of structure, both the government's positions in the Apple and Microsoft Ireland cases and the administration's reluctance to include robust safeguards in the new U.S.-EU Privacy Shield data transfer agreement have been problematic.

While the conception of stewardship advanced here evaluates the Obama administration's initiatives, this conception is relevant to any administration. The Trump administration could conceivably improve on the Obama administration's record. President Trump's criticism of the Obama administration's unilateral action in other spheres, such as

18. *See* PRESIDENTIAL POLICY DIRECTIVE/PPD-28 (Jan. 17, 2014) [hereinafter PPD-28] (promulgating certain policies for safeguarding personal information).

19. *Framework for Improving Critical Infrastructure Cybersecurity*, NAT'L INST. STANDARDS & TECHNOLOGY (Feb. 12, 2014), https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf.

20. *See* ARI SCHWARTZ & ROB KNAKE, GOVERNMENT'S ROLE IN VULNERABILITY DISCLOSURE: CREATING A PERMANENT AND ACCOUNTABLE VULNERABILITY EQUITIES PROCESS 1–2 (2016), http://www.belfercenter.org/sites/default/files/legacy/files/Vulnerability%20Disclosure%20Web-Final4.pdf.

immigration, may bode well in this regard. On issues such as encryption, it is possible that President Trump's business background will make him more attuned to the positions of technology firms. On the other hand, as a candidate, Donald Trump criticized Apple for refusing to decrypt the San Bernardino shooter's iPhone.[21] This may herald Trump administration efforts to rein in pro-privacy agencies such as the FTC and weaken safeguards in soft law frameworks such as Privacy Shield. As of December 2016, all we can say for sure is that the future is highly uncertain.

This Article is in three Parts. Part I analyzes soft law, including the U.S.-EU Privacy Shield agreement, the NIST cybersecurity standards, and the VEP. Part II discusses the agency discretion model and notes U.S. law enforcement's aggressive performance in that role. Part III describes the new stewardship paradigm, analyzing the Obama administration's performance along discursive and structural lines. It acknowledges the Obama administration's successes, particularly those in the realm of discursive stewardship, but it notes that sweeping law enforcement rhetoric and policy discretion complicated the Administration's stewardship mission. This Part argues that effective stewardship requires more stakeholder input. However, when stakeholders weigh in, courts should respect the outputs of such deliberations. Transnational tribunals such as the CJEU could bolster sound executive stewardship by granting transnational arrangements, such as Privacy Shield, a measure of deference.

I. PRIVACY, SURVEILLANCE, AND SOFT LAW

Because of the difficulty of persuading Congress to enact comprehensive legislation on cybersecurity and the Internet, the Obama administration turned increasingly to "soft law," which is a term used by international law scholars to connote a broad range of "quasi-legal instruments" that lack the formality and institutional pedigree of statutes and treaties.[22] Soft law need not be passed by Congress or signed by the President. In the international domain, soft law need not be formally ratified by states or approved by the Security Council. Hence, soft law is not legally binding on the states that agree to it.

21. Jack Detsch, *Apple v. FBI Case on Hold, but 'Going Dark' Debate Rages On*, CHRISTIAN SCI. MONITOR, (Mar. 22, 2016), http://www.csmonitor.com/World/Passcode/2016/0322/Apple-v.-FBI-case-on-hold-but-going-dark-debate-rages-on.

22. *See* DUNOFF ET AL., *supra* note 1, at 89; Andrew T. Guzman & Timothy L. Meyer, *International Soft Law*, 2 J. LEGAL ANALYSIS 171, 172 (2010).

Rather, soft law often articulates best practices that reflect consensus between multiple stakeholders.[23]

One virtue of soft law is its flexibility—states can experiment with commitments to changing norms without the irrevocability that stems from "hard law," such as treaties. In multistakeholder conversations, states can develop a vocabulary to describe such norms and forms of practice that implement that guidance. Moreover, in a state in which a treaty involves buy-in by disparate political institutions, such as the President and two-thirds of the U.S. Senate, soft law can mute or diffuse political dynamics that make treaty approval difficult. In the United States, legislative reluctance to even appear to surrender sovereign decision making to an international framework has impaired prospects for approval of human rights treaties. Similar dynamics have frustrated enactment of statutes dealing with matters of international moment, such as the technology issues studied in this Article. Nonbinding agreements such as the climate change agreements that the Obama administration entered into are a form of soft law that copes with the effects of political paralysis.

Having noted soft law's virtues, we should also attend to its drawbacks. While soft law provides states with multiple opportunities to articulate emerging norms, soft law is notably short on mechanisms for *enforcing* those norms. That nonbinding character is one of soft law's charms but also its cardinal weakness. If a state decides to shirk its soft law duties, other states can seek to shame the defaulting state into compliance.[24] However, this reputational dynamic can take some time to work. Moreover, it may not stop backsliding by officials concerned about domestic political forces or exigent national security interests. The Snowden disclosures illustrated the latter concern, spurring a trust deficit that soft law cannot fully erase.

Despite its flaws, soft law is still a valuable path to crafting and implementing best practices. Guidance about best practices can issue from a single state, an industry group, or an international organization.[25] For example, U.N. General Assembly resolutions are typically considered soft law.[26] So are industry codes of conduct such as

23. *Id*.

24. *See* Guzman & Meyer, *supra* note 21, at 177; *see also* David H. Moore, *A Signaling Theory of Human Rights Compliance*, 97 NW. U. L. REV. 879, 879, 881–82 n.17 (2003); Harold Hongju Koh, *Why Do Nations Obey International Law?*, 106 YALE L.J. 2599, 2602–03 (1997).

25. *See* DUNOFF ET AL., *supra* note 1, at 89–90.

26. *See id.* at 90.

the guidance proposed by the apparel industry to regulate global working conditions, including child labor.[27]

The Obama administration's approach to cybersecurity and surveillance has many of the benefits of soft law. It signals a penchant for collaboration, instead of exhibiting arrogance. Moreover, to the extent that soft law comes to represent ongoing practice, it can establish habits that eventually congeal into "hard" law. Customary international law (CIL) works in this way, and that is generally considered one of CIL's strengths.[28] On the minus side, soft law can sometimes distract from the need for hard law and prove to be an inadequate substitute. This is of particular concern when soft law provides flexibility that allows states to slide off the hook, instead of making the firm commitments that hard law requires.

As an example of the Obama administration's soft law approach, consider the Cybersecurity Executive Order[29] and the Cybersecurity Framework.[30] The Cybersecurity Framework was the culmination of a process triggered by the Executive Order. Each stemmed from concern that U.S. critical infrastructure, including the energy and financial sectors, faced a burgeoning array of threats from cyberspace, including the risk of incursions from foreign states and cyber criminals. These threats could result in massive data breaches, such as the hacking of the U.S. Office of Personnel Management[31] or private firms such as Target.[32] Moreover, a cyber attack posed a risk to the operation of the U.S. power grid, banking system, and other critical functions.[33] A cyber attack could cause massive blackouts or disrupt financial transactions and the sale of corporate securities. While many responsible public officials, including executive branch personnel and members of Congress, urged comprehensive cybersecurity legislation to address

27. *See id.*; *see also* Jacob E. Gersen & Eric A. Posner, *Soft Law: Lessons from Congressional Practice*, 61 STAN. L. REV. 573, 606–07 (2008) (describing Congress's use of soft law approach to express its view or mobilize political pressure against executive action).

28. *See* Koh, *supra* note 23, at 2655.

29. Exec. Order No. 13,636, 78 Fed. Reg. 11,739 (Feb. 12, 2013).

30. *See Framework for Improving Critical Infrastructure Cybersecurity*, *supra* note 18.

31. *See* Laura DeNardis, *Five Destabilizing Trends in Internet Governance*, 12 J. L. & POL'Y INFO. SOC'Y 113, 120 (2016).

32. *Id.* at 119. More recently, U.S. officials have raised concerns about alleged Russian hacks of the email system of the Democratic National Committee during the 2016 elections. *See* Jennifer Steinhauer, *G.O.P. Feud Looms as Leaders Back Russia Inquiries*, N.Y. TIMES, Dec. 13, 2016, at A1.

33. *See* Scott J. Shackelford et al., *Toward a Global Cybersecurity Standard of Care?: Exploring the Implications of the 2014 NIST Cybersecurity Framework on Shaping Reasonable National and International Cybersecurity Practices*, 50 TEX. INT'L L.J. 303, 305, 308 (2015).

these threats, Congress was too splintered to agree on a legislative package.[34] The Obama administration sought to fill the void with soft law.

The framework drafted pursuant to President Obama's Executive Order emerged from a dialogue among stakeholders, including businesses, NGOs, and technological experts. The dialogue was convened under the auspices of the Commerce Department's National Institute for Standards and Technology (NIST), which enjoyed a venerable reputation for bipartisan and principled standards setting.[35] Because cybersecurity necessarily includes accounting for risks posed by foreign state and nonstate actors, the NIST process was inherently transnational in focus. Moreover, many of the stakeholders in the process, including multinational corporations, had their eye on global conditions. The result of this process was a consensus on best practices regarding cybersecurity, such as protecting networks through the comprehensive use of robust passwords, developing methods for detecting and addressing cyber threats, sharing information with other stakeholders, protecting privacy and civil liberties, and training employees.[36]

Moreover, while the Obama administration could not persuade Congress to pass comprehensive cybersecurity legislation, it did play a vital role in enacting the Cybersecurity Information Sharing Act of 2015 (CISA).[37] CISA encouraged the sharing of information between

---

34. *Cf.* Kristen E. Eichensehr, *Public-Private Cybersecurity*, 95 TEX. L. REV. (forthcoming 2017) (suggesting that government regulation is complicated by government's interest in maintaining special access to private data for national security and law enforcement purposes by exploiting flaws in internet software at the cost of increasing cybersecurity risks to ordinary consumers); Nathan Alexander Sales, *Regulating Cyber-Security*, 107 NW. U.L. REV. 1503, 1515-18 (2013) (suggesting that regulation may be appropriate when market fails to prod firms to invest sufficiently in cybersecurity). On the utility of cybersecurity regulatory legislation, compare PAUL ROSENZWEIG, CYBERSECURITY AND PUBLIC GOODS: THE PUBLIC/PRIVATE "PARTNERSHIP" (2011), http://media.hoover.org/sites/default/files/documents/EmergingThreats_Rosenzweig.pdf (expressing concern that cybersecurity regulation will lock in technology firms to obsolete standards), with Jack Goldsmith, *Response to Paul on Cyber-Regulation for Critical Infrastructure*, LAWFARE (May 21, 2012, 12:11 PM), https://www.lawfareblog.com/response-paul-cyber-regulation-critical-infrastructure (arguing that regulation is necessary to curb the selfish behavior that impairs the public good of cybersecurity).

