Western New England University
Digital Commons @ Western New England University

Faculty Scholarship | School of Law Faculty Scholarship

2017

The President's Private Dictionary: How Secret Definitions Undermine Domestic and Transnational Efforts at Executive Branch Accountability

Sudha Setty
Western New England University School of Law, ssetty@law.wne.edu

Follow this and additional works at: https://digitalcommons.law.wne.edu/facschol

 Part of the International Humanitarian Law Commons, and the President/Executive Department Commons

Recommended Citation

Sudha Setty, The President's Private Dictionary: How Secret Definitions Undermine Domestic and Transnational Efforts at Executive Branch Accountability, 24 IND. J. GLOBAL LEGAL STUD. 513 (2017).

This Article is brought to you for free and open access by the School of Law Faculty Scholarship at Digital Commons @ Western New England University. It has been accepted for inclusion in Faculty Scholarship by an authorized administrator of Digital Commons @ Western New England University.

The President's Private Dictionary: How Secret Definitions Undermine Domestic and Transnational Efforts at Executive Branch Accountability

SUDHA SETTY*

ABSTRACT

The 2016 EU-U.S. Privacy Shield is an agreement allowing companies to move customer data between the European Union and the United States without running afoul of heightened privacy protections in the European Union. It was developed in response to EU concerns that the privacy rights of its citizens have been systematically abrogated by the U.S. government in the name of national security, and contains a variety of assurances that the United States will respect and protect the privacy rights of EU citizens.

How trustworthy are the U.S. assurances under the Privacy Shield? Both the Bush and Obama administrations secretly interpreted the terms of treaties, statutes, and regulations in a manner that allowed them to take controversial actions, keep those actions secret, and later invoke national security to defend the legality of those actions if they became public. In cases involving torture, bulk data collection, and targeted killing, these administrations did so despite the common and objective understanding of applicable legal constraints not providing authorization for the very actions that they claimed were legal.

It remains an open question as to whether the Trump administration will interpret the Privacy Shield in a similarly misleading manner: one in

* Professor of Law and Associate Dean for Faculty Development & Intellectual Life, Western New England University School of Law. Some elements of this Article are drawn from the forthcoming book: Sudha Setty, NATIONAL SECURITY SECRECY: COMPARATIVE EFFECTS ON DEMOCRACY AND THE RULE OF LAW (Cambridge Univ. Press 2017). The author is grateful for the comments offered on the presentation of this Article at the *Transnational Executive* symposium hosted by the Indiana Journal of Global Legal Studies in March 2016. Special thanks to Fred Aman and the organizers of the symposium, as well as to Matthew H. Charity, Kathleen Claussen, Federico Fabbrini, and Peter Margulies for their thoughtful comments and insights. Finally, many thanks to law librarian Renee Rastorfer and student Courtney Rafus for their research assistance. © Sudha Setty 2017.

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

which public assurances suggest compliance with the Privacy Shield's constraints, but the administration's private interpretation of the Privacy Shield secretly breaches EU privacy protections. This Article considers possible ways to constrain the executive branch from relying on secret interpretations that would undermine the Privacy Shield's transnational attempts at accountability.

INTRODUCTION

"Trust is a must, it is what will drive our digital future."[1]

National security related surveillance is always a tricky business. On the one hand, much of its operational details are solely in the hands of the executive branch and are kept out of the public eye to improve its effectiveness. On the other hand, when the public does not understand the scope of or limitations to surveillance, and the laws meant to constrain such surveillance seem ineffective, secrecy opens the door for any number of constitutional, civil, and human rights to be violated. The government can undercut privacy and dignity rights and chill freedom of expression, religion, association, and thought. As a result, trust in government and its institutions erodes.

The European Union guarantees greater privacy and dignity rights than have been found under the U.S. Constitution, bringing the two jurisdictions into a potential conflict when a transnational privacy issue occurs. One context in which these competing, transnational privacy interests are often in tension involves the transfer of data for business purposes. Many large companies utilize data transfers on a daily basis and in large volume. They depend on agreements between the United States and the European Union to facilitate these data transfers in a manner that comports with the legal framework of both jurisdictions, thus limiting the potential for a legal challenge.

From July 2000 to October 2015, companies relied on an agreement between the U.S. Department of Commerce and the European Commission for Justice, Consumers and Gender Equality called the Safe Harbor Privacy Principles[2] (Safe Harbor) to enable these transnational data transfers. In the words of one of the U.S. regulators involved in 2000, the Safe Harbor "bridges the differences between EU and U.S.

