FIXING PPD-28: IMPLEMENTATION ISSUES AND PROPOSED REVISIONS FOR PRIVACY PROTECTIONS IN SIGNALS INTELLIGENCE

*Peter G. Machtiger**

In 2014, President Barack Obama issued Presidential Policy Directive 28, which extended to foreign nationals some privacy protections in the conduct of signals intelligence (or electronic surveillance for intelligence purposes) previously only offered to U.S. persons. This document constituted part of the U.S. strategy to repair its relationship with the international community after Edward Snowden revealed the true extent of the U.S. surveillance system. PPD-28 was the first document of its kind, promising privacy protections in signals intelligence that no other country had previously offered to non-citizens. This Note examines the implementation of PPD-28 as a window into the complexities of signals intelligence oversight. After examining the issues that arose with PPD-28's implementation, this Note proposes some modest revisions that the U.S. government could embrace to make PPD-28 easier to implement and to oversee, while also rendering it a more effective act of foreign policy. In a world of growing data collection by governments and private companies with mixed levels of regulation or global consensus, proper signals intelligence activities and oversight must promote privacy interests without sacrificing intelligence capabilities.

INTRODUCTION

In January 2014, only seven months after the first reporting emerged on classified information leaked by National Security Agency contractor Edward Snowden,[1] President Barack Obama made an unprecedented speech[2] about electronic surveillance, also known as signals intelligence ("SIGINT"), and issued a policy document called Presidential Policy Directive 28: Signals Intelligence Activities ("PPD-28").[3] The speech and the policy document were unprecedented not merely because they announced any monumental changes in SIGINT policy, but because a U.S. president was speaking publicly about SIGINT at all.

President Obama began his speech by recounting intelligence successes from the Civil War to World War II to the Cold War, before going on to mention some of the Intelligence Community's (IC)[4] darker moments, namely spying on civil rights leaders and political activists during the 1960s.[5] He then turned to the era following the September 11th terrorist attacks, acknowledging controversial policies like enhanced interrogation techniques, yet praising the overall

* J.D. Candidate, 2021, New York University School of Law. The author would like to thank Lisa Monaco and Andrew Weissmann for being invaluable interlocutors during the development of this Note. Additional thanks to Stephen Schulhofer, Ryan Goodman, and Rachel Goldbrenner for their guidance and mentorship in the field of national security law, and to the editors of the *Journal of Legislation & Public Policy* for their incredible feedback. The positions expressed in this Note are the author's alone and do not necessarily reflect the views of any employer or the United States government.

[1] *See Edward Snowden: Leaks that Exposed US Spy Programme*, BBC (Jan. 17, 2017), https://www.bbc.com/news/world-us-canada-23123964.

[2] *See* Barack Obama, President, Remarks by the President on Review of Signals Intelligence (Jan. 17, 2014), https://obamawhitehouse.archives.gov/the-press-office/2014/01/17/remarks-president-review-signals-intelligence.

[3] *See* Press Release, Office of the Press Sec'y, Presidential Policy Directive—Signals Intelligence Activities (PPD-28) (Jan. 17, 2014), https://obamawhitehouse.archives.gov/the-press-office/2014/01/17/presidential-policy-directive-signals-intelligence-activities [hereinafter PPD-28].

[4] The "Intelligence Community" refers to the 17 organizational elements within the U.S. Government that collaborate to conduct intelligence collection and analysis. MICHAEL E. DEVINE, CONG. RESEARCH SERV., IF 10525, DEFENSE PRIMER: NATIONAL AND DEFENSE INTELLIGENCE (2020), https://fas.org/sgp/crs/natsec/IF10525.pdf.

[5] Obama, *supra* note 2.

professionalism of the IC. He concluded by discussing PPD-28's proposals for SIGINT reform, focusing primarily on increasing privacy protections for foreign nationals by restricting bulk SIGINT collection and implementing dissemination and retentions limits for foreign communications in line with those already in place for U.S. communications.[6] By covering both the shortcomings and successes of the IC, the speech became a sort of Rorschach test[7] in which those who identified as more civil liberties-minded and those who identified as more security-minded both discerned support for their cause.

The framework of civil liberties and security as opposing options in a zero-sum game is a long-standing but unhelpful view that fails to capture a range of practices that both protect privacy and strengthen security. Surrendering some amount of one does not necessarily increase the other, and it is possible to strive for both to some extent.[8] Three months after the Obama Administration published PPD-28, Secretary of State John Kerry tried to flesh out the idea that privacy and security are not mutually exclusive by presenting four "universal" principles for surveillance: (1) rule of law; (2) legitimate purpose; (3) oversight; and (4) transparency.[9] Like President Obama's speech, these principles read as largely uncontroversial for both self-proclaimed civil libertarians and the more security-minded. Thus, Kerry's principles can provide a common foundation upon which to consider proposals to update PPD-28 that will be broadly well-received. Reform proposals that cannot connect back to one of these four principles will likely struggle to receive widespread support.

This Note will examine how PPD-28 and its resulting implementation by the National Security Agency ("NSA"), Central Intelligence Agency ("CIA"), and Federal Bureau of Investigation ("FBI") achieved only modest privacy improvements and will evaluate potential adjustments going forward. In doing so, this Note will not come down on the side of "civil liberties" or "security," but look for ways to improve both. Part I will explain what PPD-28 is, its legal effect, and why it is important, and also contextualize its legal effect and political importance in the larger landscape of American and

[6] *Id*.

[7] A Rorschach test is a psychological test where subjects are shown an inkblot and asked to describe what they see. *See* Mike Drayton, *What's Behind the Rorschach Inkblot Test?*, BBC (July 25, 2012), https://www.bbc.com/news/magazine-18952667.

[8] ADAM KLEIN, MICHÈLE FLOURNOY & RICHARD FONTAINE, SURVEILLANCE POLICY: A PRAGMATIC AGENDA FOR 2017 AND BEYOND, CTR. FOR NEW AM. SEC., at 4 (Dec. 12, 2016), https://www.cnas.org/publications/reports/surveillance-policy.

[9] *Id.* at 26.

European[10] rhetoric about privacy and surveillance. Part II is a deep-dive into some issues with the implementation of PPD-28, including definitional problems; the confusion of intelligence agencies facing newly-required querying, dissemination, and retention procedures, and the resulting differences in the implementing procedures of each agency; and how effectively the intelligence agencies have adopted PPD-28's broader principles. Part III will propose some improvements for a potential next iteration of PPD-28. These include a definitional section, clarification regarding retention limitations, a potential demand for reciprocity, a larger public affairs campaign, increased oversight by all three branches of government, a slight increase in transparency, and potential legislative action. Finally, Part IV will briefly examine how the growth of collectable data resulting from the growth of electronic communication is affecting both individual privacy and how intelligence agencies conduct analysis.

I.
CONTEXT FOR PPD-28 AND THE SURVEILLANCE OF FOREIGN NATIONALS

A. What is PPD-28?

PPD-28 is an executive branch policy document that lays out safeguards aimed at protecting the privacy interests of foreign nationals whose communications are incidentally collected by American intelligence agencies in their surveillance of other foreign nationals who may pose a security threat.[11] As technology has evolved, a singular global communications infrastructure has increasingly transmitted both innocuous private personal communications and important foreign intelligence information, often in formats that render the two inextricable in normal SIGINT data collection. PPD-28 acknowledges this challenge and seeks to articulate principles for why, whether, when, and how the U.S. conducts SIGINT activities for foreign intelligence and counterintelligence purposes, while upholding America's

[10] This Note addresses only American and European rhetoric because the most significant litigation to arise over U.S. surveillance practices has taken place in the Court of Justice for the European Union. *See, e.g.*, Case C-311/18, Data Protection Commissioner v. Facebook Ireland Ltd., Maximilian Schrems (*Schrems II*), ECLI:EU:C:2020:559 (E.C.J. 2020).

[11] Cameron Kerry & Alan Charles Raul, *The Economic Case for Preserving PPD-28 and Privacy Shield*, LAWFARE (Jan. 17. 2017, 3:19 PM), https://www.lawfareblog.com/economic-case-preserving-ppd-28-and-privacy-shield.

commitment to democratic principles, universal human rights, global trade, privacy, and civil liberties.[12]

PPD-28 purports to address a litany of concerns offered by its White House authors: risks to U.S. relationships with partner nations; the economic impact of a loss of international trust in U.S. companies and the "decreased willingness of other nations to participate in international data sharing, privacy, and regulatory regimes"; loss of credibility in U.S. commitments to a secure global internet; and the protection of intelligence sources and methods.[13] It also emphasizes the principle that all persons, regardless of nationality, have "legitimate privacy interests in the handling of their personal information."[14] As President Obama summarized: "[J]ust as we balance security and privacy at home, our global leadership demands that we balance our security requirements against our need to maintain the trust and cooperation among people and leaders around the world."[15]

To address the concerns listed above, PPD-28 includes six sections[16]: Sec. 1 – Principles Governing the Collection of Signals Intelligence; Sec. 2 – Limitations on the Use of Signals Intelligence Collected in Bulk; Sec. 3 – Refining the Process for Collecting Signals Intelligence; Sec. 4 – Safeguarding Personal Information Collected Through Signals Intelligence (which includes most of the implementing policies); Sec. 5 – Reports; Sec. 6 – General Provisions.

Each of these sections contains various significant policies. Part II will examine these policies in greater depth, but some brief examples include: government entities must delete the collected personal information of foreign nationals after five years unless it falls within certain exceptions; government actors can only use data collected in bulk for certain enumerated purposes; the State Department must designate a senior point person to respond to SIGINT concerns raised by foreign governments; and SIGINT collection should be tailored as feasible to respect the privacy interests of innocent foreign nationals.[17]

B. Legal Effect of PPD-28

PPD-28, as a presidential directive, has "the same substantive legal effect as an executive order" and remains in effect even upon a

[12] *Id.*
[13] PPD-28, *supra* note 3.
[14] *Id.*
[15] Obama, *supra* note 2.
[16] PPD-28 also includes a classified annex. *See* PPD-28, *supra* note 3.
[17] *See generally* PPD-28, *supra* note 3.

change of administration.[18] Executive orders have the force and effect of law "if the presidential action is based on power vested in the President by the U.S. Constitution or delegated to the President by Congress."[19] Presidents are "free to revoke, modify, or supersede" any orders issued by a predecessor,[20] although PPD-28 has remained entirely intact and unchanged thus far.[21] To provide greater stability, Congress may choose to codify a presidential order (as written or with modifications),[22] but for now, Congress has not turned PPD-28 into legislation. Thus, while PPD-28 still has the force of law in its current form, any presidential administration may modify it to clarify, update, or change its provisions.

C. Reactions to PPD-28

In the aftermath of President Obama's speech and the publication of PPD-28, disagreements arose between those who saw the new document as a significant step forward for privacy protections and those who viewed it as a symbolic gesture that ultimately did little to alter the practices of the IC. Some called the speech a "fierce defense of [the NSA]" and "a big win for the intelligence community."[23] The New York Times Editorial Board, while declaring the speech an admission by President Obama that he had erred in defending the intelligence collection programs exposed to the public by Edward Snowden, still called on President Obama to build even stronger privacy protections.[24] A former privacy official in the IC called PPD-28 a "major paradigm shift" for the privacy rights of foreign nationals, while acknowledging that it "may make only modest changes to surveillance

[18] Legal Effectiveness of a Presidential Directive, As Compared to an Executive Order, 24 Op. O.L.C. 29, 29 (2000).

[19] VIVIAN S. CHU & TODD GARVEY, CONG. RESEARCH SERV., RS20846, EXECUTIVE ORDERS: ISSUANCE, MODIFICATION, AND REVOCATION 1 (2014).

[20] *Id.* at 7.

[21] OFFICE OF THE DIR. OF NAT'L INTELLIGENCE, STATUS OF THE IMPLEMENTATION OF PPD-28: RESPONSE TO THE PCLOB'S REPORT (2018), 4 (Oct. 2018), https://fas.org/irp/offdocs/pclob-ppd28-response.pdf [hereinafter STATUS OF THE IMPLEMENTATION OF PPD-28] ("In 2017, the Trump Administration conducted an interagency review of PPD-28 and determined that it should remain in place.")

[22] CHU & GARVEY, *supra* note 19, at 10.

[23] Benjamin Wittes, *The President's Speech and PPD-28: A Guide for the Perplexed*, LAWFARE (Jan. 20, 2014, 11:02 AM), https://www.lawfareblog.com/presidents-speech-and-ppd-28-guide-perplexed.

[24] *See* Editorial Board, Editorial, *The President on Mass Surveillance*, N.Y. TIMES (Jan. 17, 2014), https://nyti.ms/1axNazd.

practices in the short run."[25] Harvard Law School professor and former head of the Office of Legal Counsel, Jack Goldsmith, described PPD-28 as lacking "sharp teeth" and wrote that "while it has reportedly been a pain to implement, [it] will not likely have a material impact on U.S. collection practices."[26] But, he did note that "the United States can now proudly and truthfully claim to have the most robust protections for non-citizens of any signals collection agency in the world."[27]

While seemingly at odds, all of these reactions are reconcilable. PPD-28 is both a significant rhetorical statement on the side of privacy protection and a policy document that seems to change very little in practice about U.S. SIGINT activities.

D. The Importance of PPD-28

1. PPD-28 is the first document of its kind

PPD-28 is unprecedented in that it extends to foreign nationals certain privacy protections previously afforded only to U.S. citizens.[28] It constitutes a bold step towards establishing global norms for privacy protections in foreign surveillance, a topic most countries typically avoid discussing. PPD-28's statement that "all persons should be treated with dignity and respect, regardless of their nationality or wherever they might reside, and that all persons have legitimate privacy interests in the handling of their personal information"[29] derives from international human rights law,[30] although no government had ever translated the concept of universal dignity and privacy into self-imposed privacy protections for foreign citizens in SIGINT.