35. *See* Shackelford et al., *supra* note 32, at 306.

36. *See id.*

37. *See* Consolidated Appropriations Act of 2016, Pub. L. No. 114-113, div. N., title I, 129 Stat. 2242, 2936 (2015) (codified at 6 U.S.C. §§ 1501-1510 (2015)); *see also* Carlin, *supra* note 2, at 434 (discussing CISA); Susan Hennessey, *The Problems CISA Solves: ECPA Reform in Disguise*, LAWFARE (Dec. 23, 2015, 2:19 PM), https://www.lawfareblog.com/p

government and the private sector and gave businesses a safe harbor from privacy law restrictions for disclosing data about serious threats. Implementation of the statute reflected the same commitment to a multistakeholder approach.

To implement CISA, both the Department of Homeland Security (DHS) and the Department of Justice (DOJ) solicited input from private firms, scholars, and privacy and civil liberties advocates.[38] The approach taken by DHS and DOJ may not have appealed equally to each of these constituencies. For example, government agencies and private firms opted to permit more flexibility on the sharing of personal information as long as that information related to a cybersecurity threat.[39] Privacy advocates wanted more protection for such information.[40] However, more privacy safeguards would have had costs, since they would have hampered the information sharing that the legislation sought to promote. Privacy advocates failed to fully acknowledge that cybersecurity threats jeopardize individuals' privacy interests, since cyber criminals seek to harvest vast amounts of personal data for identity theft.[41] Curbing such threats relieves a major privacy concern. More onerous restrictions on information sharing would have ceded the initiative to cyber criminals who already benefit from the element of surprise. In this sense, CISA implementation reflected difficult but reasonable trade-offs among a range of stakeholder positions, where no single stakeholder had all the answers.

The same commitment to input from multiple stakeholders also characterized the Obama administration's responses to Edward Snowden's disclosures.[42] In January 2014, President Obama issued

---

roblems-cisa-solves-ecpa-reform-disguise (discussing CISA's operation and constraints that minimize threats to privacy when firms and government share data about cyber threats).

38. *See* Carlin, *supra* note 2, at 434–35, 434 n.179 ("[T]he FBI [an agency of the DOJ] works closely with the private sector through its InfraGard program, a public-private partnership with over 30,000 members.") ("[T]he Department of Homeland Security's National Cybersecurity and Communications Integration Center (NCCIC) collaborates closely with private sector entities to ensure access to classified and unclassified information about cyber risks and incidents."); *see also* Hennessey, *supra* note 36.

39. *See, e.g.*, U.S. DEP'T OF HOMELAND SEC. & U.S. DEP'T OF JUSTICE, PRIVACY AND CIVIL LIBERTIES FINAL GUIDELINES: CYBERSECURITY INFORMATION SHARING ACT OF 2015 7 (2016), https://www.us-cert.gov/sites/default/files/ais_files/Privacy_and_Civil_Liberties_Guidelines_(Sec%20105(b)).pdf.

40. The guidelines require that federal entities, prior to disseminating cyber threat indicators, determine whether such indicators contain information "(1) not directly related to a cybersecurity threat (2) that such federal entit[ies] know[] at the time of sharing to be personal information . . . or information that identifies a specific individual." *Id.* at 7.

41. *See* Pozen, *supra* note 16, at 235, 242.

42. Here, the Obama administration also played a crucial role in the enactment of "hard law." *See* USA Freedom Act of 2015, Pub. L. No. 114–23, 129 Stat. 268 (2015)

Presidential Policy Directive Number 28 (PPD-28).[43] Pursuant to PPD-28, federal agencies that played a role in surveillance policy participated in a wide-ranging interagency process on overseas intelligence.[44] This process included perspectives from overseas stakeholders, supplied by the State Department.[45] The PPD-28 process stressed methods for ensuring that surveillance and intelligence collection could go forward with appropriate regard for global privacy rights.[46]

Moreover, representatives of intelligence-collection agencies spoke publicly to multiple audiences, including advocacy groups, journalists, scholars, and practitioners. These representatives outlined agency positions and sought feedback from other stakeholders.[47] In addition, immediately after Snowden's revelations, President Obama established a Privacy Review Group (PRG) comprised of distinguished scholars and former government officials that assessed U.S. surveillance and issued

---

(codified in various sections of Title 50 of the U.S. Code); *see also* LAURA K. DONOHUE, THE FUTURE OF FOREIGN INTELLIGENCE: PRIVACY AND SURVEILLANCE IN A DIGITAL AGE 48–53 (2016) (discussing background of USAFA's passage and shift from prior surveillance regime). *See generally* Peter Margulies, *Surveillance By Algorithm: The NSA, Computerized Intelligence Collection, and Human Rights*, 68 FLA. L. REV. 1045 (2016) (providing background information of USAFA's effect on metadata). The USA Freedom Act mandated structural changes in the United States' metadata collection program. Congress, *inter alia*, moved collection of domestic call record information (such as phone numbers and the duration of calls) from the government to private telecommunications firms, required that all search terms proposed by the government be specific identifiers such as individual phone numbers, and mandated that the Foreign Intelligence Surveillance Court (FISC) find that any search term proposed by the government gave rise to a reasonable and articulable suspicion of links to terrorism. The USA Freedom Act was a substantial step forward in accountability and transparency, in which the Obama administration was a key player.

43. *See* PPD-28, *supra* note 17; *see also* Rascoff, *supra* note 2, at 669–71 (discussing features of PPD-28).

44. *See* PPD-28, *supra* note 17, at 1–3 (providing principles governing the collection of signals intelligence); Peter Margulies, *Defining "Foreign Affairs" in Section 702 of the FISA Amendments Act: The Virtues and Deficits of Post-Snowden Dialogue on U.S. Surveillance Policy*, 72 WASH. & LEE L. REV. 1283, 1290 (2015).

45. *See* Rascoff, *supra* note 2, at 672–73; *cf.* Ashley Deeks, *An International Legal Framework for Surveillance*, 55 VA. J. INT'L L. 291, 330 (2015) (discussing transnational factors that limit any single nation's surveillance); Ashley Deeks, *Checks and Balances from Abroad*, 83 U. CHI. L. REV. 65, 82–86 (2016) (discussing international and national checks and balances that pressured the United States to limit its national surveillance).

46. *See* PPD-28, *supra* note 17, at 5 ("All persons should be treated with dignity and respect, regardless of their nationality or wherever they might reside, and all persons have legitimate privacy interests in the handling of their personal information.").

47. *See, e.g.*, AM. BAR ASS'N STANDING COMM. ON LAW & NAT'L SEC., 24TH ANNUAL REVIEW OF THE FIELD OF NATIONAL SECURITY LAW (2014), http://www.americanbar.org/content/dam/aba/events/law_national_security/LW1114_prog.authcheckdam.pdf (listing a panel including Robert Litt, General Counsel, Office of the Director of National Intelligence, as well as law professors and privacy advocates from American Civil Liberties Union).

public findings.[48] Agencies also shared information with the Privacy and Civil Liberties Oversight Board (PCLOB), which wrote comprehensive public reports on both the USA Patriot Act Section 215 "metadata" program[49] and the FISA Section 702 program.[50] These reports were not knee-jerk endorsements of government programs. Both the PRG and the PCLOB delivered reports that were critical of the domestic metadata collection program, setting the stage for that program's replacement by Congress in the USA Freedom Act of 2015. Government officials also participated in a robust debate on compliance with the spirit and letter of legal norms.[51]

---

48. *See* THE PRESIDENT'S REVIEW GROUP ON INTELLIGENCE AND COMMUNICATIONS TECHNOLOGIES: RICHARD A. CLARKE ET AL., THE NSA REPORT: LIBERTY AND SECURITY IN A CHANGING WORLD (2014) [hereinafter THE NSA REPORT].

49. PRIVACY AND CIVIL LIBERTIES OVERSIGHT BD., REPORT ON THE TELEPHONE RECORDS PROGRAM CONDUCTED UNDER SECTION 215 OF THE USA PATRIOT ACT AND ON THE OPERATIONS OF THE FOREIGN INTELLIGENCE SURVEILLANCE COURT (Jan. 23, 2014), https://fas.org/irp/offdocs/pclob-215.pdf.

50. PRIVACY AND CIVIL LIBERTIES OVERSIGHT BD., REPORT ON THE SURVEILLANCE PROGRAM OPERATED PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT (July 2, 2014) [hereinafter Section 702 Report], https://www.pclob.gov/library/702-Report.pdf. Compare Paul Rosenzweig et al., *Maintaining America's Ability to Collect Foreign Intelligence: The Section 702 Program*, HERITAGE FOUND. (May 13, 2016), http://www.heritage.org/research/reports/2016/05/maintaining-americas-ability-to-collect-foreign-intelligence-the-section-702-program (describing Section 702's efficacy and arguing that its impact on privacy is modest), with DONOHUE, *supra* note 41, at 68–72 (arguing that Section 702 undermines privacy).