1. Press Release, European Comm'n, Restoring Trust in Transatlantic Data Flows Through Strong Safeguards: European Commission Presents EU-U.S. Privacy Shield (Feb. 29, 2016) (quoting European Commission Vice-President and European Commissioner for the Digital Single Market Andrus Ansip on the agreement over the EU-U.S. Privacy Shield).

2. U.S. DEP'T OF COMMERCE, SAFE HARBOR PRIVACY PRINCIPLES (2000) [hereinafter SAFE HARBOR].

approaches to privacy protection and will ensure that data flows between the U.S. and the EU are not interrupted. As a result, it should help ensure that e-commerce continues to flourish."[3] The Safe Harbor promoted transnational commerce and withstood legal challenge based on the different standards of privacy in the United States and European Union for over a decade.[4]

In June 2013, the global community became more aware of the breadth and depth of U.S. surveillance of internet and telephone activity in the name of national security. Former National Security Agency (NSA) contractor Edward Snowden disclosed a trove of information regarding U.S. domestic and global surveillance conducted by the U.S. government in conjunction with other governments. Those disclosures allowed the public to understand that personal internet data, if transferred to the United States, was likely accessible to the U.S. government under a variety of national security justifications and legal authorizations. Because the United States specifically carved out national security from its obligations under the Safe Harbor, it had not prevented any U.S. agency involved in national security matters from accessing and utilizing the personal data of European citizens.[5]

These developments prompted Austrian law student and Facebook user Maximilian Schrems to bring suit before Ireland's data protection commissioner. Schrems alleged that the data in his Facebook account that was transferred to and from the United States as part of Facebook's business operations was, unbeknownst to him, accessible by the NSA and other U.S. government agencies, which constituted a violation of his rights as an EU citizen. As discussed in Part I, the European Court of Justice (CJEU) agreed and invalidated the Safe Harbor agreement between the European Union and the United States. It held that the purpose of the Safe Harbor was to enable private companies to move customer-related data between the European Union and the United States without running afoul of heightened protections for personal privacy in the European Union, and that the Snowden disclosures made clear that the central purpose of the Safe Harbor was not being fulfilled.

The CJEU decision led to a fast-paced set of negotiations by U.S. and EU regulators that culminated in the creation of a new agreement, known as the EU-U.S. Privacy Shield Framework Principles (Privacy Shield), in

---

3. Letter from Robert S. LaRussa, Acting Under Sec'y, Int'l Trade Admin. (July 21, 2000), https://build.export.gov/main/safeharbor/eu/eg_main_018494.

4. *See generally* Commission Decision 2000/520/EC, 2000 O.J. (L 215) 7 (outlining safe harbor privacy principles between the EU and U.S. Department of Commerce).

5. *See* SAFE HARBOR, *supra* note 2 ("Adherence to these Principles may be limited . . . to the extent necessary to meet national security, public interest, or law enforcement requirements.").

February 2016.[6] The new Privacy Shield looked to heighten protections for the data privacy of European citizens and brought into focus the extent of the difference between the United States and European Union safeguards of individual rights. In particular, it focused on the extent to which consumers have the right to protect their data from being sold to third parties and from national security surveillance and data mining by the U.S. government. The Privacy Shield included a number of safeguards to assure EU regulators that U.S. intelligence agencies would respect the data privacy guarantees of EU citizens, including written guarantees by U.S. government officials as to their adherence to the delineated privacy protections, annual privacy reviews conducted by the U.S. government and EU regulators, and the appointment of a data privacy ombudsperson with the U.S. State Department to field any complaints from EU residents alleging privacy violations by a corporation or by the U.S. government.[7] Despite some criticism that the Privacy Shield did not sufficiently address the concerns of the CJEU in *Schrems*,[8] it was finalized in July 2016.[9]

This Article considers the theoretically robust protections for privacy embedded in the Privacy Shield and potential problems in the way the

---

6. *See* Mark Scott, *E.U. and U.S. Release Details on Trans-Atlantic Data Transfer Deal*, N.Y. TIMES (Feb. 29, 2016), https://www.nytimes.com/2016/03/01/technology/eu-us-trans-atlantic-data-transfer-deal.html.

7. *See* U.S. DEP'T OF COMMERCE, E.U.-U.S. PRIVACY SHIELD FRAMEWORK PRINCIPLES (2016) [hereinafter PRIVACY SHIELD]; Mark Scott, *European Privacy Regulators Want Details on 'Safe Harbor' Data Deal*, N.Y. TIMES (Feb. 3, 2016), https://www.nytimes.com/2016/02/04/technology/european-privacy-regulators-want-more-details-on-us-safe-harbor-data-deal.html (detailing some of the concerns surrounding the enforcement of the potential privacy protections discussed in the negotiations for the Privacy Shield).