---

[25] Timothy Edgar, *Why Should We Buy Into The Notion That the United States Doesn't Care About Privacy?*, LAWFARE (Feb. 23, 2015, 8:23 AM), https://www.lawfareblog.com/why-should-we-buy-notion-united-states-doesnt-care-about-privacy.

[26] Jack Goldsmith, *Three Years Later: How Snowden Helped the U.S. Intelligence Community*, LAWFARE (June 6, 2016, 9:32 AM), https://www.lawfareblog.com/three-years-later-how-snowden-helped-us-intelligence-community.

[27] *Id.*

[28] Obama, *supra* note 2.

[29] PPD-28, *supra* note 3.

[30] Peter Swire, Jesse Woo & Deven Desai, *The Important, Justifiable and Constrained Role of Nationality in Foreign Intelligence Surveillance*, LAWFARE (Jan. 11, 2019, 9:00 AM), https://www.lawfareblog.com/important-justifiable-and-constrained-role-nationality-foreign-intelligence-surveillance-0.

No other country has committed to broader protections for the privacy interests of foreigners in SIGINT;[31] the next most protective policy is a German law containing special protections for European Union ("EU") institutions, member states, and citizens, but the law does not extend those protections to non-EU entities, including Americans.[32] German law may shortly overtake the protections of PPD-28, as a German court opinion published in May 2020 found that surveillance of foreigners conducted by the German Federal Intelligence Service violated German law protecting the fundamental right to privacy of telecommunications and the freedom of the press.[33] The court also found that the German government must provide greater safeguards for intelligence sharing with foreign intelligence services and create an "extensive independent oversight regime."[34] This development may turn out to be the beginning of a trend among Western governments towards adoption of PPD-28-like protections or even greater protections.

Although not part of PPD-28 itself, President Obama announced another unprecedented policy when he revealed that the U.S. would not monitor the communications of the heads of state of our close allies, albeit with a carveout allowing surveillance when "there is a compelling national security purpose."[35] While it remained unclear at the time of his speech how many leaders this exemption from general surveillance would encompass, later reporting indicated that it protected at least 25 heads of state.[36] The announcement likely came in response to the revelation in a set of documents leaked by Edward Snowden that the NSA had conducted surveillance of Chancellor Angela Merkel's personal cell phone, which caused President Obama's approval rating in Germany to fall from 75 percent to 43 percent (and a 2015 poll found that Germans admired Edward Snowden more than they did President

[31] Eric Manpearl, *The Privacy Rights of Non-U.S. Persons in Signals Intelligence*, 29 FLA. J. INT'L L. 303, 341 (2018).

[32] KLEIN ET AL., *supra* note 8, at 52-53.

[33] Bundesverfassungsgericht [BVerfG] [Federal Constitutional Court Press Release No. 37/2020], May 19, 2020, In Their Current Form, Surveillance Powers of the Federal Intelligence Service Regarding Foreign Telecommunications Violate Fundamental Rights of the Basic Law (Ger.), https://www.bundesverfassungsgericht.de/SharedDocs/Pressemitteilungen/EN/2020/bvg20-037.html.

[34] *Id.*

[35] Obama, *supra* note 2.

[36] *See* Paul Rosenzweig, *Which Foreign Leaders Are On the "Do Not Listen" List?*, LAWFARE (Jan. 20, 2014, 12:09 PM), https://www.lawfareblog.com/which-foreign-leaders-are-do-not-listen-list#.

Obama).[37] President Obama's announcement curbing the surveillance of allied heads of state was uniquely responsive to the outrage of foreign citizens, even though such surveillance was common practice internationally.

One might attribute the shock over the revelations concerning the surveillance of Chancellor Merkel to the fact that, as President Obama said in his speech, the U.S. is "held to a different standard," whereas "no one expects China to have an open debate about their surveillance programs, or Russia to take privacy concerns of citizens in other places into account."[38] If the German polling above is representative of overall European sentiment, Europeans do not appear to view the US surveillance policies revealed by Mr. Snowden positively; however, there has not been similar public outrage over the fact that no country in the European Union has yet released a document like PPD-28.[39] PPD-28 marked an important unilateral step by the United States to shape global norms around privacy protections and civil liberties in foreign surveillance.[40]

2. How PPD-28 fits into U.S. vs. EU privacy rhetoric and practice

EU rhetoric and practice concerning privacy serves as crucial context for understanding PPD-28 because European litigation over U.S. surveillance practices has now twice jeopardized U.S.-EU data-

[37] KLEIN ET AL., *supra* note 8, at 18. Brazilian President Dilma Rousseff, who found out that the U.S. had similarly monitored her cell phone, called the surveillance a "violation of human rights and civil liberties" and a "disrespect to national sovereignty." Daniel Byman & Benjamin Wittes, *Reforming the NSA: How to Spy after Snowden*, FOREIGN AFFAIRS, (May/June 2014), at 127, https://www.brookings.edu/articles/reforming-the-nsa-how-to-spy-after-snowden/. While the news of U.S. surveillance of its allies' heads of state apparently shocked German citizens and President Rousseff, many intelligence services in many countries surveil the communications of foreign leaders as much as they are able. James Ball, *NSA Monitored Calls of 35 World Leaders After US Official Handed Over Contacts*, GUARDIAN (Oct. 25, 2013, 2:50 PM), https://www.theguardian.com/world/2013/oct/24/nsa-surveillance-world-leaders-calls. Reporting has indicated that both China and Russia regularly listen in on President Trump's personal cell phone calls, and Israel, a U.S. ally, is allegedly behind the placement of cellphone surveillance devices (known as "StingRays") near the White House to surveil President Trump. Matthew Rosenberg & Maggie Haberman, *When Trump Phones Friends, the Chinese and the Russians Listen and Learn*, N.Y. TIMES (Oct. 24, 2018), https://nyti.ms/2JfsQbL; *see also* Daniel Lippman, *Israel Accused of Planting Mysterious Spy Devices Near the White House*, POLITICO (Sept. 12, 2019, 6:34 PM), https://www.politico.com/story/2019/09/12/israel-white-house-spying-devices-1491351.

[38] Obama, *supra* note 2.

[39] Wittes, *supra* note 23.

[40] Kerry & Raul, *supra* note 11.

sharing agreements that are economically important to both the U.S. and the EU. The publication of PPD-28 demonstrated one effort to protect the intercontinental flow of data by mollifying EU privacy advocates. And yet, members of the EU have offered almost no such reciprocal protections or oversight for their surveillance of U.S. persons.[41] Thus, if PPD-28 can be revised and improved to provide a clear and comprehensive framework for privacy protections in signals intelligence, it may still become the international standard as EU member states seek to adopt protections before potentially facing a legal challenge like the one in Germany's Constitutional Court.

Prior to PPD-28, the U.S. federal government, much like most other national governments, had not published any public document ensuring legal safeguards in surveillance to protect the privacy of foreign persons overseas.[42] The EU is known by those with awareness of privacy law for its General Data Protection Regulation[43] ("GDPR"), but that is a set of consumer privacy rules.[44] The United States has considered proposals[45] to comprehensively address consumer privacy too, but those proposals and the GDPR mostly differ from surveillance and intelligence oversight as a substantive matter.

The EU's strong pro-privacy rhetoric is mainly grounded in human rights law. The Court of Justice of the European Union ("CJEU") requires that all countries that wish to conduct business with companies in the EU must provide "a level of protection of fundamental rights and freedoms that is essentially equivalent to that guaranteed within the European Union."[46] This mandated level of protection cites those

[41] *But see, e.g.*, Press Release No. 37/2020, Bundesverfassungsgericht, *supra* note 33. "U.S. person" is a term of art meaning "a citizen of the United States, an alien lawfully admitted for permanent residence . . . an unincorporated association a substantial number of members of which are citizens of the United States or aliens lawfully admitted for permanent residence, or a corporation which is incorporated in the United States, but does not include a corporation or an association which is a foreign power . . ." 50 U.S.C. § 1801 (2018).

[42] Obama, *supra* note 2.

[43] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC, 2016 O.J. (L 119) 1.

[44] Edgar, *supra* note 25.

[45] Issie Lapowsky, *Kirsten Gillibrand's New Bill Would Establish a US Protection Agency*, PROTOCOL (Feb. 13, 2020), https://www.protocol.com/federal-privacy-agency-gillibrand.

[46] Timothy Edgar, *Final Thoughts on Reforming Surveillance and European Privacy Rules*, LAWFARE (Nov. 8, 2015, 2:19 PM), https://www.lawfareblog.com/final-thoughts-reforming-surveillance-and-european-privacy-rules.

protections provided under the EU's Data Protection Directive, an older data privacy framework, and the Charter of Fundamental Rights of the European Union, which includes "explicit rights to privacy and the protection of personal data."[47] That standard applies to foreign countries like the U.S., even though EU Member States' SIGINT collection practices do not meet the same standard.[48] This incongruity stems from EU law providing that national security is solely the responsibility of its member states, which limits the CJEU's ability to examine the surveillance laws of EU member states.[49] However, there is no provision preventing the CJEU from evaluating the surveillance law of non-EU countries if the opportunity arises.[50]

The complexity of the normative question of whether or not to afford the same privacy protections in surveillance to one's own citizens and foreign citizens, as well as fears that other countries will not reciprocate, might explain countries' hesitation to address the issue. Certain international actors, like the United Nations Special Rapporteur on the right to privacy, espouse a "universalist" view that would apply a universal human right to be free from unjustified surveillance[51] and find asymmetrical privacy protections unlawful.[52] Laying out the normative arguments on both sides, Professor Ryan Goodman has noted that one might justify affording foreign nationals abroad less protection than a surveilling country's own citizens (the pre-PPD-28 status quo) by arguing that: (1) states have fewer tools to detect potential threats abroad than at home (making electronic surveillance more necessary because physical surveillance is less possible); (2) there is less concern about the risks of a "surveillance state" when the state is conducting surveillance abroad rather than domestically; (3) the surveilling government's ability to punish an individual based on the information gathered in surveillance is much le er ss for foreign nationals abroad

[47] Sarah St. Vincent, *Making Privacy a Reality: The Safe Harbor Judgment and Its Consequences for US Surveillance Reform*, CTR. FOR DEMOCRACY & TECH., (Oct. 26, 2015), https://cdt.org/in9sights/making-privacy-a-reality-the-safe-harbor-judgment-and-its-consequences-for-us-surveillance-reform/.

[48] *Id.*

[49] Kenneth Propp, *European Court of Justice Opinion Clouds Future of Transatlantic Commercial Data Transfers*, LAWFARE (Dec. 24, 2019, 8:08 AM), https://www.lawfareblog.com/european-court-justice-opinion-clouds-future-transatlantic-commercial-data-transfers.

[50] *Id.*

[51] Swire et al., *supra* note 30.

[52] Ryan Goodman, *Should Foreign Nationals Get the Same Privacy Protections Under NSA Surveillance—Or Less (or More)?*, JUST SECURITY (Oct. 29, 2014), https://www.justsecurity.org/16797/foreign-nationals-privacy-protections-nsa-surveillance-or-or-more/.

than for individuals domestically.[53] Conversely, one might argue that foreign nationals abroad should have greater privacy protections because: (1) foreign nationals abroad cannot voice concerns about the surveillance via the political process the way domestic citizens can; (2) foreign nationals abroad should not be expected to be aware of other countries' surveillance laws the way a domestic citizen is "on notice" about their own country's surveillance; (3) it is much harder for foreign nationals abroad to obtain a remedy if harmed by surveillance than for domestic citizens.[54] PPD-28 certainly does not give foreign nationals *greater* privacy protections than U.S. persons, but its unreciprocated increase of privacy protections for foreign nationals was a normative stance on the above debate that the U.S. had not taken before. Hesitation by many countries to apply the "universalist" view likely results from the complexity of the issues and a fear of lack of reciprocity.[55]

When the CJEU in *Schrems v. Data Protection Commissioner* ("*Schrems I*")[56]—seemingly fueled by Snowden-related revelations about NSA surveillance—struck down the Safe Harbor agreement that facilitated the transfer of personal information from Europe to the U.S., the U.S. had to reevaluate its signals intelligence activities.[57] Notably, however, France, Germany, the United Kingdom, and the Netherlands all practice (or practiced at the time of the decision) the same type of "generalized" NSA surveillance to which the CJEU objected in *Schrems I*.[58] European courts have cleared the structural safeguards in these countries as satisfying the European Convention on Human Rights, even though the European frameworks are not as rigorous as the requirements of the Foreign Intelligence Surveillance Act ("FISA"), the U.S. legislation that lays out the legal framework for how the U.S. government must conduct foreign intelligence surveillance.[59] The further irony of *Schrems I* is that the U.S. government has always controlled surveillance of data transferred to the U.S. more strictly than surveillance of data that remains overseas.[60]

---

[53] *Id.*

[54] *Id.*

[55] *Episode 283: Is Intelligence "Reform" a Self-Licking Ice Cream Cone and Compliance Trap?*, THE CYBERLAW PODCAST (Oct. 21, 2019), https://www.steptoe.com/podcasts/TheCyberlawPodcast-283.mp3.

[56] Case C-362/14, Maximillian Schrems v. Data Protection Comm'r, 2015 E.C.R. I-35.

[57] *See* Edgar, *supra* note 46.

[58] KLEIN ET AL., *supra* note 8, at 53.

[59] Edgar, *supra* note 25.

[60] Edgar, *supra* note 46.