51. *See* John DeLong, *Aligning the Compasses: A Journey through Compliance and Technology*, IEEE SECURITY & PRIVACY, July-Aug. 2014, at 85–86 (discussing technology that buttresses compliance with legal rules); *see also* Robert S. Litt, *The Fourth Amendment in the Information Age*, 126 YALE L.J. F. 8, 18 (2016) (observing that "technology can play an important role . . . in protecting privacy while enabling lawful collection of information by the government"). In this sense, scholarly efforts took up the challenge of commentators who argued that U.S. surveillance policy prior to Snowden's revelations did not leave sufficient room for debate on whether some forms of surveillance were consistent with broader U.S. interests and values, even if those policies were technically legal. *See* Margo Schlanger, *Intelligence Legalism and the National Security Agency's Civil Liberties Gap*, 6 HARV. NAT'L SECURITY J. 112, 113 (2015) (suggesting U.S. policymakers do not give full measure to costs to civil liberties in assessment of program values); *cf.* Rachel Brand, *What Does Effective Intelligence Oversight Look Like?*, LAWFARE (May 3, 2016, 3:19 PM), https://www.lawfareblog.com/what-does-effective-intelligence-oversight-look (stating that agencies should ask "whether they *should* engage in particular intelligence activities even if they *can* as a matter of law"). *See generally* Adam Klein et al., *Surveillance Policy: A Pragmatic Agenda for 2017 and Beyond*, CTR. FOR NEW AM. SECURITY (Dec. 12, 2016), https://www.cnas.org/publications/reports/surveillance-policy (suggesting that certain programs, such as the § 215 metadata program, initiated before Snowden's disclosures entailed a broad view of statutory authority that was difficult to defend politically and practically once the programs' existence became public knowledge).

As another useful example of soft law on communications technology, consider the so-called Vulnerabilities Equities Process (VEP).[52] The term, "vulnerabilities," refers to flaws in operating systems or other software, including software used to facilitate transmission of data over the Internet. Manufacturers are either wholly unaware of the flaw or indifferent to flaws created by their own lax practices. Vulnerabilities, sometimes called "zero days," allow a hacker who is aware of the flaw to release malware that exploits the vulnerability.[53] In a zero-day exploit, hackers use malware to harvest sensitive data or gain control over a computer network. U.S. officials established the VEP because, despite the dark side of zero-days, U.S. agencies regularly create or acquire such vulnerabilities for a range of purposes, including national security and law enforcement.[54]

The VEP sets up an interagency process for determining when agencies, including the NSA, alert manufacturers to zero-days.[55] Alerts serve multiple stakeholders. Manufacturers benefit because they get a chance to fix products, preserve goodwill that could be lost by a substantial data breach wrought by hackers, and avoid lawsuits that data breaches precipitate. Consumers benefit because they get to keep their data secure. Government agencies benefit because they gain goodwill with private firms that agencies can leverage to build effective public-private cybersecurity partnerships.[56] However, on the other side of the ledger, government agencies can lose if they disclose vulnerabilities that they could exploit to gain entry into the systems of foreign states or nonstate actors that underwrite cyber crime and other harmful conduct.[57] To the extent that blanket disclosure would impair

---

52. *See* Susan Hennessey, *Vulnerabilities Equities Reform That Makes Everyone (And No One) Happy*, LAWFARE (July 8, 2016, 12:27 PM), https://www.lawfareblog.com/vulnerabilities-equities-reform-makes-everyone-and-no-one-happy; Rascoff, *supra* note 2, at 673–74; SCHWARTZ & KNAKE, *supra* note 19, at 8–9.

53. P.W. SINGER & ALLAN FRIEDMAN, CYBERSECURITY AND CYBERWAR: WHAT EVERYONE NEEDS TO KNOW 115 (2014).

54. *See* Hennessey, *supra* note 51.

55. The VEP had its genesis in insights developed in the administration of President George W. Bush about the competing values that arise when government agencies become aware of vulnerabilities. *See* SCHWARTZ & KNAKE, *supra* note 19, at 4–5. The Obama administration established the VEP framework in 2010. *Id.* at 11.

56. *See* Eichensehr, *supra* note 33, at 29–31. When government shares data it has acquired about vulnerabilities, it also preserves the public good of cybersecurity, which allows everyone to benefit from the Internet. The VEP's default position favoring disclosure also decreases the risk that the government will promote a narrow agenda, such as punishing political opponents, that government hoarding of vulnerabilities might promote. *Id.* at 8, 29–31.

57. *See* David Aitel & Matt Tait, *Everything You Know About the Vulnerabilities Equities Process Is Wrong*, LAWFARE (Aug. 18, 2016, 2:46 PM), https://www.lawfareblog.co

fulfillment of such objectives, a deliberative process that conserves this government option in appropriate cases actually serves privacy interests that rogue states or cyber criminals seek to undermine.[58]

The VEP's premise is that interagency deliberation will tease out these interests and provide an orderly means for weighing their relative strength in particular cases.[59] In this sense, the VEP symbolizes the deliberative bent that characterized President Obama's administration. However, as soft law, the VEP has a weakness: it does not provide fully effective means for securing agencies' compliance with the framework.

This compliance problem also arises in the new EU-U.S. Privacy Shield data transfer agreement. The Privacy Shield agreement resulted from the CJEU's decision in *Schrems v. Data Protection Commissioner*.[60] In *Schrems*, the CJEU invalidated the so-called "Safe Harbor" agreement, under which firms in the European Union could share customer and employee information with U.S. firms in order to facilitate transnational business transactions. Under Safe Harbor, U.S. firms self-certified that they had adopted privacy principles that met EU standards, and the U.S. Federal Trade Commission monitored firms' compliance with those principles.[61] *Schrems* cited Snowden's revelations in the course of finding that U.S. firms were subject to government surveillance that made it impossible for those firms to comply with the privacy safeguards in Article 25 of the European Charter on Fundamental Rights and Freedoms.[62]

The *Schrems* Court cited three principal concerns with the scope of U.S. government surveillance and the impact of that surveillance on EU resident's data transferred to U.S. firms pursuant to Safe Harbor.[63] First, the CJEU asserted that no rules adequately constrained U.S. surveillance or prevented the indiscriminate acquisition and storage of

---

m/everything-you-know-about-vulnerability-equities-process-wrong.

58. Moreover, disclosure may reward complacency among private firms, whose negligent cybersecurity practices cause most data breaches. *Id.* (observing that "[m]ost breaches in the US, against citizens, businesses, and the government are primarily accomplished *without* zero-day vulnerabilities") (emphasis added). For example, the hacking of the Democratic National Committee during the 2016 election cycle used crude tactics such as phishing, which entails sending emails to members of organizations that entice those account holders to click on particular links. Those links contain malware that facilitates the hacker's access to the account-holder's network and personal data. *See* Lipton et al., *supra* note 2.

59. *See* Hennessey, *supra* note 51.

60. *See Schrems*, *supra* note 3.

61. *See id.* ¶ 6.

62. *Id.* ¶¶ 28, 30.

63. The following paragraphs are based on an earlier analysis. *See* Margulies, *supra* note 41.

EU residents' data.[64] Second, the CJEU asserted that to the extent that any guidelines governed U.S. surveillance, those norms were not crafted, monitored, and enforced by an agency that was independent of the U.S. intelligence community. Third, the CJEU found that no independent mechanism existed to address EU residents' complaints about U.S. surveillance.

The United States and the European Union drafted and adopted Privacy Shield to deal with the CJEU's concerns. The CJEU's first two concerns were radically overstated. They resulted from a failure to understand steps such as judicial review by the Foreign Intelligence Surveillance Court (FISC) that limited U.S. surveillance.[65] To provide a more comprehensive record for CJEU review, Privacy Shield contained an extensive list of U.S. safeguards, including those like the USA Freedom Act that were enacted after the Snowden revelations.[66]

To address the third point, Privacy Shield added another safeguard: an ombudsperson in the U.S. State Department who would respond to EU residents' complaints about U.S. surveillance. This feature illustrates soft law's promise and pitfalls. The ombudsperson may develop an effective working relationship with U.S. intelligence agencies and provide the independent check that the CJEU found lacking in *Schrems*. However, the Privacy Shield agreement lacks a concrete description of the ombudsperson's authority. Intelligence agencies such as the NSA may be reluctant to share information with a State Department official whose authority is so elusive. This is not a necessary result, but it is a ubiquitous risk in the world of nonbinding and often amorphous soft law agreements. As the next subsection shows, soft law thus fails to provide adequate protection against excesses linked to an agency discretion model.

---

64. On this point, the CJEU's analysis was inaccurate and incomplete. *See* Zachary K. Goldman, *The Emergence of Intelligence Governance*, *in* GLOBAL INTELLIGENCE OVERSIGHT: GOVERNING SECURITY IN THE TWENTY-FIRST CENTURY 207, 209–13 (Zachary K. Goldman & Samuel J. Rascoff eds., 2016). *But see* Daphna Renan, *The Fourth Amendment as Administrative Governance*, 68 STAN. L. REV. 1039, 1103–08 (2016) (discussing an administrative law model to provide more robust checks on U.S. intelligence and surveillance).

65. In a subsequent section, this Article argues that the CJEU's failure to accord a measure of deference to transnational agreements that implicate national security concerns is structurally problematic, both because it hampers such agreements and because it exceeds the CJEU's permissible role. *See infra* notes 119–24 and accompanying text.

66. Letter from Robert S. Litt, Gen'l Counsel, Office of the Dir. of Nat'l Intelligence, to Justin S. Antonipillai, U.S. Dep't of Commerce and Ted Dean, Dep. Ass't Sec'y, Int'l Trade Admin. (Feb. 22, 2016) (hereinafter ODNI Letter), http://ec.europa.eu/justice/data-protection/files/privacy-shield-adequacy-decision-annex-6_en.pdf.

II. THE PRIVACY PROS AND CONS OF AGENCY DISCRETION

In contrast to the multilateralism of the soft law approach, the agency discretion model entails unilateral action by a single government agency. The agency action included within this rubric occurs outside the regulatory process mandated for U.S. "substantive rules" under the Administrative Procedure Act (APA).[67] APA procedures mandate notice of a proposed rule to stakeholders and give them an opportunity to comment on the proposal. Outside the APA process, the deliberation encouraged by input from multiple stakeholders can give way to a more expedient perspective on parochial agency agendas.[68] That is not a *necessary* result of agency discretion; as this subsection notes, an agency such as the Federal Trade Commission has expertly served the interests of multiple stakeholders in shaping privacy policy outside the APA. However, agency discretion raises the risk that narrower goals will dominate policy formation.