8. *See* Catherine Stupp, *Privacy Shield Agreement Signed off Despite Vote Abstentions*, EURACTIV (July 8, 2016), http://www.euractiv.com/section/digital/news/privacy-shield-agreement-signed-off-despite-vote-abstentions/.

9. *See* Commission Implementing Decision 2016/1250, 2016 O.J. (L 207) 1 (EU); Mark Scott, *Europe Approves New Trans-Atlantic Data Transfer Deal*, N.Y. TIMES (July 12, 2016), https://www.nytimes.com/2016/07/13/technology/eunashvirope-eu-us-privacy-shield.html. Regulators heralded the approval of the Privacy Shield based both on the privacy protections and the enabling of transnational business:

> With the approval of the EU-U.S. Privacy Shield, we send an important message to the world: The sharing of ideas and information across borders is not only good for our businesses but also for our communities and our people. For businesses, the free flow of data makes it possible for a startup in Silicon Valley to hire programmers in the Czech Republic . . . . For consumers, the free flow of data means that you can take advantage of the latest, most innovative digital products and services, no matter where they originate.

Penny Pritzker, U.S. Sec'y of Commerce, Remarks at the E.U.-U.S. Privacy Shield Framework Press Conference (July 12, 2016), https://www.commerce.gov/news/secretary-speeches/2016/07/remarks-us-secretary-commerce-penny-pritzker-eu-us-privacy-shield.

United States might privately interpret its obligations under the Privacy Shield. Considering those pitfalls, this Article offers a suggestion for reforming the Privacy Shield to increase the likelihood that it will be interpreted and implemented by the United States in ways that adequately address the concerns of the CJEU and properly protect fundamental privacy rights for EU citizens.

Part I of this Article reviews the development and extent of privacy rights protected by EU-level institutions and discusses why the CJEU held that the Safe Harbor was unable to adequately protect those rights. Part II considers some problematic examples of misleading interpretive methodology and constructive secrecy[10] when it comes to national security matters: situations in which the U.S. government claimed adherence to a certain set of publicly available principles, but its private—and often secret—interpretation of the obligations set forth in the public document were actually quite different from what the public believed the obligations to entail. If the U.S. government's private interpretation of the Privacy Shield is significantly different than the commonly understood meanings of the terms of the deal, this would be a matter for serious concern in terms of the substantive enforcement of the negotiated agreement and for the rule of law. Given the risk of interpretive dissonance and constructive secrecy with regard to the Privacy Shield, Part III offers a simple suggestion for reform.

I. THE EU FRAMEWORK FOR PRIVACY RIGHTS

The EU framework for individual privacy rights relies on overlapping legislative and constitutional bases.[11] The interpretation of the framework, largely the work of the CJEU, limits government, law enforcement and intelligence agencies, and private companies in terms of their access to the personal information of EU residents. In doing so, the CJEU is at the forefront of institutions attempting to carve out a space for individuals to retain control over what information is made public and made available to governments, law enforcement, and the intelligence community.[12] It remains to be seen in the coming years whether the

10. Constructive secrecy is discussed in detail in Part II, *infra*.

11. Federico Fabbrini, *The EU Charter of Fundamental Rights and the Rights to Data Privacy: The EU Court of Justice as a Human Rights Court*, *in* THE EU CHARTER OF FUNDAMENTAL RIGHTS AS A BINDING INSTRUMENT 261 (Sybe de Vries et al. eds., 2015).

12. *See Tele2 Sverige AB v. Post- och telestyrelsen*, Case C-203/15, 2016 E.C.R. ¶ 112 ("*Tele2*"). This December 2016 CJEU decision invalidated sections of the United Kingdom's Data Protection and Investigatory Powers Act 2014 that required bulk collection of telecommunications metadata and invalidated data retention orders issued by the Swedish Post and Telecom Authority, on the basis that EU privacy law precludes domestic legislation

CJEU and other EU institutions continue to push forward in protecting privacy rights or the CJEU eventually succumbs to substantial governmental and private sector pressure to allow for more data collection as part of a neoliberal model of governance. As evidenced by the *Schrems* decision in 2015, the CJEU has thus far robustly protected privacy rights.