Regardless of these realities, the U.S. needed to implement SIGINT reform after *Schrems I* to protect the ability of data to flow between the U.S. and the EU, America's largest trading partner with approximately $260 billion in annual transatlantic trade via digital services.[61] PPD-28 constituted a key part of this reform, which led to a new U.S.-EU agreement called the Privacy Shield.[62] PPD-28 remains relevant because the same plaintiff from *Schrems I* again challenged U.S. surveillance practices before the CJEU and again prevailed in a case titled "*Schrems II*," thereby invalidating the Privacy Shield.[63] In the EU advocate general's opinion (which is not binding, but generally serves as a bellwether for the eventual CJEU decision), the advocate general noted that PPD-28 does not provide the degree of legal foreseeability required by EU law because of its status as a presidential directive.[64] However, the advocate general also analyzed U.S. surveillance programs more pragmatically than in previous cases, citing opinions of the European Court of Human Rights, which found bulk collection programs[65] lawful if accompanied by sufficient protections.[66] Finally, the advocate general expressed concern about the general lack of standing to sue in U.S. courts over NSA surveillance, lack of individual judicial authorization for collection pursuant to FISA Section 702,[67] lack of notice to individuals after surveillance, and worry that the ombudsperson redress mechanism built into the Privacy Shield agreement lacks independence.[68] The CJEU picked up all of these concerns in its final decision, noting that the bulk collection allowed by PPD-28 (via Executive Order 12333 ("EO 12333")) and the lack of a

[61] Kerry & Raul, *supra* note 11.

[62] Letter from Congressman F. James Sensenbrenner, Chairman, Subcomm. on Crime, Terrorism, Homeland Sec., and Investigations, House Judiciary Comm., to President-elect Donald J. Trump (Dec. 20, 2016), https://epic.org/privacy/surveillance/Sensenbrenner-PS-letter.pdf.

[63] Case C-311/18, Data Protection Commissioner v. Facebook Ireland Ltd., Maximilian Schrems (*Schrems II*), ECLI:EU:C:2020:559 (E.C.J. 2020).

[64] Propp, *supra* note 49.

[65] *See infra* Section II.A.2.

[66] Peter Swire, *Foreign Intelligence and Other Issues in the Initial Opinion in Schrems II*, LAWFARE (Dec. 23, 2019, 9:36 AM), https://www.lawfareblog.com/foreign-intelligence-and-other-issues-initial-opinion-schrems-ii [https://perma.cc/NEB7-CXH6].

[67] FISA Section 702 is the program that governs the collection from within the U.S. of the communications of non-U.S. persons located abroad. FISA Amendments Act of 2008, Pub. L. No. 110-261, § 702, 122 Stat. 2436, 2438 (2008) (codified at 50 U.S.C. § 1881a (2018)).

[68] Swire, *supra* note 66.

robust redress mechanism for those that seek to challenge U.S. surveillance did not amount to an adequate level of data protection.[69]

In sum, European reactions to Edward Snowden's divulgence of U.S. surveillance practices served as a key instigator of PPD-28. Europe still takes issue with U.S. surveillance practices, although the relatively robust, albeit imperfect, protections afforded to foreign nationals under PPD-28 have gone largely unreciprocated by European nations.[70]

3. Privacy protections for foreigners may actually protect Americans

While PPD-28 provides privacy protections for foreign nationals on paper, it also protects Americans in practice, which might make the document more compelling to ordinary American citizens. PPD-28 largely affects overseas surveillance activities conducted under EO 12333, a Reagan-era document that generally governs intelligence collection.[71] Although non-experts generally think this surveillance framework has little impact on Americans,[72] government officials have estimated that the communications and data of up to hundreds of millions of Americans are collected under EO 12333.[73] With the proliferation of cloud-based storage, more and more data uploaded by Americans on U.S. soil end up on servers all over the world.[74] Similarly, third party ads hosted on U.S. websites can track the internet habits of Americans and send those data to servers overseas.[75] As a result, even "targeted" surveillance conducted by the NSA entirely overseas may end up capturing the personal information of Americans.[76] This kind of entirely overseas surveillance conducted under EO 12333 is not subject

[69] Case C-311/18, Data Protection Commissioner v. Facebook Ireland Ltd., Maximilian Schrems (*Schrems II*), ECLI:EU:C:2020:559 (E.C.J. 2020), at ¶ 83–84.

[70] This section does not address the CJEU decision in Case C-623/17, *Privacy International v. Sec'y of State for Foreign and Commonwealth Affairs and Others*, 2020 E.C.R. 790, which was delivered shortly before this Note went to print. It is yet to be seen but likely that the case will affect the electronic surveillance practices of EU Member States.

[71] AMOS TOH, FAIZA PATEL & ELIZABETH GOITEIN, OVERSEAS SURVEILLANCE IN AN INTERCONNECTED WORLD 12 (Mar. 16, 2016), https://www.brennancenter.org/sites/default/files/publications/Overseas_Surveillance_in_an_Interconnected_World.pdf [https://perma.cc/FM4P-HTPG].

[72] Elizabeth Goitein, *Overseas Surveillance in an Interconnected World*, JUST SECURITY (Mar. 17, 2016), https://www.justsecurity.org/29994/overseas-surveillance-interconnected-world/ [[https://perma.cc/K4WW-3DV8].

[73] TOH ET AL., *supra* note 71, at 8.

[74] *Id.* at 10.

[75] *Id.*

[76] *Id.* at 1-2.

to judicial oversight like surveillance conducted under FISA,[77] so PPD-28 may play an important role in protecting the privacy interests of Americans as well as foreign nationals under these programs.

Admittedly, the practical protection of U.S. persons' privacy may seem irrelevant to those unconcerned by the incidental collection of American communications and data under EO 12333. For example, Judge Richard Posner takes the general view that the number of people at risk from crime and terrorism is much greater than the number of people who face a higher risk of being falsely accused when protections of civil liberties are modestly curtailed.[78] Thus, the benefits to security under EO 12333 may be worth the risk of incidental collection of innocent people's data. For those in this camp, PPD-28 may seem less worthwhile if it in any way diminishes the overall surveillance capacity of the U.S. government.

***

President Obama's speech and PPD-28 were rhetorically significant as unprecedented steps towards establishing international norms for privacy protections in foreign surveillance, even though PPD-28's substance only led to a modest curtailment of U.S. surveillance practices.[79] In this way, it has been most accurately characterized as an "exceedingly-clever [sic] document" that "conveys and writes into policy a great deal of values without constraining a great deal of practice."[80]

II. ISSUES WITH PPD-28'S IMPLEMENTATION

Assessing the practical impact of PPD-28 is key to forecasting what future litigation might arise abroad and what revisions might be necessary to achieve U.S. foreign policy goals. Based on the documents released by the intelligence agencies, the public implementation of PPD-28 seemed to successfully address the concerns the document purported to address.[81] However, upon closer examination, PPD-28's implementation across various intelligence agencies reveals some of the document's key flaws. These flaws do not imply any deception on

[77] *Id.*
[78] RICHARD A. POSNER, NOT A SUICIDE PACT: THE CONSTITUTION IN A TIME OF NATIONAL EMERGENCY 41 (2006).
[79] *See infra* Section II.
[80] Wittes, *supra* note 23.
[81] *See supra* Section I.A.

behalf of the implementing agencies; this is not a case of the IC secretly defying White House policy decisions. The NSA admitted that it developed its implementation policies and procedures in conjunction with the White House,[82] and it is reasonable to assume that the other intelligence agencies similarly consulted the authors of PPD-28 during the creation of their own procedures. Thus, the aspects of PPD-28's implementation that fall short of what President Obama promised in his speech primarily reflect a need to expand the capacity of intelligence oversight entities.

Because of the classified nature of most intelligence work, especially SIGINT, it is impossible for the public to know how intelligence agencies have *actually* implemented these policies and procedures. We can only look at the published implementing documents called for by Section 4 of PPD-28 and read what each intelligence agency has said it will do.[83] Further, the report on PPD-28 published by the Privacy and Civil Liberties Oversight Board ("PCLOB"), the U.S. government's only independent civil liberties oversight group, relies mostly on these same documents, unlike some of its more comprehensive reports on other major intelligence programs.[84]

Inadvertent incongruencies between different agencies' implementation policies reveal fundamental gaps and ambiguities in PPD-28's provisions regarding data retention, information dissemination, and querying procedures. These gaps and

---

[82] NAT'L SEC. AGENCY, PPD-28 SECTION 4 PROCEDURES, (Jan. 12, 2015), https://www.nsa.gov/Portals/70/documents/news-features/declassified-documents/nsa-css-policies/PPD-28.pdf [hereinafter NSA PPD-28 PROCEDURES].

[83] OFFICE OF THE DIR. NAT'L INTELLIGENCE, IMPLEMENTING PROCEDURES UNDER PRESIDENTIAL POLICY DIRECTIVE-28, SIGNALS INTELLIGENCE ACTIVITIES (PPD-28) (May 16, 2017), https://www.dni.gov/files/CLPT/documents/Chart-of-PPD-28-Procedures_May-2017.pdf.

[84] PRIVACY & CIVIL LIBERTIES OVERSIGHT BD., REPORT TO THE PRESIDENT ON THE IMPLEMENTATION OF PRESIDENTIAL POLICY DIRECTIVE 28: SIGNALS INTELLIGENCE ACTIVITIES 12 (Oct. 16, 2018), https://documents.pclob.gov/prod/Documents/OversightReport/16f31ea4-3536-43d6-ba51-b19f99c86589/PPD-28%20Report%20(for%20FOIA%20Release).pdf [https://perma.cc/2XGS-Y9KX] [hereinafter "PCLOB PPD-28 REPORT"]; *see also* Ashley Gorski, *Secret Government Report Shows Gaping Holes in Privacy Protections from U.S. Surveillance*, ACLU (Oct. 18, 2018, 11:15 AM), https://www.aclu.org/blog/national-security/privacy-and-surveillance/secret-government-report-shows-gaping-holes-privacy; *see also* Elizabeth Goitein, *The Privacy and Civil Liberties Oversight Board's Disappointing Report on PPD-28 Implementation*, JUST SECURITY (Oct. 24, 2018), https://www.justsecurity.org/61199/privacy-civil-liberties-oversight-boards-disappointing-report-ppd-28-implementation/.

incongruencies, in turn, result in multiple problems that undermine the efficacy of PPD-28 in practice. First, conflicts between different agencies' implementation procedures can hinder the type of inter-agency cooperation that has proven essential to identifying threats in the post-9/11 intelligence environment. Second, ambiguity in the wording of PPD-28 undermines the credibility of oversight efforts because government actors conducting oversight cannot be sure that agencies are correctly implementing tasks if the mandated tasks are unclear. It is also difficult to ascertain how to implement—or how and under what circumstances to depart from—some of PPD-28's loftier principles, like those calling for SIGINT activities to be tailored "as feasible" or those prohibiting the use of SIGINT to disadvantage persons based on certain personal characteristics. The following sections will address these issues in turn.

A. The Lack of a Definition Section Has Led to Ambiguity

PPD-28's failure to define certain key terms has caused some of the confusion in implementation, exacerbated by the fact that different members of the IC define certain terms of art differently. If different agencies interpret the language in documents like PPD-28 differently because of the lack of a section outlining definitions of key terms, they will not all be executing exactly what President Obama directed, complicating oversight efforts.

Like in many regulatory areas, definitional sections are central to signals intelligence procedures because many common terms are used across each of the seventeen organizations that make up the IC, but with slightly different meanings. The few terms defined in PPD-28 may provide a clue as to how to interpret some key undefined terms in the document. The definitions PPD-28 *does* provide, including for "foreign intelligence" and "personal information," come from EO 12333.[85] "Foreign intelligence" is defined as "information relating to the capabilities, intentions, or activities of foreign governments or elements thereof, foreign organizations, foreign persons, or international terrorists."[86] There seem to be almost no foreign communications that could not qualify as foreign intelligence under this definition, but, in that regard, it is very clear: any information relating to the intentions and activities of foreign persons counts as foreign intelligence. PPD-28

[85] Exec. Order No. 12,333, 3 C.F.R 200, *as amended* by Exec. Order No. 13,284, 68 Fed. Reg. 4085 (2003), Exec. Order No. 13,355, 69 Fed. Reg. 53,593 (2004), Exec. Order No. 13,470, 73 Fed. Reg. 45,325 (2008) § 3.5 [hereinafter "EO 12333"].
[86] PPD-28, *supra* note 3, at n.2; *see also* EO 12333, *supra* note 85.

also adopts EO 12333's definition of "personal information," which is equally broad and states that it covers the same types of information for both U.S. and non-U.S. persons.[87] "Personal information" encompasses communications content, metadata, geolocation data, and more.[88] For example, the NSA's CO-TRAVELER program created a database of the locations of hundreds of millions of cell phones outside the U.S., and this counts as "personal information."[89] Like the definition of foreign intelligence, the breadth of the definition of personal information makes it fairly clear: essentially any communications count.