The perils of agency discretion pervade law enforcement and national security decisions that affect privacy. The U.S. Department of Justice (DOJ) and components of the DOJ such as the Federal Bureau of Investigation (FBI) routinely make vital enforcement decisions wholly outside the APA process.[69] Some prosecutorial actions must take place

---

67. *See* 5 U.S.C. § 553 (2016); Perez v. Mortg. Bankers Ass'n, 135 S. Ct. 1199, 1203–04 (2015).

68. When an agency fails to adequately tether its discretion to the statute that authorizes it to act, the agency's failure can also clash with the separation of powers built into the U.S. Constitution. For a discussion of the constitutional and statutory problems with President Obama's Deferred Action for Parents of Americans (DAPA) program, see Patricia L. Bellia, *Faithful Execution and Enforcement Discretion*, 164 U. PA. L. REV. 1753 (2016); Peter Margulies, *The Boundaries of Executive Discretion: Deferred Action, Unlawful Presence, and Immigration Law*, 64 AM. U. L. REV. 1183 (2015); *see also* Texas v. United States, 809 F.3d 134, 169 (5th Cir. 2015) (holding that Department of Homeland Security had improperly issued DAPA regulations without following notice and comment provisions required in that context, and that DAPA was also inconsistent with U.S. Immigration and Nationality Act), *aff'd per curiam*, 136 S. Ct. 2271 (2016).

69. *See* Rachel E. Barkow, *Institutional Design and the Policing of Prosecutors: Lessons from Administrative Law*, 61 STAN. L. REV. 869, 880–84 (2009); Dan M. Kahan, *Is* Chevron *Relevant to Federal Criminal Law?*, 110 HARV. L. REV. 469, 472–79 (1996); s*ee also* McDonnell v. United States, 136 S. Ct. 2355, 2372 (2016) (interpreting federal wire fraud statute narrowly to avoid "breathtaking expansion" of prosecutorial power that could chill routine constituent service and other activities fundamental to representative government); *cf.* Daniel C. Richman & William J. Stuntz, *Al Capone's Revenge: An Essay on the Political Economy of Pretextual Prosecution*, 105 COLUM. L. REV. 583, 589–91 (2005) (discussing perils of excessive prosecutorial discretion). *See generally* Gerard E. Lynch, *Our Administrative System of Criminal Justice*, 66 FORDHAM L. REV. 2117 (1998) (examining the common occurrence of plea bargains as a way to understand what happens if we think of the American criminal justice system as one in which an administrative

outside this process, which is often too cumbersome for the fine-grained decisions that are the province of prosecutors. However, the broad ambit of prosecutorial discretion can reduce deliberation on privacy matters with global reach.

A. Pro-Privacy Agency Discretion: The Federal Trade Commission

Law enforcement's tendency to discount privacy concerns has obscured some *pro-privacy* moves within the agency discretion model. For example, the Federal Trade Commission (FTC) has taken a lead role in privacy policy, filling a vacuum created by Congress's failure to pass a comprehensive cybersecurity law.[70] While some experts argue that the FTC has not provided firms with sufficient guidance, the agency has acted consistently with multistakeholder consensus. The FTC has stressed rudimentary cybersecurity measures, including targeting firms that resorted to easy-to-guess or publicly available passwords.[71] The FTC's stress on basic cybersecurity has produced a straightforward regime that allows U.S. firms to assert their compliance with global privacy norms, including those embodied in transatlantic data transfer agreements.[72]

B. Agency Discretion That Clashes with Privacy: Federal Law Enforcement

Unfortunately, Edward Snowden's disclosures have muted the global salience of U.S. pro-privacy agency discretion. Instead, the trust

---

agency, like the Department of Justice, administratively decides, subject to judicial review, who is worthy of criminal punishment).

70. *See* FTC v. Wyndham Worldwide Corp., 799 F.3d 236, 259 (3d Cir. 2015) (holding that Federal Trade Commission had authority to sue corporation on theory that firm's failure to take reasonable cybersecurity measures constituted unfair trade practice that harmed consumers when firm's privacy policy claimed more robust safeguards were in place and hack exposed customer information); *see also* Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583, 589 (2014) (praising the FTC's approach and theorizing that its actions have developed a rich jurisprudence that is effectively the law of the land for businesses that deal in personal information). *But see* LabMD, Inc. v. FTC, 2016 U.S. App. Lexis 23559 (11th Cir. Nov. 10, 2016) (granting stay pending appeal based on finding substantial likelihood that FTC had exceeded its statutory mandate in imposing remedial measures on company that had merely been a victim of unauthorized cyber intrusion by data security firm seeking company's business); Justin (Gus) Hurwitz, *Data Security and the FTC's UnCommon Law*, 101 Iowa L. Rev. 955, 980-88 (2016) (questioning whether FTC's approach offers sufficient guidance to stakeholders).

71. *See Wyndham Worldwide Corp.*, 799 F.3d at 240–41.

72. *See* Solove & Hartzog, *supra* note 69, at 603–04.

deficit engendered by Snowden's revelations[73] has highlighted the privacy *costs* of agency discretion.[74] That trust deficit lacks strong empirical support: agency discretion can *enhance* privacy, as with the FTC. Moreover, the surveillance systems disclosed by Snowden typically featured internal and external constraints, including review by a specialized federal court that acolytes of the trust deficit fail to acknowledge.[75] Nevertheless, perhaps because the agency discretion model fits well within a European narrative of the United States' cowboy mentality, the narrative of U.S. unilateralism has dominated global privacy narratives since Snowden's disclosures. Despite the valuable soft law initiatives described above, the Obama administration did not fully appreciate the way in which unilateral U.S. law enforcement actions cemented this anti-U.S. frame.[76]

Federal law enforcement agencies are not well situated to act as stewards of technological progress. These agencies generally focus on maximizing access to information that will facilitate successful investigations and prosecutions.[77] They are less cognizant of the long-term impact of this access on transnational comity or technological development.[78] Yet, in the absence of congressional action that could

---

73. The phrase *trust deficit* refers to the tendency of some Europeans and European institutions to distrust U.S. actions and motives. Of course, civil liberties and privacy cases *within* the U.S. often take the same view. *See* DONOHUE, *supra* note 41, at 104–05. This Article does not concede that the trust deficit spurred by Edward Snowden is an accurate or complete perspective on U.S. surveillance. However, the trust deficit is a phenomenon that U.S. policymakers must address in a clear-eyed fashion.

74. *See* Christopher Kuner, *Reality and Illusion in EU Data Transfer Regulation Post Schrems*, 18 GERMAN L.J. (forthcoming 2017).

75. *See* Peter Margulies, *Dynamic Surveillance: Evolving Procedures in Metadata and Foreign Content Collection After Snowden*, 66 HASTINGS L.J. 1, 9 (2014).

76. *Cf.* DANIEL KAHNEMAN, THINKING, FAST AND SLOW (2011) (discussing ways in which certain cognitive scripts enforce preexisting ways of thinking about the world, even if those methods reflect faulty logic and judgment).

77. *Cf.* Rascoff, *supra* note 2, at 684–88 (noting problems with unilateral approach to intelligence gathering and, by extension, law enforcement). *But see* Carrie Cordero, *A Response to Professor Samuel Rascoff's Presidential Intelligence*, 129 HARV. L. REV. F. 104 (2016) (noting that the need to act quickly and decisively to gather intelligence makes it difficult to require strict adherence to the more time-consuming multi-stakeholder process).

78. *See* BERKMAN CTR. FOR INTERNET & SOC'Y AT HARVARD UNIV., *Don't Panic: Making Progress on the "Going Dark" Debate* 15 (2016). Of course, technologists, technology firms, and foreign countries also have incomplete frames. They may *overestimate* the costs to technological progress or international comity of law enforcement access, just as U.S. law enforcement agencies *underestimate* such costs. *See also Going Dark: Encryption, Technology, and the Balance Between Public Safety and Privacy: Hearing Before the S. Comm. on the Judiciary*, 114th Cong. (2015) (statement of Herbert Lin, Research Fellow, Hoover Inst., Stanford Univ.) [hereinafter *Lin Testimony*] (cautioning against "theological clash of absolutes" on issues of law enforcement access).

effectively balance law enforcement access with technological and transnational concerns, U.S. law enforcement agencies have filled the void. The following paragraphs address two recent examples of flaws in federal enforcement's adoption of the agency discretion approach to communications technology.

1. Hacking iPhone Encryption: The San Bernardino Shooting Case

In the Apple San Bernardino shooting case, the Justice Department argued that the carefully crafted limits imposed by Congress in the Communications Assistance for Law Enforcement Act (CALEA)[79] did not bar the FBI's efforts to force Apple to bypass privacy protections on the iPhone of one of the San Bernardino shooters.[80] Rather than operate within CALEA's limits, the FBI sought to rely on the All Writs Act,[81] a 1789 statute that offered no privacy protections. Generally, a later, more comprehensive statute like CALEA would trump an earlier, general statute such as the All Writs Act. By seeking to upend that structural precept, the FBI introduced a dangerous element of volatility that undermined the stewardship model.[82]

Global consequences would arise if U.S. law enforcement could compel technology companies to disable key security features such as encryption. Technology firms such as Apple and Google, which together manufacture the operating systems of most of the world's smart phones, have extraordinary global reach. Billions of people all over the world rely on their products. Those individuals place vast amounts of personal

79. 47 U.S.C. §§ 1001–1010 (2012).