The CJEU decision in *Schrems* drew on a relatively strong backdrop of EU protections for informational privacy that had been in place for decades. In 1995, the adoption of a Data Protection Directive included the affirmative obligation of EU Member States to "protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy, with respect to the processing of personal data."[13] Further, Member States are responsible for ensuring that data collection is not excessive and is conducted only when the target has given consent.[14] The standard for compliance under the Data Protection Directive turns on either affirmative consent or the data collection being "necessary:"[15]

> Member States shall provide that personal data may be processed only if: (a) the data subject has *unambiguously given his consent*; or (b) processing is *necessary* for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; or (c) processing is *necessary* for compliance with a legal obligation to which the controller is subject; or (d) processing is *necessary* in order to protect the vital interests of the data subject; or (e) processing is *necessary* for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed; or (f) processing is *necessary* for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for

---

that provides for "general and indiscriminate retention of all traffic and location data of all subscribers and registered users." Press Release No. 145/16, E.C.J. (Dec. 21, 2016).

13. Directive 95/46/EC, art. 1, 1995 O.J. (L 281) 31, 38. This Directive will be replaced by the more comprehensive General Data Protection Regulation that will go into effect in May 2018. *See* Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016, 2016 O.J. (L 119) 1.

14. Directive 95/46/EC, art. 1.

15. *Id.* art. 7.

> fundamental rights and freedoms of the data subject which require protection under Article 1(1).[16]

In terms of the first way in which the Data Protection Directive has historically been satisfied, European Union users of Facebook and many other services have given their consent to transfer data through the use of Standard Contractual Clauses[17] that the European Commission preapproved as satisfying data protection requirements. In consenting to user agreements that contain these Standard Contractual Clauses, European citizens may have wittingly or unwittingly contributed to the undercutting of their own guaranteed fundamental right to privacy.[18] Litigation on the question of consent and the use of Standard Contractual Clauses is ongoing. As such, it is still unclear how the European courts view arguments regarding whether consent is made unknowingly or without meaningful choice and, therefore, whether privacy rights are implicated when consumers consent to the sharing of their data.[19]

Regarding the second prong, the Data Protection Directive is directed at governments and private entities alike. As evidenced in *Schrems*, the European Union has been skeptical of the stated corporate need for seamless information transfer about individuals across international

---

16. *Id.* (emphasis added).

17. *See Model Contracts for the Transfer of Personal Data to Third Countries*, EUR. COMM'N (Nov. 24, 2016); Christopher Kuner, *Improper Implementation of EU Data Protection Law Regarding Use of the Standard Contractual Clauses in Germany*, (Oct. 6, 2006), *available at* https://papers.ssrn.com/sol3/papers2.cfm?abstract_id=1444813 (critiquing the Standard Contractual Clauses for undercutting individual privacy rights).

18. *See* Francesca Bignami, *Transatlantic Privacy Regulation: Conflict and Cooperation*, 78 LAW & CONTEMP. PROBS. 231, 239-40 (2015); *European Ruling Is Merely a Symbolic Victory for Privacy*, N.Y. TIMES (Oct. 9, 2015), https://www.nytimes.com/2015/10/09/opinion/european-ruling-is-merely-a-symbolic-victory-for-privacy.html.

19. Soon after the 2015 CJEU ruling in *Schrems*, Schrems himself challenged the standard form contractual language used by Facebook before the Irish Data Protection Commissioner. *See* Update on Litigation Involving Facebook and Maximilian Schrems: Explanatory Memo, OFFICE OF THE DATA PROT. COMM'R, https://www.dataprotection.ie/docs/28-9-2016-Explanatory-memo-on-litigation-involving-Facebook-and-Maximilian-Schrems/1598.htm (Mar. 16, 2017). The Data Protection Commissioner issued a Draft Decision in May 2016 that Facebook's contractual language did not adequately address the concerns over data privacy. *See id.* The question of whether the matter should be referred to the CJEU for consideration was heard by the Irish High Court in February 2017. *See id.* As of April 2017, the Irish Data Protection Commissioner had not yet made a decision as to whether to refer Schrems's case to the CJEU. *See id.* A similar concern over data privacy was apparent in *Tele2*, in which the CJEU opined that, in order for European telecommunications providers to comport with their EU privacy obligations, "national legislation must make provision for the data to be retained within the European Union and for the irreversible destruction of the data at the end of the data retention period." *Tele2*, *supra* note 12, ¶ 122.

borders.[20] Regular and voluminous transfers of user data are essential to Facebook's ability to process, store, and monetize user data. Schrems contested the transfer of the data in his Facebook profile from Ireland, where Facebook's European operations are headquartered, to the United States. Ireland's Data Protection Commissioner denied Schrems's initial complaint on the grounds that a 2000 European Commission Decision found that the Safe Harbor provides sufficient protection for consumer data.[21]

The Irish High Court heard Schrems' appeal and sought guidance from the CJEU as to whether a domestic data protection authority had the right, despite the 2000 European Commission decision, to conduct an independent investigation as to whether the 1995 Data Protection Directive was being enforced in ways that provided adequate protection to EU customers. As an initial matter, the CJEU found that domestic data protection commissions in the European Union had such authority.