1. PPD-28 does not define "signals intelligence"

Unfortunately, although PPD-28 is titled "Signals Intelligence Activities," the document fails to define "signals intelligence," which has led to unnecessary confusion for the implementing agencies. This failure to define "signals intelligence" creates a threshold problem of unclear applicability because, without a definition of "signals intelligence," PPD-28's implementing agencies cannot know exactly which programs count as "signals intelligence" activities and therefore require the new procedures. As described in the PCLOB report, "it was left to each IC element to determine how to apply PPD-28 to its respective activities," leading to variations in application that undermined both proper oversight and inter-agency collaboration.[90]

Several sources that predate PPD-28 provide potentially useful clues as to the intended meaning of "signals intelligence" in PPD-28. One source is EO 12333's definitional section, which PPD-28's authors referenced for "foreign intelligence" and "personal information."[91] The closest phrase in EO 12333's definitional section would be "electronic surveillance," which it defines as "acquisition of a nonpublic communication by electronic means without the consent of a person who is a party to an electronic communication or, in the case of a nonelectronic communication, without the consent of a person who is visibly present at the place of communication, but not including the use of radio direction-finding equipment solely to determine the location of a transmitter."[92] However, this definition would be too broad for

[87] PPD-28, *supra* note 3, at § 4 n.7; *see also* EO 12333, *supra* note 85, at § 2.3.
[88] TOH ET AL., *supra* note 71, at 4.
[89] *Id.* at 7.
[90] PCLOB PPD-28 REPORT, *supra* note 84.
[91] *See supra* Section II.A.
[92] EO 12333, *supra* note 85, at § 3.5.

"signals intelligence" in the context of PPD-28, as it would seemingly include all surveillance conducted under FISA (including surveillance of U.S. person communications similar to criminal wiretaps), which seems contrary to PPD-28, a document concerned with the privacy of *foreign* nationals.

The practice of the NSA, a signals intelligence agency, can also help identify a definition of "signals intelligence" because defining "signals intelligence" is necessary for the NSA to understand its own mandate. The NSA collects phone calls, e-mails, web chats, web-browsing history, pictures, documents, webcam photos, web searches, website and advertising analytics, social media traffic, keystrokes, usernames and passwords, online video chats, and more.[93] In internal training slides, the NSA defines "Raw SIGINT" as "[r]esults of collection BEFORE the information has been evaluated for foreign intelligence AND minimization purposes, per USSID CR1610."[94] This definition does not illustrate which activities should be considered "signals intelligence" activities, although it does point out that any attempt at defining "signals intelligence" should differentiate between "raw" SIGINT and SIGINT that has undergone some level of processing.

To complicate EO 12333's definition of "electronic surveillance," the "FBI states in its PPD-28 implementing procedures that it does not conduct signals intelligence."[95] Nevertheless, the FBI interprets footnote 6 of PPD-28 to mean that it should apply PPD-28 to communications collected under FISA Section 702, a "non-signals intelligence activity."[96] The NSA and CIA also apply PPD-28 to FISA Section 702 communications.[97] However, the PCLOB report notes that the FBI does not apply PPD-28 to FISA Sections 704 or 705(b), or to FISA Title I, because "those surveillances require an individualized

[93] TOH ET AL., *supra* note 71, at 5.

[94] OFFICE OF GEN. COUNCIL, NAT'L SEC. AGENCY, AUGUST 2009 NSA CRYPTOLOGICAL SCHOOL COURSE 65 (Sept. 10, 2013), https://www.dni.gov/files/documents/1118/CLEANED021.extracts.%20Minimization%20Pr...cted%20from%20file%20021-Sealed.pdf [https://perma.cc/7QCM-TSJN]. "Minimization" in this quotation refers to procedures that protect the identity of U.S. persons before the intelligence is disseminated to others. *See* 50 U.S.C. § 1801(h) (2018).

[95] PCLOB PPD-28 REPORT, *supra* note 83, at 4.

[96] *Id.*

[97] *Id.*

finding of probable cause;[98] in contrast, the NSA applies PPD-28 to "all of the above."[99]

Based on the ambiguous definitions above, electronic surveillance activities conducted under FISA do *not* qualify as signals intelligence activities, but the NSA, CIA, and FBI apply PPD-28 ("Signals Intelligence Activities") to FISA Section 702 communications anyway. And, the FBI does not think it should do the same for FISA Title I information, but the NSA applies PPD-28 to all FISA information. After the PCLOB published its report on PPD-28, the Office of the Director of National Intelligence clarified that Section 702 collection "is considered SIGINT subject to the requirements of PPD-28," but reiterated that "the identity of the programs and activities to which PPD-28 applies remains classified to protect national security."[100] The simple act of explicitly defining "signals intelligence activities" at the outset of PPD-28—rather than leaving interpretation up to the various entities that may or may not believe themselves to be tasked with its implementation—could have prevented all of this confusion and these discrepancies.

2. PPD-28's treatment of "bulk" and "targeted" collection still allows for massive data collection

PPD-28 called for a reduction in "bulk" signals intelligence collection; however, the exceptions it carved out from the bulk collection restrictions that it enacted, as well as the potential breadth of "targeted" collection, ultimately resulted in only slightly greater privacy protections for foreign communications. Potentially in response to some of the European reactions to U.S. surveillance activities revealed by Edward Snowden,[101] PPD-28 seeks to rein in "bulk collection," which PPD-28 defines as "the authorized collection of large quantities of signals intelligence data which, due to technical or operational considerations, is acquired without the use of discriminants (e.g., specific identifiers, selection terms, etc.)."[102] However, PPD-28's restrictions on bulk collection have only limited effect due to the practically amorphous distinction between "bulk collection" and "targeted collection" (i.e. collection that uses a "discriminant," which might be a phone number or email, but can also be a broad "selection

[98] *Id.* at 13.
[99] *Id.* at 21 (Separate Statement of Board Members Rachel Brand and Elisabeth Collins).
[100] STATUS OF THE IMPLEMENTATION OF PPD-28, *supra* note 21, at 5.
[101] *See supra* Section I.D.2.
[102] PPD-28, *supra* note 3, at § 2 n.5.

term" such as "Russia" or "ISIS"), as well as the breadth of the exceptions to the bulk collection restrictions. The uncertainty around how much PPD-28 actually reins in bulk collection may affect the EU's analysis of how much PPD-28 actually protects the privacy of foreign nationals not suspected of malicious activity. PPD-28 acknowledges that both benign and potentially threatening communications increasingly are sent via the same network infrastructure and, thus, it tries to apply restrictions to collecting this information indiscriminately, regardless of the nationality of the sender.[103] Clarifying the line between bulk and targeted collection and narrowing the exceptions to the bulk collection restrictions would likely help technical experts create systems that can make the collection process more efficient and privacy-protective.

The first difficulty with identifying the line between bulk and targeted collection is that "collection" itself does not have a standardized meaning across the IC. The old Department of Defense "U.S. Persons Procedures" manual (DoD 5240.1-R) said that information was "collected" only when it was processed into an "intelligible form."[104] The updated 2016 manual (DoD 5240.01) says that "information is collected when it is received by a Defense Intelligence Component," regardless of how it was "obtained or acquired."[105] But, while the NSA is a component of the Defense Department, it has its own manual. The same activity the old DoD manual (DoD 5240.1-R) calls "collection," with its "intelligible form" requirement, is referred to as "interception" in the NSA's manual.[106] For the NSA, "collection" occurs when an analyst intentionally "tasks" or selects a communication "for subsequent processing aimed at reporting or retention as a file record."[107] In sum, the new DoD manual calls it "collection" when they receive the information, the old DoD manual would have waited until the information was processed into an

[103] PPD-28, *supra* note 3, at § 2.

[104] Diana Lee & Paulina Perlin, *What Does 'Collection' Mean? Discretion and Confusion in the Intelligence Community*, LAWFARE (July 17, 2019, 8:13 AM), https://www.lawfareblog.com/what-does-collection-mean-discretion-and-confusion-intelligence-community [https://perma.cc/DN44-R5AM].

[105] *Id.*; *see generally* Diana Lee, Paulina Perlin, & Joe Schottenfeld, *Gathering Intelligence: Drifting Meaning and the Modern Surveillance Apparatus*, 10 J. NAT'L SECURITY L. & POL'Y 77 (2019).

[106] Lee et al., *supra* note 104.

[107] 71*Id.* (citing NAT'L SEC. AGENCY, USSID 18: LEGAL COMPLIANCE AND U.S. PERSONS MINIMIZATION PROCEDURES § 9.2 (Jan. 15, 2011)).

intelligible form, and the NSA manual waits until an analyst is looking at the information.[108]

PPD-28 does not delineate the contours of "collection," but, read in its entirety, the document seems to suggest a meaning of "collection" similar to the old DoD definition with the "intelligible form" requirement. Section 2 of PPD-28 only permits the bulk collection of nonpublicly available signals intelligence when such collection is necessary to detect and counter the following: (1) "espionage and other threats and activities directed by foreign powers or their intelligence services against the United States and its interests"; (2) "threats to the United States and its interests from terrorism"; (3) "threats to the United States and its interests from the development, possession, proliferation, or use of weapons of mass destruction"; (4) "cybersecurity threats"; (5) "threats to U.S. or allied Armed Forces or other U.S. or allied personnel"; and (6) "transnational criminal threats, including illicit finance and sanctions evasion related to the other purposes named in this section."[109] Going through each requirement, these provisions ultimately do not appear very restrictive. First, these restrictions apply only to "nonpublicly available" information, so all public social media information could presumably be collected in bulk without restriction (and potentially much more information depending on how one defines "nonpublicly available"[110]). Moreover, the U.S. can use data collected in bulk "for the purposes of detecting and countering . . . other threats and activities directed by foreign powers," "threats to . . . U.S. or allied personnel," and "transnational criminal threats."[111] This seems to encompass almost every reason an intelligence agency would want to collect information and effectively just prohibits the bulk collection of unhelpful information.[112] This list is also subject to change, as PPD-28 calls for the Director of National Intelligence ("DNI") to update the list as necessary,[113] and the intelligence agencies themselves have adopted

[108] Lee & Perlin, *supra* note 104.
[109] PPD-28, *supra* note 3, at § 2.
[110] *See infra* Section IV.B.
[111] PPD-28, *supra* note 3.
[112] Wittes, *supra* note 23 ("In other words, bulk SIGINT can be used only for legitimate and identified national security purposes. If you work for a SIGINT group that's collecting material in bulk for no discernible reason, this may be a problem, but I don't think that's really happening.").
[113] PPD-28, *supra* note 3, at § 2.

procedures to advise the DNI on recommended additions or removals.[114]

It is also worth noting that these restrictions apply only to "bulk" collection, but not to "targeted" collection. U.S. intelligence agencies have adopted essentially verbatim definitions of "bulk collection" as PPD-28.[115] Collection that is targeted can still yield enormous amounts of data.[116] A committee of technical experts convened by the National Research Council (as called for in Section 5(d) of PPD-28) also flagged the potential breadth of targeted collection as part of their report addressing technical options that would allow the IC to more easily conduct targeted rather than bulk collection.[117] The committee proposed an alternative definition ("if a significant portion of the data collected is not associated with current [surveillance] targets, it is bulk collection; otherwise, it is targeted"), but noted that bulk collection is a continuum, with "no bright line separating bulk from targeted."[118] Both the CIA and NSA, in their PPD-28 procedures, note an aspiration to conduct targeted collection rather than bulk collection "when practicable."[119] Between the breadth of the allowable enumerated uses for bulk collection and the potential scope of targeted collection, however, the entire section of PPD-28 that provides restrictions on the use of information collected in bulk seems to do very little work in practice.

The civil liberties community has also voiced some privacy-related concerns[120] about PPD-28's footnote 5, which provides: "The limitations contained in this section do not apply to signals intelligence data that is temporarily acquired to facilitate targeted collection. . . ."[121] This footnote does not clearly state what would be considered

---

[114] CENT. INTELLIGENCE AGENCY [CIA], POLICY AND PROCEDURES FOR CIA SIGNALS INTELLIGENCE ACTIVITIES (n.d.) 3, https://www.cia.gov/library/reports/Policy-and-Procedures-for-CIA-Signals-Intelligence-Activities.pdf [https://perma.cc/HJH4-YMFM] [hereinafter CIA PPD-28 PROCEDURES] (last visited Sept. 26, 2020).

[115] CIA PPD-28 PROCEDURES, *supra* note 114, at 1; NSA PPD-28 PROCEDURES, *supra* note 81, at 7 n.1.

[116] Margo Schlanger, *US Intelligence Reforms Still Allow Plenty of Suspicionless Spying on Americans*, JUST SECURITY (Feb. 13, 2015), https://www.justsecurity.org/20033/guest-post-intelligence-reforms-plenty-suspicionless-surveillance-americans [https://perma.cc/X56Q-H8M3].

[117] COMM. ON RESPONDING TO SECTION 5(D) OF PRESIDENTIAL POLICY DIRECTIVE 28, BULK COLLECTION OF SIGNALS INTELLIGENCE: TECHNICAL OPTIONS 2 (2015), https://www.nap.edu/read/19414/chapter/1 [https://perma.cc/4B9J-4A79].

[118] *Id.*

[119] CIA PPD-28 PROCEDURES, *supra* note 114, at 2; NSA PPD-28 PROCEDURES, *supra* note 82, at 6.

[120] Goitein, *supra* note 72.

[121] PPD-28, *supra* note 3, at n.5.

"temporary" acquisition and, thus, does not clarify how protective the restrictions are. The NSA has interpreted the footnote to exempt "the processing of a signal that is necessary to select specific communications for forwarding for intelligence analysis,"[122] as well as signals collection only for the purpose of identifying those signals that: "(1) May contain information related to the production of foreign intelligence or counterintelligence; (2) Are enciphered to appear to contain secret meaning; (3) Are necessary to assure efficient signals intelligence collection or to avoid the collection of unwanted signals; or (4) Reveal vulnerabilities of United States communications security."[123] In other words, automatically processing bulk data to enable targeted collection does not count as "bulk collection" itself. This aligns with the view of the advocate general in *Schrems II* and the EU Commission that "temporary access by the intelligence authorities to all the content of the electronic communications for the sole purpose of filtering . . . cannot be treated as equivalent to generalised access to that content."[124] What remains unclear is whether "temporary" for purposes of this filtering refers more to fractions of a second or years.