80. For a similar case, see *In re* Order Requiring Apple, Inc. to Assist in the Execution of a Search Warrant Issued by this Court, 149 F. Supp. 3d 341 (E.D.N.Y. 2016) [hereinafter *In re* Apple, Inc.]; John L. Potapchuk, *A Second Bite at the Apple: Federal Courts' Authority to Compel Technical Assistance to Government Agents in Accessing Encrypted Smartphone Data Under the All Writs Act*, 57 B.C. L. REV. 1403 (2016) (discussing the underlying legal implications surrounding the heated public debate that has emerged in the wake of *In re Apple, Inc.* and other similar cases as well as the practical challenges enhanced data encryption creates for law enforcement officials). The FBI eventually purchased a software vulnerability from a third party that allowed it to access the shooter's iPhone. *See* Ellen Nakashima, *Comey Defends FBI's Purchase of iPhone Hacking Tool*, WASH. POST (May 11, 2016), https://www.washingtonpost.com/world/national-security/comey-defends-fbis-purchase-of-iphone-hacking-tool/2016/05/11/ce7eae54-1616-11e6-924d-838753295f9a_story.html?utm_term=.02499c6f1228.

81. 28 U.S.C. § 1651(a) (2016).

82. Marty Lederman has discussed this structural element, as raised in another iPhone encryption case. *See* Marty Lederman, *Magistrate Judge Orenstein's Order in the EDNY, Denying DOJ's All Writs Act Request . . .* , JUST SECURITY (Mar. 1, 2016, 8:01 AM), https://www.justsecurity.org/29599/magistrate-judge-orensteins-order-denying-dojs-writs-act-request/.

data on their smart phones, which have become the modern mobile equivalent of an office, study, library, diary, and address book.[83] Manufacturers design security features such as encryption to allow consumers to protect this data against unauthorized intrusions.[84] The players behind unauthorized intrusions include not only U.S. law enforcement, which generally must obtain a court order, but also foreign governments and cyber criminals in the U.S. and abroad, who do not comply with U.S. privacy laws or the U.S. Constitution. These bad actors will seek to obtain any pathway into encrypted smart phones that federal law enforcement requires technology firms to provide. Because cyber criminals and foreign states constantly seek access to private firm networks, widespread dissemination of such pathways would render insecure both smart phones and all the data kept on those devices.[85]

The government's litigating stance raised legal as well as policy issues. As Magistrate Judge James Orenstein pointed out in an earlier case, the government's position distorted statutory frameworks by making the All Writs Act into an omnibus source of authority for injunctions against technology companies.[86] Congress never intended that the All Writs Act serve this function. Rather, the All Writs Act merely authorized courts to fill gaps when that interstitial role was consistent with the statutory landscape.

Magistrate Orenstein linked this gap-filling function to the All Writs Act's requirement that an order issued pursuant to the statute be "agreeable to the usages and principles of law."[87] In finding that the government's position did not conform to such precepts, Judge

---

83. *See* Riley v. California, 134 S. Ct. 2473, 2483 (2014) (holding that a digital search of a smartphone required a showing of probable cause to believe that material on the phone contained evidence of a crime).

84. *See* ASHLEY DEEKS, THE INTERNATIONAL LEGAL DYNAMICS OF ENCRYPTION 13 (2016).

85. In fairness, the government also has compelling arguments on its side. Law enforcement may need access to information on smart phones to investigate crime and protect public safety. This subsection's sole point is that relying on discretionary judgments by federal law enforcement officials may result in harm to statutory schemes that require more respect for technology firms' concerns, including protecting internet security and encouraging innovation. There may be approaches that reconcile these competing goals. *See Lin Testimony*, *supra* note 77. Generally, however, Congress should formulate these approaches through legislation. Litigation positions by federal law enforcement that fail to respect Congress's previous efforts send an unsettling signal to both domestic and global audiences.

86. *See In re* Apple, Inc., 149 F. Supp. 3d at 351 ("In arguing to the contrary, the government posits a reading of the latter phrase so expansive—and in particular, in such tension with the doctrine of separation of powers—as to cast doubt on the AWA's constitutionality if adopted.").

87. *Id.* at 353.

Orenstein found that CALEA is "part of a comprehensive legislative scheme."[88] That scheme tellingly fails to include any mandate that Apple assist the government in decrypting an encrypted device.

As Magistrate Orenstein explained, this omission gives rise to the inference that Congress intended to "prohibit the imposition of such a duty."[89] There is an exception to this provision, but only for instances in which a company has provided a customer with the encryption code.[90] Under the statute, the government cannot require a provider or manufacturer to implement "any specific design of equipment, facilities, services, features, or system configurations."[91] Moreover, the government cannot "prohibit the adoption of any equipment, facility, service, or feature."[92] According to Magistrate Judge Orenstein, these provisos reflect Congress's wish that encouraging cooperation between government and business "would not stem technological progress."[93] As Congress noted in the House Report, Congress wished to spur cooperation between communications firms and the government "without impeding the introduction of new technologies, features, and services."[94]

The development of encryption in the wake of Edward Snowden's revelations is a commercial decision by manufacturers, but it is no less protected for that reason. Congress in CALEA acknowledged the salutary role of private sector competition in crafting innovations that would aid consumers, including those that would "protect privacy in the face of increasingly powerful and personally revealing technologies."[95] The undermining of encryption sought by the FBI, with or without a court order, would distort the product that Apple had developed and marketed to consumers. That distortion of market forces could chill innovation at software companies, intimating that new features are not worth the time, trouble, and cost required to develop and market them.

---

88. *Id.* at 357.

89. *Id.*

90. 47 U.S.C. § 1002(b)(3).

91. *Id.* at § 1002(b)(1)(A). The government claimed that CALEA may not address data at rest. However, this is doubtful, since CALEA requires telecommunications companies to possess the ability to furnish "call-identifying information" to law enforcement after a call has ended. Data possessed by a telecommunications firm after a call's conclusion would presumably be data "at rest" under the government's formulation. *See In re* Apple, Inc., 149 F. Supp. 3d at 356 n.15.

92. 47 U.S.C. § 1002(b)(1)(B).

93. *In re* Apple, Inc., 149 F. Supp. 3d at 354.

94. *See* U.S. Telecom Ass'n v. FCC, 227 F.3d 450, 454 (D.C. Cir. 2000); H.R. REP. NO. 103-827, pt. 1, at 12 (1994). Moreover, Apple could be considered a provider of "information services," not communications services, which would make Apple wholly exempt from CALEA. *See* 47 U.S.C. § 1002(b)(2); *In re* Apple, Inc., 149 F. Supp. 3d at 356.

95. H.R. REP. NO. 103-827, pt. 1, at 15 (1994).

Hindrances to innovation decreed on law enforcement's request are a negative externality imposed on consumers, who must make do with a narrower range of options. Congress enacted CALEA to forestall this possibility.

The FBI's energetic approach to agency discretion in the San Bernardino shooting iPhone case continued even after the FBI purchased use of a software vulnerability that allowed it to gain access to the smartphone at issue. The FBI failed to disclose that vulnerability as part of the Vulnerabilities Equities Process.[96] Explaining this failure, FBI Director James Comey revealed that the FBI had only purchased the ability to use the software flaw for access to data on the shooter's iPhone. The FBI had not purchased the vulnerability itself, or technical knowledge about the vulnerability's operation or how to patch it. As a result, Apple was left in the dark, and its customers were left without Apple's help in maintaining the security of their own smartphones. Admittedly, acquiring knowledge of the vulnerability's operation would have increased the price the Bureau had to pay. However, the interagency deliberation of the VEP could have informed the trade-off between a higher purchase price and the virtues of disclosing the flaw to Apple. The FBI's own internal process evidently prioritized incurring lower costs. That skewed calculus constituted the very problem that the VEP was designed to avoid. Here, as well, law enforcement discretion prevailed over privacy.

2. Territory, Access to Data, and Agency Discretion

The conflict between privacy and law enforcement discretion in the Obama administration also played out in a case that arrayed the U.S. Department of Justice against another major technology firm: Microsoft. In *Microsoft Corp. v. United States* (*Microsoft Ireland*),[97] the Justice Department insisted that it could bypass international agreements, called Mutual Legal Assistance Treaties. The Justice Department, which was seeking information relevant to a criminal investigation, sought a court order requiring Microsoft to produce data that the corporation had stored abroad. The Stored Communications Act (SCA)[98] contained language suggesting that the statutory scheme did not authorize a court order in this context. However, the Justice Department's aggressive litigation posture unduly discounted this constraint.

96. *See* Nakashima, *supra* note 79.
97. 829 F.3d 197, 221 (2d Cir. 2016) [hereinafter Microsoft Ireland].
98. 18 U.S.C. §§ 2701–2712.

The SCA, as part of the Electronic Communications Privacy Act (ECPA), aimed to safeguard privacy in new technology that featured a more dynamic relationship between user and service provider. According to the Second Circuit, Congress had legislated against the backdrop of a traditional construction of the term *warrant* that had a limited territorial reach.[99] The Justice Department's litigation stance obscured that backdrop. As in the Apple San Bernardino iPhone case, the government's position threatened to impose subtle but significant costs on global consumers.

The stakes in *Microsoft Ireland* were high. The government's position in *Microsoft Ireland* undermined technology companies' reliance on the limited territorial scope of warrants. Surveying that legal landscape, companies like Microsoft had devised a regime that combined the exigencies of cloud computing with the demands of global government relations. Microsoft generally stores a customer's data in a site that is proximate to the physical coordinates that the customer has cited as his or her home location.[100] Microsoft applies this storage-user location nexus to avoid delays in the functioning of cloud computing services.[101] Pursuant to this storage-user location nexus, Microsoft runs storage centers in over one hundred countries.[102] In the *Microsoft* warrant case, the U.S. prosecutors (DOJ) sought data from a storage center in Ireland. Microsoft sought to quash the warrant on grounds that Ireland had more rigorous laws on data protection. An MLAT between Ireland and the United States governed access to this data and provided a vehicle for reconciling the needs of U.S. law enforcement with Ireland's more protective privacy laws.[103] Admittedly, MLATs are

99. Microsoft Ireland, 829 F.3d at 208. Because of this backdrop, the Second Circuit viewed the issuance of a warrant for data abroad as clashing with the presumption, recently reinforced by the Supreme Court, against extraterritorial application of statutes. *Id.* at 210 (citing Morrison. v. Nat'l Australia Bank Ltd., 561 U.S. 247, 255 (2010)). An amendment to Rule 41 of the Federal Rules of Criminal Procedure that became effective after the Second Circuit's decision liberalized venue rules for warrants in certain cases involving computer crime. *See* FED. R. CRIM. P. 41, 2016 Amendment Note (b)(6) (providing that venue was proper in any district where law enforcement was investigating computer fraud or activity on networks whose location had been hidden by subjects of the investigation). The changes to Rule 41 were controversial. However, they would not have changed the outcome in the *Microsoft Ireland* case.