The CJEU also took on the central issue that Schrems raised: whether the Safe Harbor was an insufficient control on U.S. data sharing practices, particularly in light of the 2013 Snowden disclosures. Schrems pointed to two conflicting principles. The first was the guarantee of privacy protection as a fundamental human right under the Data Protection Directive and Article 7 of the Charter of the European Union. Article 25 of the Data Protection Directive makes the obligations of EU nations clear:

> 1. The Member States shall provide that the transfer to a third country of personal data . . . may take place only if . . . the third country in question ensures an adequate level of protection.
>
> 2. The adequacy of the level of protection afforded by a third country shall be assessed in the light of all the circumstances surrounding a data transfer operation or set of data transfer operations; particular consideration shall be given to the nature of the data, the purpose and duration of the proposed processing operation or operations, the country of origin and country of final destination, the rules of law, both general and sectoral, in force in the third country in question and the professional

20. *See* Case C-362/14, Schrems v. Data Protection Comm'r, 2015 E.C.R. 650, ¶ 34 (noting that legislation allowing general access to electronic data transfers undercuts the fundamental right to private life).

21. *See id.* ¶¶ 5–10 (discussing Commission Decision 2000/520/EC, *supra* note 4).

> rules and security measures which are complied with in that country.[22]

This protective language conflicts, however, with the second principle embodied in the language of the Safe Harbor, which qualifies the obligations of U.S. companies in numerous ways:

> Adherence to these Principles may be limited: (a) to the extent necessary to meet national security, public interest, or law enforcement requirements; (b) by statute, government regulation, or case-law that create conflicting obligations or explicit authorisations, provided that, in exercising any such authorisation, an organisation can demonstrate that its non-compliance with the Principles is limited to the extent necessary to meet the overriding legitimate interests furthered by such authorisation.[23]

The CJEU evaluated the privacy protection against the national security carve-out, along with information about the actual domestic practices of the United States that could protect or undercut privacy.[24] Looking at the actual practices of the United States in terms of bulk data and metadata collection and storage and the lack of effective oversight of these practices, the CJEU concluded that the Safe Harbor did not adequately protect the fundamental right to privacy as guaranteed under the EU Charter and the Data Protection Directive.[25] Ultimately, it held that the entire agreement was invalid.[26]

The *Schrems* decision had immediate effects for regulators in several countries: numerous domestic privacy regulators within the EU began taking a closer look at whether their citizens' data was being misused by U.S. companies in ways that violated EU privacy rights. As a result, a number of U.S. companies were ordered to modify their practices for data collection and use.[27] Also, U.S. and EU negotiators began talks to draw

---

22. Directive 95/46/EC, *supra* note 13, art. 25.

23. *Schrems*, 2015 E.C.R. 650, ¶ 8 (citing U.S. Department of Commerce communications regarding its safe harbor obligations).

24. *Id.* ¶ 75.

25. *See id.* ¶¶ 90-96 ("In particular, legislation permitting the public authorities to have access on a generalised basis to the content of electronic communications must be regarded as compromising the essence of the fundamental right to respect for private life, as guaranteed by Article 7 of the Charter . . . .").

26. *Id.* ¶ 106.

27. *See, e.g.*, *Facebook Hit by French Privacy Order*, BBC (Feb. 9, 2016), http://www.bbc.com/news/technology-35531224 (discussing the order of the French data protection authority, the Commission Nationale de l'Informatique et des Libertes, to

up a replacement for the Safe Harbor that would provide privacy protections satisfactory to the CJEU while also letting companies conduct the transnational data transfers and processing that is integral to their business models and worth billions of dollars annually.[28]

In February 2016, negotiators came to agreement over the EU-U.S. Privacy Shield, enabling heightened oversight of U.S. governmental data collection.[29] Various safeguards were proposed to assure EU regulators that U.S. intelligence agencies would respect the data privacy guarantees for EU citizens. Those safeguards focused on three particular areas. First, U.S. government officials provided written guarantees as to the manner in which European privacy rights were being respected and data collection would be limited.[30] Second, the U.S. government promised to undertake annual data privacy reviews in conjunction with their EU counterparts.[31] Third, the U.S. State Department promised to appoint a data privacy ombudsperson to field complaints from EU residents regarding the violation of privacy rights by a corporation or by the U.S. government.[32]

Both U.S. and EU negotiators stated that protecting the privacy rights of EU residents was paramount, and the United States attempted to demonstrate its public commitment to the parameters of the Privacy Shield by publishing detailed letters by administrative agencies to that effect.[33] Despite those reassurances and even though the new framework was approved in July 2016, deep skepticism remains as to whether the U.S. intelligence agencies will abide by the terms of the new Privacy

---

Facebook to prevent unfettered online access to data about French Facebook users, and to stop transferring all of its French user data to the United States).