If the restrictions on bulk collection do not apply to temporary bulk collection and provide little practical restriction on bulk analysis—and if targeted collection can acquire almost as much data—PPD-28's restrictions provide minimal privacy protections to foreign communications. Revising this section of PPD-28 to provide more specificity might also help technical experts get closer to building less intrusive ways of collecting only communications responsive to authorized intelligence requirements, which has not been possible thus far.[125]

---

[122] NSA PPD-28 PROCEDURES, *supra* note 82, at 7 n.2.

[123] NAT'L SEC. AGENCY, USSID 18: LEGAL COMPLIANCE AND U.S. PERSONS MINIMIZATION PROCEDURES app. E ¶ E1.2.a (Jan. 15, 2011), https://www.dni.gov/files/documents/1118/CLEANEDFinal%20USSID%20SP0018.pdf [https://perma.cc/3L96-C55H].

[124] Swire, *supra* note 66.

[125] Robert Litt, Gen. Counsel, Office of the Dir. of Nat'l Intelligence, Prepared Remarks on Signals Intelligence Reform at the Brookings Institute (Feb. 4, 2015), https://www.dni.gov/index.php/newsroom/speeches-interviews/speeches-interviews-2015/item/1171-odni-general-counsel-robert-litt-s-as-prepared-remarks-on-signals-intelligence-reform-at-the-brookings-institute (noting that experts from the National Academy of Sciences concluded that no software-based solutions were currently available to eliminate the need for bulk collection).

B. Gaps in PPD-28's Dissemination and Retention Procedures

Although PPD-28 lays out restrictions for the dissemination (i.e., sharing between agencies) and retention (i.e., storage by each agency) of non-U.S. person communications, they appear to have caused minimal actual change, which may jeopardize intercontinental data-sharing agreements. This minimal change comes from fairly loose mandated restrictions and even looser implementing procedures by the agencies; the FBI, for instance, seems to have ignored or forgotten some of these requirements of PPD-28 entirely. Controlling dissemination and retention of information, rather than allowing agencies to share information widely and store it indefinitely, reduces the chances of someone using private information for an improper purpose. In addition, insufficient dissemination and retention rules could lead to "information overload," causing intelligence agencies to miss key intelligence because it is buried within databases containing far too much data. By allowing agencies to deviate from the strict requirements of this section of PPD-28, the White House allows the document as a whole to lose efficacy and, therefore, credibility.

1. PPD-28's dissemination and retention requirements

PPD-28 clearly lays out its dissemination and retention requirements, made easier by the fact that the requirements are not extensive. PPD-28 notes: "long-term storage of personal information unnecessary to protect our national security is inefficient, unnecessary, and raises legitimate privacy concerns. Accordingly, IC elements shall establish policies and procedures reasonably designed to minimize the dissemination and retention of personal information collected from signals intelligence activities."[126]

The document goes on to specify that, as regards dissemination, "[p]ersonal information shall be disseminated only if the dissemination of comparable information concerning U.S. persons would be permitted under section 2.3 of Executive Order 12333."[127] Section 2.3 is the same extremely broad section of EO 12333 discussed in the definition of "personal information"[128] and it results in the same effect: almost any piece of information that would be considered useful to an intelligence agency will fall within a permitted category in section 2.3 and can be disseminated from one agency to another, meaning more personal

[126] PPD-28, *supra* note 3, at § 4.a.1.
[127] *Id.*
[128] *See supra* Section II.A.

information accessible by more government officials and greater potential for improper use.

Similarly, for retention, PPD-28 requires that "[p]ersonal information shall be retained only if the retention of comparable information concerning U.S. persons would be permitted under section 2.3 of Executive Order 12333 and shall be subject to the same retention periods as applied to comparable information concerning U.S. persons."[129] Again, this provides minimal practical restriction because it allows the retention of vast quantities of personal information. The section goes on to say: "Information for which no such determination has been made shall not be retained for more than 5 years, unless the DNI expressly determines that continued retention is in the national security interests of the United States."[130] This provision is potentially privacy-protective, although it has not been implemented exactly as stated.[131] Finally, PPD-28 called on the DNI, the Attorney General, and the heads of the other elements of the IC to prepare a report "evaluating possible additional dissemination and retention safeguards for personal information collected through signals intelligence, consistent with technical capabilities and operational needs."[132] Despite the promise of this mandate, no reporting has suggested any further safeguards resulting from this process.[133]

2. The incomplete implementation of dissemination and retention limits

PPD-28 mandates that intelligence agencies apply the same dissemination and retention limits to the information of both U.S. and non-U.S. persons "to the maximum extent feasible consistent with the national security."[134] While caveats allowing for departure in the name of "national security" are somewhat unavoidable in the realm of security policy, monitoring whether they end up swallowing the rules to which they are appended helps oversight personnel determine whether agencies are conforming to the spirit of the original rule.

The CIA and FBI determined that PPD-28 required no changes to their existing practices, while the NSA determined that PPD-28

[129] PPD-28, *supra* note 3, at § 4.a.1.
[130] *Id.*
[131] *See supra* Section II.B.2-3.
[132] PPD-28, *supra* note 3, at § 4.a.1.
[133] Wittes, *supra* note 23.
[134] PPD-28, *supra* note 3, at § 4.a.

required no "substantial" changes.[135] The CIA and NSA's PPD-28 implementing procedures both require that, in order to qualify for dissemination, personal information concerning a foreign person must relate to an authorized intelligence requirement.[136] Alternatively, the NSA provides that the information must relate to a crime that has been, is being, or is about to be committed, or must indicate a possible threat to the safety of any person or organization.[137] It is unclear what accounts for the difference between the CIA's and NSA's dissemination procedures. The PCLOB report points out that both the CIA and NSA's standards for non-U.S. persons' information are less strict than these agencies' standards for the dissemination of U.S. persons' information (requiring "necessity"), in violation of Section 4 of PPD-28.[138] However, redactions in the PCLOB report make it unclear whether either or both agencies defended the difference under the "to the maximum extent feasible consistent with the national security" caveat.[139]

The PCLOB report does not examine whether the FBI provides equal protections for U.S. and non-U.S. persons' information, potentially (although not explicitly) because the FBI does not conduct "signals intelligence activities."[140] However, the FBI's PPD-28 procedures say that the FBI will disseminate non-U.S. person personal collected pursuant to Section 702 of FISA only if "dissemination of comparable information concerning U.S. persons would be permitted under Section 2.3 of Executive Order 12333"; "the information relates specifically to an activity authorized by the Attorney General or an intelligence requirement authorized by the Director of National intelligence"; and "the information is relevant to the underlying purpose of the dissemination."[141] If implemented as written, these qualifications reflect the mandated restrictions of PPD-28.

---

[135] STATUS OF THE IMPLEMENTATION OF PPD-28, *supra* note 21, at 10-11.

[136] CIA PPD-28 PROCEDURES, *supra* note 114, at 5; NSA PPD-28 PROCEDURES, *supra* note 82, at 9.

[137] NSA PPD-28 PROCEDURES, *supra* note 82, at 9.

[138] STATUS OF THE IMPLEMENTATION OF PPD-28, *supra* note 21, at 10-11.

[139] *Id.*

[140] *See supra* Section II.A.1.

[141] FED. BUREAU OF INVESTIGATION, FBI POLICIES AND PROCEDURES FOR SAFEGUARDING PERSONAL INFORMATION AS REQUIRED BY PPD-28 (SIGNALS INTELLIGENCE ACTIVITIES) 2 (JULY 5, 2016), https://www.fbi.gov/file-repository/ppd-28-policies-procedures-signed.pdf/view [https://perma.cc/5SJB-TS7N] [hereinafter FBI PPD-28 PROCEDURES].

3. Exceptions to PPD-28's five-year retention limit

PPD-28 requires that information that has not been determined to fall within section 2.3 of EO 12333 shall not be retained for longer than five years unless the DNI "expressly determines that continued retention is in the national security interests of the United States."[142] The PCLOB report states that the five-year retention period is not a change in practice for the NSA or FBI;[143] the report does not mention whether this holds true for the CIA, but the CIA's PPD-28 procedures mirror the language of PPD-28 fairly directly.[144]

The PCLOB report also does not mention that the NSA and FBI apply exceptions to the five-year retention period that are not expressly authorized by PPD-28. The NSA notes in its PPD-28 procedures that "[i]nformation that has not been processed into an intelligible form because of unknown communication methods, encryption, or other methods of concealing secret meaning is not subject to the foregoing retention limit; however, the up-to-5-year retention period for such information will begin when the information has been made intelligible."[145] The NSA possibly applied this exception because it would not consider such information to be "collected" yet under its definition.[146]

Meanwhile, the FBI's exceptions deviate even further from PPD-28's mandated restrictions, although the FBI does not reveal this in its PPD-28 implementing procedures. The FBI's PPD-28 procedures make no mention of any exceptions to the five-year retention period[147] and, in turn, the PCLOB report does not either.[148] Like the NSA, the FBI applies an exception for encrypted communications, although the FBI mentions this only in its separate "minimization procedures" for FISA Section 702.[149] These Section 702 minimization procedures also note

[142] PPD-28, *supra* note 3, at § 4.a.1.

[143] STATUS OF THE IMPLEMENTATION OF PPD-28, *supra* note 21, at 9.

[144] CIA PPD-28 PROCEDURES, *supra* note 114, at 4.

[145] NSA PPD-28 PROCEDURES, *supra* note 82, at 8.

[146] *See supra* Section II.A.2.

[147] FBI PPD-28 PROCEDURES, *supra* note 141, at 3.

[148] STATUS OF THE IMPLEMENTATION OF PPD-28, *supra* note 21, at 9.

[149] FED. BUREAU OF INVESTIGATION, MINIMIZATION PROCEDURES USED BY THE FEDERAL BUREAU OF INVESTIGATION IN CONNECTION WITH ACQUISITIONS OF FOREIGN INTELLIGENCE INFORMATION PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978, AS AMENDED 42 (Mar. 27, 2018), https://www.intelligence.gov/assets/documents/702%20Documents/declassified/2018_Cert_FBI_Minimization_27Mar18.pdf [https://perma.cc/FKJ6-2UYS] [hereinafter FBI 702 MINIMIZATION PROCEDURES]. These procedures address the handling of U.S. person information in collected communications.

that information that has not been reviewed shall be destroyed after five years "unless an executive at FBI Headquarters in a position no lower than an Assistant Director (AD) determines that an extension is necessary because the information is reasonably believed to contain significant foreign intelligence information, or evidence of a crime that has been, is being, or is about to be committed."[150] This clearly defies the rule stated in PPD-28, but the FBI 702 procedures contain a note explaining that such authorizations should be reported to the Office of the Director of National Intelligence (ODNI).[151] This reporting provision makes the exception seem less like intentional deception and more like the FBI forgetting that PPD-28 speaks with the force of law, including on this topic. The FBI's 702 procedures further provide that FISA-acquired information that has been "retained and reviewed," but does not reasonably appear "to be foreign intelligence information, to be necessary to understand foreign intelligence information or assess its importance, or to be evidence of a crime," may be retained and fully accessible to authorized personnel for further review and analysis for "10 years from the expiration date of the certification authorizing the collection."[152] This guidance, too, goes against PPD-28's explicit mandate. This incongruity is worrisome not just because it appears the FBI is violating PPD-28, but also because it went unreported in the FBI's public PPD-28 procedures and unnoticed by the PCLOB.

The FBI's deviation from PPD-28 might be part of a larger issue with the lack of interest in the contents of PPD-28, even within government. Interestingly, the Intelligence Authorization Act of 2015, passed by Congress and signed into law by President Obama just eleven months after the publication of PPD-28, mandates its own five-year retention period, with its own exceptions. Among them are an exception for encrypted communications and an exception where "all parties to the communication are reasonably believed to be non-United States persons."[153] It seems unlikely that the President would sign a presidential policy directive calling for the same retention period to apply for U.S. and non-U.S. person information and then, less than a year later, purposefully sign into law a bill that calls for the elimination of any retention period limit for communications between non-U.S. persons. It seems more likely that whoever in Congress drafted the bill

[150] *Id.* at 19.
[151] *Id.*
[152] *Id.* at 20.
[153] Intelligence Authorization Act for Fiscal Year 2015, Pub. L. No. 113-293, § 309, 128 Stat. 3990, 3998 (2014) (codified at 50 U.S.C. § 1813 (2018)).

and whoever in the White House reviewed the bill forgot about the substance of PPD-28. A discussion of the legal implications of the passage of the Intelligence Authorization Act of 2015 later in time than PPD-28 lies beyond the scope of this Note, but the signing into law of this provision that contradicts PPD-28 provides another interesting example of PPD-28's failure to leave a lasting impression.