100. Microsoft Ireland, 829 F.3d at 202–03.

101. *Id.*

102. *Id.*

103. *See* Daskal, *Un-Territoriality*, *supra* note 4, at 393–94.

often cumbersome.[104] However, failing to work within the MLAT left a vacuum without guidance for technology companies.[105]

The Justice Department's position also created uncertainty for other frameworks. The government disregarded well-established arguments that the SCA's rules on remote computing protected files held in foreign data centers.[106] The government's position would have bypassed the SCA's protections and disrupted technology firms' relations with foreign states. In addition, adopting the FBI's position would have encouraged demands on technology companies from states such as Russia and China, whose privacy policies are far less protective than those of either Ireland *or* the United States.

The Justice Department's position, which the Second Circuit held was inconsistent with the SCA, failed to address these concerns. Instead, the Justice Department's stance elevated access to information over all countervailing values. That posture exemplified the flaws in the agency discretion model.

III. A NEW STEWARDSHIP: THE OBAMA ADMINISTRATION'S CONFLICTED LEGACY

To assess the merits of the soft law and agency discretion approaches and forge a path forward, this Part suggests a new vision of cybersecurity and surveillance stewardship. The new stewardship outlined here has both discursive and structural components. I outline each in turn.

---

104. *Id.* at 393 (noting that MLATs have "historically been slow and clumsy").

105. Here, too, law enforcement officials had legitimate concerns. When the law limits compulsory process based on the location of data, those limits incentivize criminals to misrepresent their location in order to avoid the law's reach. *See* Microsoft Ireland, 829 F.3d at 224 (Lynch, J., concurring) (noting that Microsoft's policy assisted "*foreign* customers, and those Americans who *say* that they reside abroad"). Counterterrorism officials also have legitimate concerns about potential *foreign* targets of investigations who game the system in an analogous fashion, by using virtual private networks (VPNs) to mimic or "spoof" a U.S. location, requiring the government to meet a higher standard to conduct surveillance. *See* DAVID S. KRIS, TRENDS AND PREDICTIONS IN FOREIGN INTELLIGENCE SURVEILLANCE: THE FAA AND BEYOND 8-27 (discussing surveillance issues relevant to VPNs).

106. *See* Kerr, *supra* note 9, at 1215–16; *cf.* H.R. REP. No. 99-647, at 64–65 (1986) (observing that opened email messages stored on a server are protected under SCA's remote computing provisions).

A. Discursive Stewardship

After Snowden's revelations, President Obama signaled a sincere desire to open up discourse on both surveillance and cybersecurity.[107] However, discordant tones also emerged, particularly from federal law enforcement. A more comprehensive regime of discursive stewardship would have set a coherent tone *throughout* the administration.

Discursive stewardship has two facets: seeking input from other stakeholders and providing information to those players about one's own practices. These facets are two sides of the same coin: input from other stakeholders will be of limited utility if those stakeholders lack information on which to base opinions. Similarly, the executive branch has little incentive to provide input to other players if it does not sincerely value the opinions that it will receive in return. Just as importantly, discursive stewardship as practiced by senior officials in an influential state such as the United States has demonstration effects.[108] In other words, the effective seeking of input and provision of information by an influential state can help persuade other states that these discursive habits are worth cultivating. That then leads to even

107. One can argue that this post-Snowden focus is incomplete, since it omits consideration of the administration's pre-Snowden public silence. This argument clearly has some force. However, it fails to acknowledge the difficult choices built into transnational policy on surveillance. As the European Court of Human Rights has observed, undue disclosure of surveillance methods undermines their utility. *See* Kennedy v. United Kingdom, EUR. CT. H.R. 45 (May 18, 2010), http://hudoc.echr.coe.int/eng?i=001-98473. *But see* Sudha Setty, *Surveillance, Secrecy, and the Search for Meaningful Accountability*, 51 STAN. J. INT'L L. 69, 71–72 (2015) (conceding that some secrecy is necessary, but arguing that excessive secrecy allows government to circumvent checks and balances). While *one* of the programs that Snowden revealed—the former metadata program for collecting U.S. call records—may not have thwarted terrorist attacks that officials can identify, the surveillance programs as a whole were useful in providing information about notoriously furtive global terrorist networks. *See* THE NSA REPORT, *supra* note 47, at 104. Moreover, each program was the subject of scrutiny within independent branches of the U.S. government, including both Congress and the courts. *See generally* David S. Kris, *On the Bulk Collection of Tangible Things*, LAWFARE RES. PAPER SERIES, Sept. 29, 2013 (discussing the U.S. government's use of the tangible-things provision of FISA and the disclosure of bulk metadata collection, which contributed to a broader policy debate concerning the transparency of intelligence activities and the role of the FISA court); Margulies, *supra* note 74 (outlining a dynamic conception of national security surveillance that supports the legality of section 215 of the USA Patriot Act and section 702 of FISA, programs that received informed input from all three branches of government). Further public disclosure prior to Snowden's revelations might well have jeopardized these programs' effectiveness. Any conception of stewardship needs to acknowledge these complex trade-offs.

108. *See* Jane Stromseth, *Post-Conflict Rule of Law Building: The Need for a Multi-Layered, Synergistic Approach*, 49 WM. & MARY L. REV. 1443, 1466 (2008).

more sharing of information and input, in a cycle of positive reinforcement.

Discursively, stewardship seeks to effectuate a reasonable degree of state transparency. Heightened transparency is vital to ease the trust deficit caused by the secret programs disclosed by Edward Snowden. However, stewardship balances the transparency imperative against the risk posed by supplying terrorists and transnational criminals with a roadmap. Discursive stewardship also expressly recognizes a mutuality of interest among countries and internet stakeholders, including the public, media, business, and technologists. It uses a vocabulary of inclusion, rather than exclusion.

With respect to discursive stewardship, the Obama administration's record has been mixed. On post-Snowden surveillance policy, the administration has engaged in unprecedented transparency. Outreach to stakeholders has also been a feature of cybersecurity policy, particularly on the protection of critical infrastructure. However, the dominance of the agency discretion paradigm in federal law enforcement has shrunk the space available for discursive stewardship on internet security issues such as encryption.

On surveillance policy, PPD-28 heralded a transparency that is unique among states. No other state has done as much to document its own practices and articulate principles that guide its policies. Of course, some of those principles leave the government wiggle room: the United States' commitment to all "feasible" tailoring of surveillance preserves significant flexibility for the intelligence community. However, a measure of flexibility is both advisable and legally valid in the dynamic world of foreign intelligence gathering. What counted most was PPD-28's promotion of a conversation both within the U.S. government[109] and among other global stakeholders about surveillance's benefits and limits.

The cybersecurity framework developed under the aegis of NIST also represented a step forward in discursive stewardship. The cybersecurity framework's process featured a series of lengthy meetings and workshops with technology experts and representatives from a wide range of private firms. The final framework reflected that dialogue. Some players may have wished that the framework provided more specific guidance. However, more specific guidance may have locked in approaches that would soon become obsolete. The open-ended nature of the guidance left room for conversations to continue.

---

109. The VEP was also useful in prompting dialogue in and out of government. *See* Hennessey, *supra* note 51.

Unfortunately, there were also more discordant notes in the stewardship discourse of the Obama administration. Here, the agency discretion model has had an adverse impact. The post-Snowden trust deficit has muted appreciation for the strong pro-privacy efforts of the FTC. The most salient narrative stems from the view expressed by prominent federal law enforcement officials, including former FBI director James Comey, that law enforcement requires some manner of access to encrypted communications between terrorists, criminals, and other parties of interest.[110]

Comey's view, which echoed earlier debates, is not without foundation. According to law enforcement officials, use of encryption that hinders the execution of warrants and other court orders that assist in the investigation of crime raises the risk of "going dark"—of a pervasive governmental ability to enforce the criminal law. Encryption, which technology firms turned to both because of internet security concerns and because of worries about government surveillance in the wake of Snowden's disclosures, may well make it far more difficult for law enforcement to obtain information in ways it has relied on for decades, such as data from court-ordered wiretaps. Legislation to deal with this problem, such as the measure introduced by U.S. senators Richard Burr of North Carolina and Dianne Feinstein of California,[111] has not elicited the support necessary for passage. Skepticism about the

---

110 Former Director Comey's views resist an unduly stark characterization. In July, 2015, Comey acknowledged the importance of privacy and internet security even as he warned the Senate Judiciary Committee about the "serious public-safety ramifications" of encryption and the consequences of "moving inexorably to a place where all of our lives, all of our papers and effects, all of our communications will be covered by universal strong encryption." *See Going Dark: Hearing Before the S. Comm. on the Judiciary*, *supra* note 78. In asking for a resolution "before we get to that world," Comey appeared to suggest that technology firms should design approaches to encryption that ensured law enforcement access (so-called "backdoors"). Internet security experts generally view such approaches as posing a threat to privacy. *See* BERKMAN CTR. FOR INTERNET & SOC'Y, *Don't Panic*, *supra* note 78. While the overall tenor of these remarks was ominous, Director Comey's tone became substantially more conciliatory in the opening months of 2017, after much of this Article was written. Just prior to his dismissal by President Donald Trump, then-Director Comey informed the Senate Judiciary Committee that federal law enforcement officials had engaged in "very good, open and productive conversations" with technology firms since the flurry of litigation involving the iPhone of the San Bernardino shooter. *See Full committee hearing on "Oversight of the Federal Bureau of Investigation"*, Fed. News Service, May 3, 2017. In his testimony, Comey stressed the commitment of all parties to harmonizing privacy and public safety, and forthrightly disclaimed interest in technological "backdoors" that would be "built-in" to devices to ensure law enforcement access. *Id.*

111. *See* Stephanie K. Pell, *You Can't Always Get What You Want: How Will Law Enforcement Get What It Needs in a Post-CALEA, Cybersecurity-Centric Encryption Era?*, 17 N.C. J.L. & TECH. 599, 606 n.25 (2016).