28. *See* Kelly Couturier, *How Europe Is Going After Google, Amazon and Other U.S. Tech Giants*, N.Y. TIMES (updated Dec. 20, 2016), https://www.nytimes.com/interactive/2015/04/13/technology/how-europe-is-going-after-us-tech-giants.html (noting the business value of the data transfers as part of the backdrop that pressured negotiators to move quickly on replacing the invalidated safe harbor provisions after *Schrems*).

29. *See* Press Release, European Comm'n, *supra* note 1.

30. *See generally* Letter from Penny Pritzker, U.S. Sec'y of Commerce, to Věra Jourová, Comm'r for Justice, Consumers, & Gender Equal., European Comm'n (Feb. 23, 2016) (noting the inclusion, with the Privacy Shield, of letters from the Federal Trade Commission, Department of Transportation, and Office of the Director of National Intelligence, each detailing the ways in which each agency would comply with the parameters of the Privacy Shield).

31. *See, e.g.*, PRIVACY SHIELD, *supra* note 7, Annex I: Arbitral Model.

32. *See id.* Annex A: EU-U.S. Privacy Shield Ombudsperson Mechanism.

33. *See, e.g.*, Letter from Robert S. Litt, Office of the Gen. Counsel of the Office of the Dir. of Nat'l Intelligence, to Justin S. Antonipillai & Ted Dean (Feb. 22, 2016) (sending a detailed letter to the U.S. Department of Commerce and the International Trade Administration describing the information that the ODNI shared with European Union regulators in the process of negotiating the Privacy Shield).

Shield,[34] particularly in light of the post-September 11 practice of the U.S. government to use national security as a pretext for reinterpreting its obligations under international law and transnational agreements.

II. POTENTIAL PITFALLS IN INTERPRETING THE PRIVACY SHIELD

Numerous important concerns hang over the new Privacy Shield,[35] and this Part focuses on one of the interpretive questions: how will the United States construe the limitations in the Privacy Shield as an operational matter? Will it comport with the generally understood meaning of the terms of the agreement, or will it use a type of "constructive secrecy" to undermine the CJEU's decision in *Schrems*?

Constructive secrecy can be best understood as occurring when the government makes a commitment on terms that are commonly understood, but the government has a second interpretation of that commitment—kept secret from the public—that is quite different than the public understanding. Under such circumstances, the government may claim that it has abided by its public commitment and that it is not developing secret law and policy that undermines the public commitment; in fact, the meaning on which the government is relying may be technically available through piecing together a variety of sources and making inferential leaps as to what the government is actually doing.[36] But if the government allows the dissonance between the publicly understood meaning and the private, legally operative meaning to stand, then oversight becomes less effective, transnational counterparties cannot properly hold the executive branch to account, and the rule of law is undermined—all in secret.[37]

Although it seems Orwellian to foster or at least allow for a disjunctive understanding of a legally operative term in order to further utilitarian national security ends, the last fifteen years suggest that this

---

34. *See* Mark Scott, *U.S. and Europe in 'Safe Harbor' Data Deal, but Legal Fight May Await*, N.Y. TIMES (Feb. 2, 2016), https://www.nytimes.com/2016/02/03/technology/us-europe-safe-harbor-data-deal.html.

35. *See* Peter Margulies, *Privacy Shield's Prospects: The Good, the Bad, and the Ugly*, LAWFARE (Mar. 3, 2016, 8:50 AM), https://www.lawfareblog.com/privacy-shields-prospects-good-bad-and-ugly.

36. *See generally* Sudha Setty, NATIONAL SECURITY SECRECY: COMPARATIVE EFFECTS ON DEMOCRACY AND THE RULE OF LAW (forthcoming Cambridge Univ. Press 2017) (introducing the concept of constructive secrecy and its implications for oversight in national security contexts).