C. Issues with Implementing PPD-28 Compliant Querying Procedures

Much of the intelligence agencies' confusion around how PPD-28 should affect querying procedures—i.e., rules for searching previously collected data—seems to flow from the definitional issues.[154] PPD-28 states as one of its governing principles that "signals intelligence shall be collected exclusively where there is a foreign intelligence or counterintelligence purpose to support national and departmental missions and not for any other purposes."[155] PPD-28 Section 2 narrows the acceptable uses even more for any signals intelligence collected in bulk.[156] The FBI's PPD-28 procedures, however, say that personnel will structure queries of FISA Section 702 information in order to return information simply "relevant to a valid intelligence requirement or an authorized law enforcement activity," which encompasses more information than PPD-28's mandated restrictions.[157]

The disparity between the FBI's procedures and what PPD-28 requires might be explained by the FBI's position that it does not conduct signals intelligence activities.[158] The PCLOB report notes that "FBI interprets footnote 6 of PPD-28 to mean that PPD-28 applies to FBI in some way, so it is applying PPD-28 to communications collected under Section 702 of the Foreign Intelligence Surveillance Act ("FISA"), a non-signals intelligence activity."[159] Footnote 6 of PPD-28 refers to Section 3, concerning the annual review of priorities and requirements for signals intelligence collection, and says that Section 3 does not apply to "signals intelligence activities undertaken by or for the Federal Bureau of Investigation in support of predicated

[154] *See supra* Section II.A. A "query" is "the use of one or more terms to retrieve the unminimized contents or noncontents located in electronic and data storage systems . . .". 50 U.S.C. § 1881(a)(f)(3) (2018).
[155] PPD-28, *supra* note 3, at § 1(b).
[156] *See supra* Section II.A.2.
[157] FBI PPD-28 PROCEDURES, *supra* note 141, at 3.
[158] STATUS OF THE IMPLEMENTATION OF PPD-28, *supra* note 21, at 4.
[159] *Id.*

investigations other than those conducted solely for purposes of acquiring foreign intelligence . . ."[160] This clearly implies that the FBI *does* conduct signals intelligence activities. Nevertheless, we are left with confusion about what PPD-28 applies to. If the FBI does not conduct signals intelligence activities, and thus does not need to follow PPD-28's guiding principles or use restrictions for signals intelligence collected in bulk, why has it chosen to apply PPD-28 to FISA Section 702 information at all? Footnote 6, by specifying that Section 3 of PPD-28 does *not* apply to certain FBI activities, seems to imply that the other sections of PPD-28 *do* apply to the FBI, so the FBI's confusion is understandable. This is the confusion that led ODNI to clarify the application of PPD-28 to Section 702 after the PCLOB report.[161]

Compare this to the CIA's procedures, which require personnel querying SIGINT databases to structure queries "in a manner reasonably designed to identify intelligence relevant to an authorized intelligence requirement and minimize the review of personal information not relevant to an authorized intelligence requirement."[162] This phrasing aligns more with PPD-28 (notwithstanding the question of what "signals intelligence" means[163]) because the use of the phrase "authorized intelligence requirement" seems to acknowledge compliance with the PPD-28 process more than the FBI's use of "valid intelligence requirement," which leaves open the question of who exactly is determining what intelligence requirements are "valid."

D. The Implementation of PPD-28's Broad Principles is Difficult to Concretely Assess

The implementation of PPD-28 Section 1, which contains broad principles intended to govern signals intelligence collection, is hard to assess and would benefit from more concretely defined and easily monitored milestones.[164] Section 1 starts by calling for agencies to conduct signals intelligence in a lawful manner and a manner considerate of privacy and civil liberties.[165] Next, it notes that agencies cannot collect signals intelligence "for the purpose of suppressing or burdening criticism or dissent, or for disadvantaging persons based on

[160] PPD-28, *supra* note 3, at § 3 n.6.
[161] STATUS OF THE IMPLEMENTATION OF PPD-28, *supra* note 21, at 5.
[162] CIA PPD-28 PROCEDURES, *supra* note 114, at 5.
[163] *See supra* Section II.A.1.
[164] PPD-28, *supra* note 3, at § 1(b).
[165] *Id.*

their ethnicity, race, gender, sexual orientation, or religion."[166] Section 1 also forbids the conduct of economic espionage for the purpose of affording a competitive advantage to U.S. companies, and generally calls for agencies to tailor signals intelligence activities "as feasible" and to prioritize alternatives as appropriate.[167] These principles appear commendable, but difficult to oversee without concrete implementation goals.

1. Disadvantaging persons based on certain characteristics

The requirement that signals intelligence not be collected for "the purpose of suppressing or burdening criticism or dissent, or for disadvantaging persons" based on "ethnicity, race, gender, sexual orientation, or religion" could be quite protective if implemented as written.[168] Intelligence agencies can and historically have used information about sexual proclivities to coerce targets to take actions for a foreign government.[169] This practice has only gotten easier with the proliferation of digital personal data. Two Harvard undergraduates, by aggregating leaked datasets, were able to produce a list of "more than 1,000 people who have high net worth, are married, have children, and also have a username or password on a cheating website" in less than 10 seconds.[170] It is unclear whether taking advantage of this kind of tactic would be considered intelligence collection to disadvantage someone "based on" sexual orientation under PPD-28, or whether coercion based on knowledge of an affair would only be barred if the information revealed a previously undisclosed sexual orientation.

U.S. intelligence agencies may already tend not to conduct this kind of coercion or blackmail as a matter of poor source development

---

166 *Id.*

167 *Id.*

168 *Id.*

169 Stuart A. Thompson & Charlie Warzel, Opinion, *How to Track President Trump*, N.Y. TIMES (Dec. 20, 2019), https://nyti.ms/2Z8ANaN. *See also* Olivia B. Waxman, *Document Claims Russia Has Donald Trump 'Kompromat.' What Is That?*, TIME (Jan. 12, 2017, 4:20 PM), https://time.com/4632111/kompromat-history-donald-trump/ (detailing examples of Russian use of compromising sexual material for blackmail); John F. Burns, *Britain Warned Businesses of Threat of Chinese Spying*, N.Y. Times (Jan 31, 2020), https://www.nytimes.com/2010/02/01/world/europe/01spy.html (citing evidence that Chinese intelligence agencies were using compromising sexual material for blackmail).

170 Adam Zewe, *Imperiled Information: Students Find Website Data Leaks Pose Greater Risks Than Most People Realize*, HARV. JOHN A. PAULSON SCH. OF ENG'G & APPLIED SCI.: NEWS & EVENTS (Jan. 17, 2020), https://www.seas.harvard.edu/news/2020/01/imperiled-information.

(it is generally more effective to gain a source's cooperation through positive rapport-building),[171] but the practices of foreign intelligence partners may be different. The U.S. shares some amount of signals intelligence information with the other members of the "Five Eyes" intelligence alliance (the UK, Canada, Australia, New Zealand), and with other countries like Germany and Israel.[172] Leaked documents have shown that the NSA has shared some raw signals intelligence (i.e. not reviewed or minimized by U.S. analysts) with Israel's signals intelligence agency, and former Israeli intelligence employees have "accused Israel of gathering information about Palestinians' sexual orientation and other private matters."[173]

Effective oversight of these provisions would include an ex ante requirement for intelligence-sharing partners to abide by the principles of PPD-28 to receive intelligence and regular ex post assessments by U.S. intelligence agencies and oversight entities to see if their intelligence-sharing partners have violated the principles of PPD-28. The CIA's PPD-28 procedures require that SIGINT information be disseminated to foreign governments only if "the dissemination complies with applicable laws,"[174] and the FBI's FISA Section 702 Minimization Procedures require that the FBI undertake "reasonable steps to ensure that the disseminated information will be used in a manner consistent with United States laws."[175] However, absent any information about how agencies are reviewing these requirements, it is impossible to know to what extent any review is actually happening.

2. Signals intelligence activities must be "as tailored as feasible"

Among the principles hardest to assess in PPD-28 Section 1 is the idea that: "Signals intelligence activities shall be as tailored as feasible. In determining whether to collect signals intelligence, the United States shall consider the availability of other information, including from diplomatic and public sources. Such appropriate and

---

[171] John Sipher, *Murdering Reality: The Spurious Spies of Fiction*, STANDPOINT (Feb. 26, 2020), https://standpointmag.co.uk/issues/march-2020/murdering-reality-the-spurious-spies-of-fiction/ ("Blackmail. A staple tension-builder in spy films—but it is drilled into us from day one that we just don't do it. Like torture: not only is it wrong, it doesn't work. Anyone strong-armed into cooperating looks for a means to get out of it. We would not be successful if those people working for us despised us and were looking for revenge.").

[172] TOH ET AL., *supra* note 71, at 7-8.

[173] *Id.* at 29-30.

[174] CIA PPD-28 PROCEDURES, *supra* note 113, at 6.

[175] FBI 702 MINIMIZATION PROCEDURES, *supra* note 148, at 44-45.

feasible alternatives to signals intelligence should be prioritized."[176] This requirement to consider alternatives and tailor collection "as feasible" is too amorphous to review without some concrete procedures mandated. U.S. intelligence agencies have echoed this language in their PPD-28 procedures,[177] but do not elaborate on what this decision-making process might look like.

If bulk collection is still occurring, and the committee of technical experts convened by the National Research Council to evaluate privacy-protecting alternatives found that "there is no software technique that will fully substitute for bulk collection where it is relied on to answer queries about the part after new targets become known,"[178] it may be difficult to determine whether SIGINT activities are "as tailored as feasible." One possible procedure might include a checklist of alternatives that analysts need to go through before they can determine that signals intelligence needs to be conducted rather than alternatives.

Even if the government wanted to keep this sort of process classified, U.S. intelligence agencies could confirm in a public document like their PPD-28 procedures the fact that there *is* some sort of real process underlying this requirement. This might also help assuage the advocate general and the Court of Justice of the European Union, who both found in their *Schrems II* opinions that "as tailored as feasible" does not meet the "strict necessity" test of EU law, which requires intelligence agencies to collect only what is "strictly necessary" for the country's national security.[179]

3. Training and auditing as an incomplete answer to PPD-28 Section 1

Thus far, the only procedures that we know intelligence agencies have implemented that might operationalize PPD-28 Section 1 are general training and auditing procedures. Training and auditing generally help compliance and oversight, but cannot by themselves address all of the problems identified above without more concrete goals to make sure the Section 1 principles are adhered to at various stages. The FBI, CIA, and NSA all mention that only personnel that

[176] PPD-28, *supra* note 3, at § 1(d).

[177] *See* CIA PPD-28 PROCEDURES, *supra* note 113, at 1; *see also* NSA PPD-28 PROCEDURES, *supra* note 81, at 6.

[178] COMMITTEE ON RESPONDING TO SECTION 5(D) OF PRESIDENTIAL POLICY DIRECTIVE 28, *supra* note 116, at 9.

[179] Propp, *supra* note 49; Case C-311/18, Data Protection Commissioner v. Facebook Ireland Ltd., Maximilian Schrems (*Schrems II*), ECLI:EU:C:2020:559 (E.C.J. 2020), at ¶ 184.

have received adequate training can access SIGINT or FISA Section 702 information.[180] The CIA procedures task all agency personnel with reporting compliance issues to the head of their section and the agency's Privacy and Civil Liberties Office.[181] The NSA procedures go even further by requiring all personnel to "immediately inform the SIGINT Director" of any instructions "that appear to require actions at variance with" the procedures and to report to the NSA Inspector General and consult with the NSA General Counsel on "all activities that may raise a question of compliance."[182] The agencies have also mandated periodic auditing and mention that systems will record queries to facilitate oversight.[183] These steps will improve compliance and oversight, but if President Obama determined that this section should be included in PPD-28, more concrete compliance targets—i.e., how exactly the agencies will implement and confirm compliance with these principles—would better achieve the President's desired end-state of respecting the principles laid out in Section 1.

E. Approval of Departures from PPD-28

One final minor discrepancy between President Obama's intent when he published PPD-28 and its ultimate implementation is the slight difference between the CIA and the NSA procedures for departing from the requirements of PPD-28. The CIA procedures note that the CIA Director has to approve any exception to PPD-28 and "if practicable consult in advance" the ODNI and the National Security Division (NSD) of the Department of Justice (DOJ).[184] However, the NSA's procedures outline that the NSA Director or a designee must approve departures from PPD-28 necessary "to protect the national security of the United States" only "following consultation with the Office of the Director of National Intelligence, the National Security Division of the Department of Justice, and the Office of the Secretary of Defense."[185]

---

[180] *See* FBI PPD-28 PROCEDURES, *supra* note 140, at 5; *see also* CIA PPD-28 PROCEDURES, *supra* note 113, at 5; *see also* NSA PPD-28 PROCEDURES, *supra* note 81, at 8–9.

[181] CIA PPD-28 PROCEDURES, *supra* note 113, at 8.

[182] NSA PPD-28 PROCEDURES, *supra* note 81, at 12.

[183] FBI PPD-28 PROCEDURES, *supra* note 140, at 4; CIA PPD-28 PROCEDURES, *supra* note 113, at 6; *see also id.* at 3.

[184] *Id.* at 6-7.

[185] NSA PPD-28 PROCEDURES, *supra* note 81, at 3-4.

This difference between the NSA *requiring* consultation with the ODNI and DOJ and the CIA only *consulting "if practicable*," while minor, could be easily remedied in any update to PPD-28 by dictating a uniform practice for agencies in circumstances requiring departure.

III. PROPOSALS TO REVISE PPD-28

In order to continue shaping global norms for privacy protections in foreign surveillance, the United States should regularly update PPD-28 as potential issues arise especially in light of the constant evolution of communication technology. Any president could revise and update PPD-28, a presidential policy directive, at any time. Even moderate revisions could signal to the public, domestically and internationally, that the U.S. government takes privacy concerns seriously, which would, in turn, foster trust that would support global data sharing agreements. Optimally, these revisions would include a definitional section, a decision from the White House delineating retention limitations for encrypted communications, a demand for reciprocity from allies, a larger global public affairs campaign, improvement of oversight, maintenance of improved transparency practice, and potentially codification of PPD-28 by Congress. Each of these proposed revisions seeks to further Secretary Kerry's "universal" principles for surveillance: (1) rule of law; (2) legitimate purpose; (3) oversight; and (4) transparency.[186]

A. Definitional Section

The first and least controversial revision to PPD-28 should be the inclusion of a definitional section. This would help minimize the "great deal of confusion among the agencies" about whether, when, and how to apply each of the provisions of PPD-28 and increase transparency as to the intended application of the document.[187] At a minimum, this would include definitions of "signals intelligence activities," "collection," "acquisition," "temporary acquisition," "bulk collection," and "targeted collection." A definitional section would mollify those who worry that our intelligence agencies over-apply PPD-28,[188] those who worry the agencies do not

[186] KLEIN ET AL., *supra* note 8, at 26.
[187] PCLOB PPD-28 REPORT, *supra* note 83, at 20 (Separate Statement of Board Members Rachel Brand and Elisabeth Collins).
[188] *Id.*

apply it widely enough, and the agencies themselves, which just want to make sure they implement the law with fidelity.