Burr-Feinstein bill stems from the same source as technologists' critique of law enforcement's "going dark" fears. Law enforcement special access can lock in features that inhibit technological innovation. It can also be fertile ground for hackers, both state and private, who seek to exploit gaps in internet security for their own purposes. While the Obama administration as a whole, including its senior national security officials, seemed to take the technologists' side in this debate,[112] the salience and persistence of law enforcement concerns muddied the Obama administration's discursive efforts.

B. Structural Stewardship

While discursive stewardship can inspire trust and serve as a catalyst for new initiatives, structural stewardship is a necessary complement. Structural stewardship entails the checks and balances that ensure input from multiple stakeholders. Each stakeholder's independence from the others insulates stakeholder views from intimidation or groupthink. Regard for structure domestically and transnationally thus promotes a higher level of deliberation and a lower risk of precipitous unilateral action. In the domestic realm, structural stewardship requires due regard for the frameworks, such as FISA, the Stored Communications Act, or the Communications Assistance for Law Enforcement Act, that Congress has labored to fashion to balance stakeholder interests and promote stakeholder input. Structural stewardship also contemplates attention to time-tested courses of dealing in which Congress has acquiesced.[113]

Structural stewardship has domestic and transnational prongs. On the domestic level, structural stewardship entails the respect for the legislature that Justice Jackson identified as a key ingredient in the separation of powers.[114] When, as in CALEA or the SCA, Congress has carefully crafted a framework for an area of communications technology, executive branch officials should not permit the agency discretion model to circumvent that framework. In the international arena, structural stewardship involves building institutions with clear ground rules that promote dialogue between states. Structural stewardship also entails independent avenues for participation by the full range of stakeholders,

112. *Id.* at 617 n.61.

113. *See* Curtis A. Bradley & Trevor W. Morrison, *Historical Gloss and the Separation of Powers*, 126 HARV. L. REV. 411, 415 (2012).

114. *See* Youngstown Sheet & Tube Co. v. Sawyer, 343 U.S. 579, 637 (1952) (Jackson, J., concurring) ("When the President acts pursuant to an express or implied authorization of Congress, his authority is at its maximum, for it includes all that he possesses in his own right plus all that Congress can delegate.").

including businesses, scholars, nongovernmental organizations, and ordinary citizens. Equipped with respect for structure, the good steward rejects actions that privilege any single value, such as profit, public safety, or national security. Structure integrates due concern for these values with other goods, such as trust and cooperation. To respect structure, when transnational agreements such as MLATs govern a field, the government should either strive to work within those structures or seek new legislative reforms. With respect to Privacy Shield or other transnational agreements, the executive should enhance the independence of accountability mechanisms such as the new State Department ombudsperson.

The Obama administration's actions sometimes presented a clash between structural stewardship and the agency discretion model. Structural stewardship, in its fidelity to congressional choices, has two important transnational benefits. First, it assures other countries that U.S. rules governing privacy flow from duly enacted legislation, visible to the public and to global audiences. That input from a co-equal branch of government provides an imprimatur of legitimacy that unilateral executive action rarely possesses. Relatedly, a strong nexus between executive action and underlying legislation assures the world that U.S. rules will not be volatile, changing willy-nilly with the next presidential election's results. While presidents can revise rules governed solely by executive discretion, changing rules keyed to legislation requires more elaborate procedures, such as notice and comment under the U.S. Administrative Procedure Act. That stability provides additional reassurance to transnational institutions in assessing how their own norms match up against U.S. rules.

U.S. law enforcement's failure to buy into these frameworks harmed the Obama administration's legacy of structural stewardship. In the Apple San Bernardino iPhone and Microsoft Ireland cases, U.S. law enforcement took aggressive litigation positions that failed to acknowledge the spirit, if not the letter, of legislative frameworks such as CALEA and the SCA. U.S. law enforcement officials' aggressive posture signaled that those frameworks were mere expedient vessels for gaining access to data. Structural stewardship suffered from law enforcement officials' eagerness to shoehorn their single-minded agenda into frameworks designed to balance competing interests.

In the surveillance arena, the Obama administration's post-Snowden pivot was substantial, but nonetheless left room for improvement. However, the Obama administration's wariness about adopting the most robust structural fixes also reflected legitimate fears that transnational tribunals such as the CJEU would unduly discount the safeguards that the United States implemented. A tribunal that

affords a measure of deference to the executive will encourage more innovative structural checks. Viewed in this sense, the CJEU's rejection of deference in *Schrems v. Data Commissioner* is counterproductive for both national security and privacy. This section first discusses the need for more robust U.S. safeguards and then links that position with a call for a measure of deference from the CJEU and other transnational tribunals.

As one index for the scope and pace of post-Snowden structural change, consider the partially successful efforts by the United States to provide a public voice at the FISC. Before Snowden's revelations, the vast majority of legal questions at the FISC were decided without a public voice that opposed the government's position. This lack of an opposing voice was problematic. As the Framers understood, a court's ability to deliberate is its most crucial virtue.[115] While the Framers were familiar with ex parte proceedings,[116] they also recognized that as a general matter more than one voice would assist the court in seeing different perspectives. After Snowden, the Obama administration supported congressional efforts that resulted in enactment of the USA Freedom Act (USAFA).[117]

The USAFA made an important structural change by expressly authorizing the FISC to designate lawyers as *amici curiae* who would oppose government positions on novel legal issues.[118] These *amici* have served with distinction. Nevertheless, a more robust, full-time public advocate who could monitor daily activities by the NSA would represent a major improvement[119] over the current situation, in which the FISC

115. *See* THE FEDERALIST No. 78, at 465 (Alexander Hamilton) (Clinton Rossiter ed., 1961) (observing that a court has "neither force nor will but merely judgment").

116. *See* Peter Margulies, *Searching for Federal Judicial Power: Article III and the Foreign Intelligence Surveillance Court*, 85 GEO. WASH. L. REV. (forthcoming 2017); James E. Pfander & Daniel D. Birk, *Article III Judicial Power, the Adverse-Party Requirement, and Non-Contentious Jurisdiction*, 124 YALE L.J. 1346, 1446–47, 1464–65 (2015); Stephen I. Vladeck, *The FISA Court and Article III*, 72 WASH. & LEE L. REV. 1161, 1170-80 (2015).

117. *See supra* note 41 and accompanying text (describing how the USA Freedom Act shifted collection of domestic call-record information back to private telecommunications firms).

118. *See* 50 U.S.C. § 1803(i)(2) (amended 2015); *see also In re* Application of the FBI for Orders Requiring the Prod. of Call Detail Records, 24 (FISA Ct. Dec. 31, 2015), https://www.dni.gov/files/documents/12312015BR_Memo_Opinion_for_Public_Release.pdf [hereinafter *In re* Application of the FBI]; [Name Redacted by the Court], 5 (FISA Ct. Nov. 6, 2015), https://www.dni.gov/files/documents/20151106-702Mem_Opinion_Order_for_Public_Release.pdf [hereinafter Name Redacted by the Court].

119. *See generally* Marty Lederman & Steve Vladeck, *The Constitutionality of a FISA "Special Advocate"*, JUST SECURITY (Nov. 4, 2013, 1:34 PM), https://www.justsecurity.org/2873/fisa-special-advocate-constitution/ (discussing the benefits of having a full-time public advocate participate in FISC proceedings).

relies almost exclusively on government disclosures of noncompliance with FISC rules. While the government has disclosed several significant episodes,[120] the FISC has on several occasions remarked on delays in the government's disclosures.[121] Delays are not as serious as outright defiance of the court's decrees. Moreover, many delays in reporting noncompliance entail good-faith misunderstandings about the court's rules, not willful disregard.[122] However, since delays have the effect of allowing noncompliance to continue, a pattern of delays can have an adverse impact that is almost as severe as the impact caused by deliberate defiance. A full-time public advocate would ease those impacts, and therefore alleviate the concerns of transnational tribunals like the CJEU about the scope and intrusiveness of U.S. surveillance.

These concerns apply with an even greater force to the ombudsperson established at the U.S. State Department pursuant to the Privacy Shield data transfer agreement. On the one hand, establishing a U.S. mechanism to address EU residents' privacy complaints was overdue. On the other hand, the ombudsperson approach does not fully resolve the problems identified by the CJEU in *Schrems*.[123] First, the ombudsperson appears to lack independence, since she serves at the pleasure of the Secretary of State, who in turn serves at the pleasure of the President.[124] The agreement fails to delineate crucial matters such as the scope of the ombudsperson's access to intelligence agencies' records and personnel. Without this access, the ombudsperson may become the equivalent of a hood ornament on an expensive automobile, pleasant to look at but not serving any useful

120. *See* John DeLong & Susan Hennessey, *Understanding Footnote 14: NSA Lawyering, Oversight, and Compliance*, LAWFARE (Oct. 7, 2016, 7:44 AM), https://www.lawfareblog.com/understanding-footnote-14-nsa-lawyering-oversight-and-compliance (last visited Feb. 5, 2017) (describing one such episode).

121. *See* Name Redacted by the Court, *supra* note 116, at 5.

122. *See* DeLong & Hennessey, *supra* note 118; Peter Margulies, *Reauthorizing the FISA Amendments Act: A Blueprint for Enhancing Privacy Protections and Preserving Foreign Intelligence Capabilities*, 12 J. BUS. & TECH. L. 23, 46 n.166 (2016).