37. *See* Shirin Sinnar, *Rule of Law Tropes in National Security*, 129 HARV. L. REV. 1566, 1568–69 (2016) ("By publicly promoting a known standard but concealing its actual interpretation, the national security executive hinders meaningful evaluation of the extent to which its actions comport with individual rights, democratic values, and the law itself.").

kind of constructive secrecy is not uncommon. Its use in both the Bush and Obama administrations should prompt further inquiry into the trustworthiness of recent U.S. government reassurances regarding the Privacy Shield. In the post-September 11 context, both the Bush and Obama administrations interpreted treaties, statutes, and regulations in a manner that allowed the executive branch to take desired but controversial actions, keep those actions secret for some time, and later claim their actions were legally authorized when those actions became public. These administrations did so despite the common and objective understanding of applicable legal constraints seeming not to authorize the actions that the administrations claimed were authorized. The sometimes inconsistent decisions made by the Trump administration thus far with regard to national security, privacy rights, and the obligation to follow existing law also suggest that the European Union should be wary as to how the Trump administration will interpret its obligations under the Privacy Shield.[38]

Three examples from the last fifteen years—the legal justification for torture, the use of weaponized drones to kill individuals outside of a theater of war, and the mass data collection and surveillance of U.S. citizens within the United States—illustrate how corrosive secrecy can be and serve as a reminder as to why measures should be taken to minimize the risk of misleading interpretative approaches that may undermine the letter and aspirations of the Privacy Shield under the Trump administration and beyond.

A. Torture

The Bush administration legitimized torture as an interrogation and control technique for detainees through the development of a body of secret law that authorized torture despite international and domestic prohibitions.[39] As part of that effort, administration lawyers gave legal comfort to those engaging in or promoting the use of torture. Both the acts of torture and the legal justification for it were deliberately kept secret so as to avoid accountability and a public airing of the administration's policy.[40] The justification for torture was based

38. *See, e.g.*, Evan Perez, Pamela Brown & Kevin Liptak, *Inside the Confusion of the Trump Executive Order and Travel Ban*, CNN (Jan. 30, 2017) (describing the confusion among federal government officials and the public as to the scope and applicability of President Trump's Jan. 27, 2017 executive order regarding immigration).

39. Sudha Setty, *No More Secret Laws: How Transparency of Executive Branch Legal Policy Doesn't Let the Terrorists Win*, 57 U. KAN. L. REV. 579, 591 (2009).

40. *Id.* at 593–94.

primarily on two August 2002 memoranda from the Office of Legal Counsel in the Department of Justice (OLC)—held secret until leaked years later—that analyzed the definition of "torture" as applied to interrogation techniques used on persons captured in the so-called "war on terror" and held outside of the United States.[41]

The first memorandum[42] was drafted by then-OLC attorney John Yoo[43] and signed by then-Assistant Attorney General Jay Bybee. Although the Bush administration relied on this memorandum from 2002 to 2004 to delineate those interrogation techniques that were—under its interpretation—lawful,[44] the memorandum itself was only made public through a mid-2004 leak, after the public learned of detainee abuses at the Abu Ghraib prison in Iraq.[45] Congressional and public outrage[46] at the authorization of harsh interrogation techniques, like waterboarding, which had long been considered a form of torture under international law, and the narrowing of the conventional definition of torture[47] to provide

41. *Id.* at 589 (describing the rule of law problems associated with secret lawmaking by the Office of Legal Counsel).

42. Memorandum from Jay S. Bybee, Assistant Att'y Gen., U.S. Dep't of Justice Office of Legal Counsel, to Alberto R. Gonzales, Counsel to the President (Aug. 1, 2002) [hereinafter Bybee Memorandum]. The Bybee Memorandum was superseded, in part, by another memorandum drafted by the acting head of the OLC, Daniel Levin, that addressed the applicability of the Convention Against Torture and disavowed some of the conclusions made in the Bybee Memorandum. *See* Memorandum from Daniel Levin, Acting Assistant Att'y Gen., U.S. Dep't of Justice Office of Legal Counsel, to James B. Comey, Deputy Att'y Gen. (Dec. 30, 2004) [hereinafter Levin Memorandum].

43. John Yoo, *Behind the "Torture Memos"*, SAN JOSE MERCURY NEWS (Jan. 2, 2005), http://www.aei.org/publication/behind-the-torture-memos/.

44. The Defense Department incorporated significant portions of the language from the Bybee Memorandum in its own report on interrogation practices. *See* U.S. DEP'T OF DEF., WORKING GROUP REPORT ON DETAINEE INTERROGATIONS IN THE GLOBAL WAR ON TERRORISM 61–69 (2003) (enumerating thirty-five techniques and evaluating the usefulness of those techniques); Douglas Jehl et al., *C.I.A. Is Seen as Seeking New Role on Detainees*, N.Y. TIMES (Feb. 16, 2005), http://www.nytimes.com/2005/02/16/politics/cia-is-seen-as-seeking-new-role-on-detainees.html (explaining that the Bybee Memorandum was "sought by the C.I.A. to protect its employees from liability").