The PCLOB recommends that the National Security Council and the ODNI together issue guidelines for the application of PPD-28's requirements.[189] Others have also proposed these two organizations or Congress should create a "glossary" to define all common terms across the Intelligence Community, outside of the PPD-28 context.[190]

In the interest of modest, easily-administrable proposals, ODNI, which regularly manages interaction between all of the agencies in the IC, could most naturally coordinate a definitional section for PPD-28, with the involvement of representatives from across the IC, for approval by the White House and inclusion in a revision to PPD-28. If this triggers interest in a larger statute or directive defining all common terms across the IC, that would be an added benefit, but resistance to consensus on that idea should not hold back this fix to PPD-28.

B. Retention Limitations for Encrypted Communications

A revised PPD-28 should explicitly state whether or not the five-year retention limit applies to encrypted communications. While encryption once served as a potential indicator of foreign intelligence information, it is now widely used in popular electronic communication platforms.[191] A complete discussion of the growth of encryption lies beyond the scope of this Note, but it is worth recognizing that among encryption users are those whose communications should be most protected, including journalists and human rights advocates;[192] those whose communications pose the greatest potential threat to international security, including terrorists;[193] and many people in between.

Because of the privacy and security interests at stake, the White House needs to be accountable for the decision of whether or not to apply the retention exception for encrypted communications that the agencies have implemented on their own. If the agencies have the means to store as much data as they would like, retaining encrypted data until it can be rendered intelligible and then starting the five-year clock would align with the spirit of PPD-28's original restriction of only allowing the intelligence agencies five years to retain intelligible

[189] *Id.* at 13.
[190] Lee & Perlin, *supra* note 104.
[191] TOH ET AL., *supra* note 71, at 23.
[192] *Id.*
[193] KLEIN ET AL.,, *supra* note 8, at 43.

communications. If the U.S. government is unable to crack an encrypted communication, the privacy risks of that data sitting on a government server are low; however, there may still be potential benefits from its decryption later.

C. Demanding Reciprocity from Other Countries and Pursuing the Development of International Norms

Given the tension between the U.S. and EU over surveillance and data privacy,[194] a revised PPD-28 could also include a provision declaring that PPD-28's protections will only apply to the citizens of countries that provide reciprocal rights for Americans. A former General Counsel of the NSA recommended this course of action,[195] and a former NSA Inspector General even proposed a lawsuit by Americans in Europe demanding protection for their data, along the lines of the *Schrems* cases.[196] This would surely anger the EU, but it would force the EU and its member states to confront their hypocrisy on this issue. The advocate general and the CJEU in their *Schrems II* opinions expressed dissatisfaction with "the mechanism created in the Privacy Shield for U.S. government review of complaints lodged by Europeans" via the State Department ombudsperson, but U.S. persons have the protection of no similar mechanism under the laws of EU member states.[197]

The Center for New American Security has suggested that any such demands for reciprocity should be conducted as "high-level, public, political" commitments with other countries rather than formal treaties.[198] While political commitments might not be codified as clearly as legal commitments, this approach would probably be easier to accomplish than an international agreement like a treaty, which would require negotiation between the U.S. and another country as well as between the Senate and the Executive branch. Public political commitments would also help establish international norms about reciprocity of privacy protections.

Reciprocity from our allies would also fix the problems about ensuring that countries with whom we share our SIGINT information

---

[194] *See supra* Section I.D.2.

[195] THE CYBERLAW PODCAST, *supra* note 55.

[196] Edgar, *supra* note 46.

[197] Propp, *supra* note 49, at 3. The successful case brought before the German Federal Constitutional Court by non-German citizens represents the first possible example to the contrary. *See* BVerfG, *supra* note 33.

[198] KLEIN ET AL.,, *supra* note 8, at 8.

do not use it to facilitate practices with which we do not agree.[199] A revised PPD-28 could mention that failure to provide reciprocal commitments may jeopardize intelligence-sharing agreements with other countries.

One aspect of PPD-28 for which it mandated reciprocity would likely engender push-back is the provision against economic espionage for the benefit of domestic companies.[200] It is not only U.S. rivals (like China) that are particularly active in economic espionage, but also U.S. allies like France.[201] While China has promised to cease economic espionage in the past and has subsequently broken that promise,[202] U.S. allies that benefit from intelligence-sharing arrangements with the U.S. would likely be more faithful to such a public commitment.

Establishing an international norm of privacy protections for the citizens of allies that are willing to reciprocate and a norm against economic espionage are long-term goals that would promote privacy as a fundamental right and reduce government intrusion into certain private spheres.[203] Getting other countries on board with these goals might require strong-arm tactics like threatening to limit intelligence-sharing unless and until countries comply. Despite the admitted harshness of such a measure, proponents of this kind of hardball with individual states predict it would be more effective than dealing with, for example, the European Commission, which has not been able to regulate the signals intelligence activities of its own member states.[204] This has not been attempted before, likely because refusing to share intelligence has a "cold-hearted air," but it could be a strong lever to induce support for these new norms.[205]

---

[199] *See supra* Section II.D.1.

[200] PPD-28, *supra* note 3, at § 1.

[201] KLEIN ET AL.,, *supra* note 8, at 56.

[202] Jack Goldsmith & Robert D. Williams, *The Failure of the United States' Chinese-Hacking Indictment Strategy*, LAWFARE (Dec. 28, 2019, 9:00 AM), https://www.lawfareblog.com/failure-united-states-chinese-hacking-indictment-strategy.

[203] *See generally* Samuel J. Rascoff, *The Norm Against Economic Espionage For The Benefit of Private Firms: Some Theoretical Reflections*, 83 U. CHI. L. REV. 249 (2016).

[204] Stewart Baker, Opinion, *Time to Get Serious About Europe's Sabotage of US Terror Intelligence Programs*, WASH. POST: THE VOLOKH CONSPIRACY (Jan. 5, 2016, 10:21 AM), https://www.washingtonpost.com/news/volokh-conspiracy/wp/2016/01/05/time-to-get-serious-about-europes-sabotage-of-us-terror-intelligence-programs/.

[205] *Id.*

D. Undertaking a Global Public Affairs Campaign

Regardless of any revisions to PPD-28, the policy substance of the document would greatly benefit from a much broader public affairs push than it originally received. Negative European opinions about American surveillance oversight likely result from the fact that "most people simply are not aware of [PPD-28]."[206] Specifically, according to one expert in Germany, whose citizenry had some of the most negative backlash to the Snowden revelations,[207] "most Germans are 'totally unaware' of PPD-28."[208]

It is doubtful that German citizens are the only ones unaware of PPD-28. In fact, most Americans likely know nothing about PPD-28's existence, let alone its content, and even those involved in intelligence oversight sometimes forget what PPD-28's commitments entail. A significant public awareness campaign surrounding PPD-28's privacy protections would help cultivate good will for the United States, which would, in turn, help maintain data-sharing agreements like future iterations of the Privacy Shield and galvanize public support among the citizens and leadership of other countries to extend reciprocal protections for Americans.[209]

E. Increasing Oversight of PPD-28's Provisions

All three branches of the federal government can and should have a heightened role in oversight of PPD-28's provisions. Increased oversight will help prevent against overreach by government agencies, promote consistency, and improve public trust.

1. The Executive Branch

Executive branch entities like the PCLOB can serve as convenient mechanisms for oversight, given the fact that they fall within the same branch of government as the agencies they oversee. While PCLOB's PPD-28 Report fell short in extensively looking at documents beyond the intelligence agencies' self-reported implementation procedures, the PCLOB has proven itself capable of publishing commendably

---

[206] KLEIN ET AL., *supra* note 8, at 30.
[207] *See supra* Section I.D.1.
[208] KLEIN ET AL., *supra* note 8, at 53.
[209] This might also help curtail instances where government agencies appear to have forgotten the contents of PPD-28. *See* Section II.B.3.

thorough, detailed, and revealing reports regarding other programs.[210] One relatively simple solution would be to increase the capacity and power of PCLOB. As one resigning member of the PCLOB observed, "a supervised and controlled PCLOB was not what the 9/11 Commission had in mind when it recommended in its final report an independent PCLOB in the executive branch, with subpoena power — such as the FTC or even such as inspectors general within executive departments."[211] Providing the PCLOB with more personnel, independence, and power would allow it to make every program review as thorough as its Section 702 and 215 reports, rather than forcing it to rely mostly on self-reporting from the agencies, as it must do with the PPD-28 implementing procedures. While the PCLOB falls within the executive branch, significant reform would require congressional action, as the PCLOB in its current form was established by the Implementing Recommendations of the 9/11 Commission Act.[212]

A reformed PCLOB might also be the right forum to create an independent tribunal that would satisfy the requirement for the type of redress mechanism called for in *Schrems II*.[213] Non-U.S. persons who believe U.S. surveillance practices have violated their rights and freedoms would be entitled to a hearing by this "independent and impartial" tribunal, which would eliminate a major concern of the CJEU, thereby affording U.S. SIGINT policies more legal and political legitimacy.[214]

---

[210] *See, e.g.*, PRIVACY & CIVIL LIBERTIES OVERSIGHT BD., REPORT ON THE SURVEILLANCE PROGRAM OPERATED PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT, (July 2, 2014), https://documents.pclob.gov/prod/Documents/OversightReport/823399ae-92ea-447a-ab60-0da28b555437/702-Report-2.pdf [https://perma.cc/5XP5-JPBX]; PRIVACY & 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 (2014), https://fas.org/irp/offdocs/pclob-215.pdf.

[211] Lanny Davis, *Why I Resigned from the President's Privacy and Civil Liberties Oversight Board — And Where We Go from Here*, HILL (May 18, 2007, 2:15 PM), https://thehill.com/blogs/pundits-blog/the-administration/34214-why-i-resigned-from-the-presidents-privacy-and-civil-liberties-oversight-board--and-where-we-go-from-here-.

[212] GARRETT HATCH, CONG. RESEARCH SERV., RL 34385, PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD: NEW INDEPENDENT AGENCY STATUS (2012), https://fas.org/sgp/crs/misc/RL34385.pdf.

[213] Case C-311/18, Data Protection Commissioner v. Facebook Ireland Ltd., Maximilian Schrems (*Schrems II*), ECLI:EU:C:2020:559 (E.C.J. 2020), at ¶196–97.

[214] *Id.* at ¶ 186. There are constitutional issues that might prevent any such tribunal from being truly "independent." *See generally* Seila Law v. Consumer Financial Protection Bureau, 591 U.S. ___ (2020) (2020).

One potential downside of relying on executive branch entities to conduct oversight of the executive branch is that a President can decide that oversight no longer serves the President's interests. In that case, a President can fire oversight personnel like inspectors general with little to no legal recourse.[215] One solution to a President dismantling executive branch oversight mechanisms would require members of Congress to react strongly enough to make such actions politically costly for the President.

2. Congress

Although Congress has the authority and the explicit mandate to conduct oversight of intelligence activities via the House and Senate intelligence committees, this oversight has not always been as complete as Congressional leaders hoped it would be and may no longer be totally possible. In 2013, Senator Dianne Feinstein, as chair of the Senate Select Committee on Intelligence "suggested that the Committee had not been 'satisfactorily informed' of intelligence surveillance activities, and that a 'total review of all intelligence programs' was necessary."[216] While this review began in 2014, the new committee leadership that took over in 2015 has not provided any updates.[217]

Some experts have argued that Congress, with a 22-member intelligence committee in the House and a 15-member committee in the Senate, no longer has the capacity to conduct effective oversight of the ever-growing IC, with "seventeen agencies . . . hundreds of thousands of employees, [and] with a declared budget of almost 70 billion dollars."[218] Further, Congressional oversight of overseas surveillance, like most of the surveillance discussed in this Note, will likely always receive some resistance from the executive branch, as the authority to conduct this surveillance is rooted in the President's Article II powers, including the President's designated role as Commander in Chief and the President's enumerated powers in the field of foreign affairs.[219]

As a result, the most effective way to improve Congressional oversight, apart from a radical expansion of Congressional bureaucracy,

---

[215] Benjamin Wittes, *Why is Trump's Inspector General Purge Not a National Scandal?*, LAWFARE (Apr. 8, 2020, 7:00 AM), https://www.lawfareblog.com/why-trumps-inspector-general-purge-not-national-scandal [https://perma.cc/3ECY-EENA].
[216] TOH ET AL., *supra* note 71, at 32.
[217] *Id.* at 32-33.
[218] *Id.* at 33.
[219] *Id.* at 45 n.66.

would be to expand the capacity of the PCLOB[220] and ensure mandatory reporting of findings to Congress.