123. *Compare* Francesca Bignami & Giorgio Resta, *Transatlantic Privacy Regulation: Conflict and Cooperation*, 78 L. & CONTEMP. PROBS. 231, 261–62 (2016) (praising CJEU's focus on privacy), *with* Scott J. Shackelford, *Seeking a Safe Harbor in a Widening Sea: Unpacking the EJC's* Schrems *Decision and What It Means for Transatlantic Relations*, SETON HALL J. DIPL. & INT'L REL. (2016) (critiquing decision as providing inaccurate description of U.S. intelligence collection), *and* PETER SWIRE, U.S. SURVEILLANCE LAW, SAFE HARBOR, AND REFORMS SINCE 2013 10–20, https://fpf.org/wp-content/uploads/2015/12/Schrems-White-Paper-12-18-2015.pdf.

124. *See* Margulies, *supra* note 43. The CJEU recently reaffirmed the importance of independence. *See Tele2 Sverige*, *supra* note 12, ¶ 120 (prescribing that state access to retained data should, as a general rule, be subject to a "prior review carried out either by a court or by an independent administrative body.").

purpose. In cases involving due process issues with the imposition of financial sanctions on suspected terrorists, European courts have found an ombudsperson inadequate to address structural flaws with suspects' recourse.[125] A strong track record on recourse might persuade the CJEU of the ombudsperson's worth. However, specific written norms would reinforce that point.[126] The parties to Privacy Shield should collaborate on such written norms if they hope to ensure the agreement's survival.

That said, the CJEU would encourage more robust structural norms if it provided a measure of deference to EU-U.S. agreements that implicate national security concerns. This measure of deference, or "margin of appreciation," is a touchstone of decisions by the European Court of Human Rights on questions of national security and public safety.[127] Privacy Shield does not directly implicate such concerns since it deals only with ordinary commercial uses of data. However, national security concerns help form the backdrop for data transfer. The CJEU's refusal to consider such concerns[128] puts both the European Union and

125. *See* Joined Cases C-584/10, C-593/10 & C-595/10, Kadi v. Comm'n, 2013 E.C.R. III-5177.

126. The U.S. could also do more to address EU concerns that surveillance under § 702 of the FISA Amendments Act sweeps too broadly. *See* Timothy Edgar, *Focusing PRISM: An Answer to European Privacy Concerns?*, LAWFARE (Oct. 10, 2015, 5:20 PM), https://lawfareblog.com/focusing-prism-answer-european-privacy-concerns (noting worries about statutory authorization of collection relevant to "foreign affairs" of the U.S., with respect to a foreign power or foreign territory); *cf.* Faiza Patel, *Safe Harbor and Reforming Section 702*, JUST SECURITY (Oct. 22, 2015, 11:25 AM), https://www.justsecurity.org/27009/safe-harbor-reforming-section-702/ (outlining concerns of CJEU and U.S. privacy advocates). The European Community appeared satisfied with U.S. representations regarding the scope of such surveillance. *See* EC Adequacy Decision, *supra* note 11. However, the content of those representations was not disclosed in the documents outlining the Privacy Shield agreement. Given the post-Snowden trust deficit, a more concrete public statement would be useful.

127. *See* Handyside v. United Kingdom, *supra* note 13 (regulating mass market sale and distribution of accounts of human sexuality in order to protect children); *see also* Sloane, *supra* note 13 (noting that extending margin of appreciation to national policies lodges decisions with officials with most immediate knowledge of the problems the policies address).

128. The CJEU's rejection of even a modicum of deference is even plainer in its most recent privacy decision. *See Tele2 Sverige*, *supra* note 12 (striking down national data retention directives designed to facilitate law enforcement and counterterrorism, despite acknowledging that measures struck down by court overlap substantially with the types of measures that EU law designates as state responsibilities *outside EU control*, such as measures involving "public security, defence, . . . and the activities of the State in areas of criminal law"); *see also* Consolidated Version of the Treaty on the European Union and the Treaty on the Functioning of the European Union art. 4(2), Mar. 30, 2010, 2010 O.J. (C83/13) (noting that "maintaining law and order" is an "essential State function" that the EU must "respect," and that "national security remains the *sole responsibility* of each Member State") (emphasis added); *cf.* Andrew Keane Woods, *Implications of the EU's Data*

the United States in a very difficult position. It forces the European Union and United States to choose between data transfer that is necessary for ordinary commerce and surveillance that is necessary for public safety. Imposing that stark choice on EU and U.S. officials does not favor either security *or* privacy.

In addition, the CJEU's apparent lack of deference chills the willingness of EU and U.S. officials to agree on workable ways to reconcile competing values. Since international relations is often a two-level game,[129] efforts at compromise come with political costs in both the United States and the European Union. In the United States, efforts to temper security with regard for privacy risk the ire of legislators who prioritize security. In the European Union, efforts to calibrate privacy with security risk blowback from officials for whom privacy is paramount. Officials on both sides of the Atlantic might view attempts at compromise as worthwhile if they had a reasonable belief that the CJEU would extend a measure of deference to such attempts. However, the prospect of CJEU invalidation of compromise measures erases the possible benefits of compromise, while leaving costs intact. The CJEU's lack of deference thus acts as a brake on good-faith efforts to reach common ground.

If the CJEU chills compromise efforts, serious unintended consequences may ensue. One consequence may be reduced functionality of commercial internet transactions for persons on both sides of the Atlantic. Another even more serious consequence could be post-Brexit moves by other EU countries to exit the EU framework. Nominal privacy guarantees are a small consolation for the costs precipitated by either of these grim scenarios. For this reason, a measure of deference by EU courts is a crucial complement to further EU-U.S. moves to bolster structural privacy guarantees.

IV. CONCLUSION

In the wake of Edward Snowden's disclosures, the world looked to the United States for responses on issues of surveillance and privacy. In cybersecurity, as well, the increasing incidence of global hacking by criminals and rogue states called for a coordinated response, with the United States making a major contribution. Given paralysis in the U.S. Congress, responsibility for this transnational response fell largely to

---

Retention Ruling, LAWFARE, (Dec. 22, 2016, 11:45 AM), https://lawfareblog.com/implications-eus-data-retention-ruling (discussing *Tele 2 Sverige*).

129. *See* Robert D. Putnam, *Diplomacy and Domestic Politics: The Logic of Two-Level Games*, 42 INT'L ORG. 427, 436 (1988).

the executive branch, led by President Barack Obama. A complicating factor was the post-Snowden trust deficit regarding U.S. action.

The U.S. response fell into two categories: soft law and agency discretion. The soft law response involved the identification of best practices for public and private sector stakeholders. Initiatives such as PPD-28 and Privacy Shield affirmed global privacy rights. The Vulnerabilities Equities Process (VEP), NIST Cybersecurity Framework, and Cybersecurity Information Sharing Act (CISA) bolstered cybersecurity while curbing privacy harms. However, soft law is not a perfect remedy. While it encourages consensus and rewards experimentation, it often lacks enforcement mechanisms. That may imperil Privacy Shield, the U.S.-EU data transfer agreement, which relies on a vaguely described State Department ombudsperson to address EU privacy concerns about U.S. surveillance. Soft law's endemic lack of mechanisms for compliance also proved inadequate to control U.S. law enforcement positions that had adverse ramifications for privacy and internet security.

U.S. law enforcement embodied soft law's competitor: agency discretion. Agency discretion entails unilateral action by a single governmental unit pursuing a particular agenda. In some cases, such as the Federal Trade Commission's enforcement of corporate privacy and cybersecurity policies in the wake of massive data breaches, agency discretion entailed stakeholder participation in crafting best practices, such as the need for robust passwords. However, the Obama administration allowed federal law enforcement too much discretion, leading to confrontations with technology firms in the Apple San Bernardino iPhone and Microsoft Ireland cases. All too often, federal law enforcement took positions that conflicted with the letter and/or spirit of legislative frameworks, such as CALEA or the Stored Communications Act (SCA).

To analyze the Obama administration's efforts and suggest a path forward, this Article outlines a new stewardship paradigm. That paradigm has both discursive and structural components. The Obama administration often fared well in the discursive realm, where input from and transparency with stakeholders is central. Initiatives such as the NIST Cybersecurity Framework and the VEP showed due regard for a spectrum of stakeholders and a sincere commitment to dialogue. However, the confrontational rhetoric of federal law enforcement agencies, such as the FBI, often distracted from this commitment.

In the structural realm, even more work is needed. Federal law enforcement's aggressive pursuit of access to data threatened to upend legislative frameworks. While law enforcement's interests were legitimate, its litigation positions paid insufficient attention to

consumers' stake in secure communications and technology firms' interest in managing information requests from disparate states with widely varying systems of governance. With respect to the U.S.-EU Privacy Shield data transfer agreement, the State Department ombudsperson's lack of independence may not satisfy the CJEU, which in *Schrems v. Data Commissioner* struck down the former data transfer pact. Even in the USA Freedom Act, which returned U.S. domestic call record collection to private firms, the provision for *amici curiae* at the FISC did not go far enough. A full-time public advocate would supply the institutionalized pushback against government positions that structural stewardship requires.

However, initiatives consistent with structural stewardship also require understanding from transnational tribunals. Stewardship on a global scale contemplates coordination between disparate systems of governance. Effectuating that coordination requires that courts accord a measure of deference to transnational agreements, such as Privacy Shield, in keeping with the "margin of appreciation" that European courts have historically shown for national policies on public safety and national security. The trust deficit engendered by Snowden's revelations should inform the degree of deference shown but should not obscure deference's structural importance. Therefore, in assessing Privacy Shield, the CJEU should look to the State Department ombudsperson's course of dealing with EU privacy complaints. The ombudsperson's location in a cabinet department accountable to the U.S. president should trigger more searching inquiry into the ombudsperson's practice. Nevertheless, adherence to the daily practice of constraint is the best test of Privacy Shield's legality.

In sum, the Obama administration faced a daunting series of challenges on surveillance, cybersecurity, and privacy. The administration left both stewardship's discursive and structural aspects as works in progress. That absence of closure might be an emblem of future potential or a marker of promise unfulfilled. The Trump administration may reverse the dialogic direction of the Obama administration and opt for unilateralism across the board. In the alternative, the new administration might perceive engaged rhetoric and frameworks that build productive relationships with multiple stakeholders as both sound governance and good business. Only time will tell.

Reproduced with permission of copyright owner. Further reproduction prohibited without permission.

www.manaraa.com