3. Judiciary

The judiciary plays "no role in overseeing EO 12333 activities," but the Foreign Intelligence Surveillance Court ("FISC")—a group of U.S. District Court judges designated by the Chief Justice of the Supreme Court to also serve a role in overseeing FISA activities[221]—*is* involved in reviewing the procedures for FISA Section 702 collection.[222] Given the potential implications for Americans' privacy,[223] it would be worthwhile to explore a framework for high-level judicial review of overseas surveillance under EO 12333 similar to the FISC's annual review of Section 702 procedures. Just like it does for Section 702, the FISC could annually review the targeting, minimization, and querying procedures related to EO 12333.[224] Judge Richard Posner called civil liberties a "means of bringing the judiciary into the national security conversation, with a perspective that challenges that of the national security experts," which can, in turn, "stimulate thought, correct errors, force experts to explain themselves, expose malfeasance, and combat slack and complacency."[225] This has proven true in terms of FISC oversight of FISA—the FISC has consistently discovered government non-compliance with FISA's legal requirements.[226] Expanding this judicial involvement to EO 12333 activities would provide a similar oversight function over even broader surveillance programs.

One potential model for limited judicial involvement in oversight could be allowing an expanded PCLOB to flag any issues identified in its oversight for further review by the FISC. If the FISC is similarly troubled by the issue, it could demand briefing from the DOJ National Security Division in conjunction with lawyers from the relevant agency. This would conserve judicial resources while also providing a path to

[220] *See supra* Section III.E.1.

[221] DAVID KRIS & J. DOUGLAS WILSON, NATIONAL SECURITY INVESTIGATIONS & PROSECUTIONS 3D § 5.1 (2019).

[222] TOH ET AL., *supra* note 71, at 34.

[223] *See supra* Section I.D.3.

[224] 50 U.S.C. 1881a(j) (2018).

[225] POSNER, *supra* note 77, at 5.

[226] Elizabeth Goitein, *The FISA Court's 702 Opinions Part I: A History of Non-Compliance Repeats Itself*, JUST SECURITY (Oct. 15, 2019), https://www.justsecurity.org/66595/the-fisa-courts-702-opinions-part-i-a-history-of-non-compliance-repeats-itself/ [https://perma.cc/GXG6-8XNM].

judicial review if full-time oversight staff think judicial review is warranted.

F. Maintaining Transparency

One major achievement that has come with PPD-28 is the increase in government transparency about many of its surveillance programs. As Justice Hugo Black wrote in the "Pentagon Papers" case: "The guarding of military and diplomatic secrets at the expense of informed representative government provides no real security for our Republic."[227]

Since the issuance of PPD-28, the IC has "declassified thousands of pages of court filings, opinions, procedures, compliance reports, congressional notifications and other documents" and "released summary statistics about our use of surveillance authorities, and have authorized providers to release aggregate information as well."[228] IC officials have also increased public communications and started a Tumblr[229] account to post official statements and declassified documents.[230]

As part of the CIA's PPD-28 procedures, the CIA Director tasked the Privacy and Civil Liberties Officer with producing privacy and civil liberties reports.[231] The CIA's Privacy and Civil Liberties Office releases these reports to the public and helps people understand the efforts the CIA is taking to improve training on PPD-28's requirements, review compliance, and test new systems that will help protect privacy.[232]

A revised PPD-28 should incorporate this good idea and mandate the production of brief semiannual reports by all of the intelligence agencies so that the public can track governmental efforts and improvements in the area of privacy and civil liberties.

---

[227] New York Times Co. v. United States, 403 U.S. 713, 719 (1971) (Black, J., concurring).

[228] Litt, *supra* note 125.

[229] Brian Boone, *How Tumblr Works*, HOWSTUFFWORKS (Sept. 4, 2012), https://computer.howstuffworks.com/tumblr.htm.

[230] *Id.*

[231] CIA PPD-28 PROCEDURES, *supra* note 114.

[232] *See generally* OFFICE OF PRIVACY & CIVIL LIBERTIES, CENT. INTELLIGENCE AGENCY, SEMIANNUAL REPORT: JANUARY–JUNE 2016 (2017), https://www.cia.gov/about-cia/privacy-and-civil-liberties/semiannual-reports/Sec_803_Report_June2016.pdf; OFFICE OF PRIVACY & CIVIL LIBERTIES, CENT. INTELLIGENCE AGENCY, SEMIANNUAL REPORT: JULY 2016–DECEMBER 2016 (2017), https://www.cia.gov/about-cia/privacy-and-civil-liberties/semiannual-reports/2016_Q3_Q4_CIA_OPCL_Semi_Annual_Report.pdf.

G. Ratification by Congress

Based on the Court of Justice of the European Union and the advocate general's concerns in *Schrems II*, Congress may need to take action to codify the protections of PPD-28 in legislation. Legislation would be much harder to update in the future than a presidential policy directive, so any proposed bill should include a sunset clause requiring reauthorization every few years. Despite this diminished flexibility, legislation would address the advocate general's observation[233] that PPD-28 could be "revoked or amended by the U.S. executive at any time" and "therefore do[es] not afford the degree of legal foreseeability that EU law requires."[234] Any proposed legislation would likely come with significant debate, but it is possible that the protection of U.S.-EU trade relationships could garner bi-partisan support.

IV. THE GROWTH OF DATA AND THE FUTURE OF INTELLIGENCE AND PRIVACY

As President Obama emphasized in his remarks accompanying the release of PPD-28, U.S. "intelligence agencies will continue to gather information about the intentions of governments . . . around the world, in the same way that the intelligence services of every other nation does."[235] Given the reality of more available data to collect, signals intelligence procedures must evolve to take advantage of the explosion in available data while still protecting the privacy of ordinary citizens. This issue will drive not only intelligence oversight, but also how we think about oversight of private sector data collection, which the federal government has largely ignored.

A. Dealing with the Growth of Data in Intelligence

The volume of information the IC must process has been growing for decades, but as signals intelligence collects increasing amounts of data, the IC will need to continually improve practices to identify and analyze the right information while avoiding or discarding the rest.

Commentators have argued that the terrorist attacks of September 11, 2001 did not result from a lack of intelligence collection, but rather from "the government not making effective use of the

[233] *See supra* Section I.D.2.
[234] Propp, *supra* note 49.
[235] Obama, *supra* note 2.

information already in its possession, and failing to adequately share information among government agencies."[236] The information overload that existed as far back as 2001 so severely hampered analysis that Congress, in passing the Patriot Act, "instructed the Treasury Department to find ways to cut down on the amount of intelligence collected because the volume of reports was 'interfering with effective law enforcement.'"[237]

In 2004, DOJ reported that over 120,000 hours of surveillance tapes "remained untranslated at FBI headquarters because of a continuing shortage of qualified personnel."[238] A White House review of the 2009 "underwear bomber," Umar Farouk Abdulmutallab, found that "a significant amount of critical information was available to the intelligence agencies but was 'embedded in a large volume of other data.'"[239] Similarly, an investigation following the 2009 Fort Hood shootings by U.S. Army Major Nidal Hassan found that "the 'crushing volume' of information was one of the factors that hampered accurate analysis prior to the attack."[240] As of 2014, the NSA estimated that it "touches" information equivalent to 580 million file cabinets of documents every single day.[241] The amount of information being collected is so vast that U.S. Cyber Command in 2016 reportedly "lack[ed] the storage space to store all the information stolen from ISIS accounts" during Operation Glowing Symphony, a cyber campaign against ISIS.[242]

Creating systems that identify and analyze the "right" information presents an extremely difficult challenge, and officials will have to conduct rigorous oversight to ensure that SIGINT programs do not waste taxpayer money. For example, an NSA system "that analyzed logs of Americans' domestic phone calls and text messages cost $100

---

[236] Stephanie Cooper Blum, *What Really Is At Stake With the FISA Amendments Act of 2008 and Ideas for Future Surveillance Reform*, 18 B.U. PUB. INT. L. J. 269, 313 (2009).

[237] STEPHEN J. SCHULHOFER, RETHINKING THE PATRIOT ACT: KEEPING AMERICA SAFE AND FREE 27 (2005).

[238] *Id.* at 27.

[239] *FISA Amendments Act: Reauthorizing America's Vital National Security Authority and Protecting Privacy and Civil Liberties: Hearing Before the S. Comm. on the Judiciary*, 115th Cong. 21 (2017) (statement of Elizabeth Goitein, Co-Dir., Brennan Ctr. for Justice at N.Y.U.).

[240] *Id.*

[241] Byman & Wittes, *supra* note 37, at 134.

[242] Catalin Cimpanu, *US Cyber Command Was Not Prepared to Handle the Amount of Data It Hacked From ISIS*, ZDNET (Jan. 21, 2020, 8:53 PST), https://www.zdnet.com/article/us-cyber-command-was-not-prepared-to-handle-the-amount-data-it-hacked-from-isis/ [https://perma.cc/766T-WHBU].

million from 2015 to 2019, but yielded only a single significant investigation," according to a PCLOB report.[243] The NSA decided to end the program, partly because of this "high cost and low value," but it can take substantial time and monetary investment just to realize that an intelligence program does not work. Evaluating the appropriate balance between the cost of SIGINT programs and how much valuable intelligence they produce is a process that will continue to require substantial oversight.

The growth of intelligence collected poses a further difficulty of achieving perfect procedural compliance with so much intercepted information. For example, in 2018, the NSA "purged hundreds of millions of [phone] records after it realized that its database was contaminated with some files the agency had no authority to receive."[244] The NSA ended the program partially because of these compliance issues.

If a SIGINT agency like NSA has compliance problems with a phone records collection program, agencies across the IC will likely struggle with compliance as the government starts collecting all sorts of other kinds of data from all over the world. Technologist Bruce Schneier has expressed concern about facial recognition technology, laser-based systems that can identify people based on their heart beat or gait, cameras that can read fingerprints of iris patterns from meters away, and other identifying information such as MAC addresses, phone numbers, credit card numbers, and car license plates.[245] The current Chinese government provides a cautionary tale about the power of a surveillance state that uses these technologies in combination. Government as a whole will need intelligence protocols in place sufficient to minimize the collection of superfluous information, analyze the significant amount of potentially valuable information that is collected, and maintain oversight mechanisms sufficient to ensure that promised privacy protections are being observed.

B. Dealing with the Growth of Data in the Private Sector

If the government acts proactively in conducting strong surveillance oversight, it may also pave the way for much-needed

---

[243] Charlie Savage, *N.S.A. Phone Program Cost $100 Million, but Produced Only Two Unique Leads*, N.Y. TIMES (Feb. 25, 2020), https://www.nytimes.com/2020/02/25/us/politics/nsa-phone-program.html.

[244] *Id.*

[245] Bruce Schneier, *We're Banning Facial Recognition. We're Missing the Point.*, N.Y. TIMES (Jan. 20, 2020), https://www.nytimes.com/2020/01/20/opinion/facial-recognition-ban-privacy.html.

oversight of private sector data collection. Technology companies collect information on their users that is "more detailed than those of any police state of the previous century," and yet only Vermont has passed a law "that requires data brokers to register and explain in broad terms what kind of data they collect."[246]

Consumer data-sets available online containing user location information collected by private companies can and have been used to "track the movements of President Trump's Secret Service guards and of senior Pentagon officials . . . connect[ing] a supposedly anonymous data trail to a name and address."[247] A new facial recognition company called Clearview AI also created a database of over three billion photos by scraping "Facebook, YouTube, Venmo and millions of other websites."[248] While technology companies like Google have refrained from similar projects in the past due to fears of abuse, the lack of regulation has allowed Clearview AI to build the platform that other companies avoided out of discretionary prudence.[249] This kind of technology has both compelling use cases (e.g., the Indiana State Police solving a shooting case "within 20 minutes of using the app"[250]) and extremely concerning and even abusive use cases (e.g., a billionaire using the app to instantly identify a man on a date with the billionaire's adult daughter[251]). At the time of this writing, Facebook, Google, and other companies have sent cease-and-desist letters to the facial recognition company, plaintiffs have filed lawsuits in Illinois and Virginia, and "the attorney general of New Jersey issued a moratorium against the app in that state."[252]

As the federal government, in its implementation of signals intelligence oversight regimes, tackles issues of protecting privacy in a world of massive data collection, it should also consider applying that expertise to the private sector, at least more than it has thus far.

---

[246] *Id.*

[247] Editorial Board, Editorial, *Total Surveillance Is Not What America Signed Up For*, N.Y. TIMES (Dec. 21, 2019), https://www.nytimes.com/interactive/2019/12/21/opinion/location-data-privacy-rights.html.

[248] Kashmir Hill, *The Secretive Company that Might End Privacy as We Know It*, N.Y. TIMES (Jan. 18, 2020), https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html.

[249] *Id.*

[250] *Id.*

[251] Kashmir Hill, *Before Clearview Became a Police Tool, It Was a Secret Plaything of the Rich*, N.Y. TIMES (Mar. 5, 2020), https://www.nytimes.com/2020/03/05/technology/clearview-investors.html.

[252] *Id.*

CONCLUSION

The issues identified in this Note are small relative to the enormity of the U.S. intelligence-gathering apparatus and the proposed revisions presented are modest. However—in a world in which European courts void data-sharing agreements between the U.S. and EU that would support billions of dollars of industry based on their review and rejection of US surveillance policy—the U.S. government must exercise extreme care when crafting documents like PPD-28. As evidenced by the *Schrems* cases, even a generally overlooked document like PPD-28 can emerge as a key factor in international relations.

As global norms develop around data collection by governments and private sector companies, the U.S. would benefit from pioneering norms with which Americans and non-Americans alike agree rather than being dragged along by the rest of the world. With the U.S., EU, and China vying for global influence, the U.S. can earn its spot as a global leader in the realm of privacy if it proactively pushes for privacy norms that reasonably respect each country's right to gather intelligence to protect itself, while resisting government overreach into private spheres. Otherwise, the U.S. will get stuck between a European Union trying to impose potentially impractical privacy rules on the rest of the world and China constructing an increasingly pervasive and invasive surveillance state. U.S. leadership on this issue helps promote the security and the liberty of U.S. persons, if not all persons subject to signals intelligence surveillance by any nation.