45. *See* Dana Priest & R. Jeffrey Smith, *Memo Offered Justification for Use of Torture; Justice Dept. Gave Advice in 2002*, WASH. POST (June 8, 2004), http://www.washingtonpost.com/wp-dyn/articles/A23373-2004Jun7.html ("[T]he Justice Department advised the White House that torturing al Qaeda terrorists in captivity abroad 'may be justified,' and that international laws against torture 'may be unconstitutional if applied to interrogations' conducted in President Bush's war on terrorism . . . .").

46. *See* Adam Liptak, *Legal Scholars Criticize Memos on Torture*, N.Y. TIMES, June 25, 2004, at A14 ("[A] law professor at the University of Chicago, said: 'It's egregiously bad. It's very low level, it's very weak, embarrassingly weak, just short of reckless.'").

47. *See* Bybee Memorandum, *supra* note 42, at 46 ("[W]e conclude that torture as defined in and proscribed by [the Convention Against Torture], covers only extreme acts . . . . Because the acts inflicting torture are extreme, there is [a] significant range of acts that though they might constitute cruel, inhuman, or degrading treatment or punishment fail to

legal comfort to interrogators who engaged in harsh techniques,[48] forced President Bush to disavow the use of torture during interrogations.[49]

The second August 2002 memorandum, issued on the same day as the first and also authorized by Bybee,[50] reinforced the administration's view that the definition of torture was extremely narrow and required specific intent by interrogators to cause serious physical or mental harm. Additionally, the second memorandum's specific intent requirement protected interrogators.[51] A heavily redacted version of this memorandum was released by the Bush administration on July 24, 2008, in response to a Freedom of Information Act (FOIA) request.[52] Only the late 2004 OLC memorandum declaring that "[t]orture is abhorrent both to American law and values and to international norms" was voluntarily made public by the administration. However, even this memorandum contained legal protection for CIA interrogators to insulate them from future prosecution.[53]

A March 2003 OLC memorandum[54] provided additional legal comfort to interrogators by asserting that "federal laws prohibiting assault, maiming and other [violent] crimes did not apply to military interrogators" who questioned captives in the war on terror.[55] This

---

rise to the level of torture."). The Bybee Memorandum also stated that the proscriptions of the Convention Against Torture likely did not apply to the President's execution of the war on terror, under the rationale that the Convention infringed upon the President's executive authority as Commander-in-Chief. *Id.* at 36–39 ("[T]he structure of the Constitution demonstrates that any power traditionally understood as pertaining to the executive—which includes the conduct of warfare and the defense of the nation—unless expressly assigned in the Constitution to Congress, is vested in the President.").

48. Additionally, Bybee offered two broad defenses to individuals who used techniques which would fall within the narrowed definition of torture: necessity and self-defense. *See id.* at 39–46.

49. *See* Eric Mink, Editorial, *The Torture Memos Lies, Deceit - and Maybe War Crimes*, ST. LOUIS POST-DISPATCH, Apr. 9, 2008, at D11. *See generally* Levin Memorandum, *supra* note 42 (replacing parts of the Bybee Memorandum that addressed the applicability of the Convention Against Torture and disavowed some of the conclusions from the Bybee Memorandum).

50. Memorandum from Jay S. Bybee, Assistant Att'y General, U.S. Dep't of Justice Office of Legal Counsel, to John Rizzo, Gen. Counsel of the Cent. Intelligence Agency, U.S. Dep't of Justice Office of Legal Counsel (Aug. 1, 2002) [hereinafter Second Bybee Memorandum].

51. *See id.* at 16–17.

52. *Documents Released by the CIA and Justice Department in Response to the ACLU's Torture FOIA*, ACLU, http://www.aclu.org/safefree/torture/36104res20080724.html (last visited Mar. 5, 2017).

53. Levin Memorandum, *supra* note 42, at 1.

54. *See* Memorandum from John C. Yoo, Deputy Assistant Att'y Gen., Office of the Deputy Assistant Att'y Gen., to William J. Haynes II, Gen. Counsel of the Dep't of Def., U.S. Dep't of Justice Office of Legal Counsel 8 n.10 (Mar. 14, 2003).

55. Dan Eggen & Josh White, *Memo: Laws Didn't Apply to Interrogators*, WASH. POST, Apr. 2, 2008, at A1.

memorandum sought to insulate U.S. government agents from prosecution or other legal liability if they used highly coercive interrogation techniques, such as waterboarding, head slapping, and exposure of prisoners to extreme temperatures.[56] The memorandum was initially classified by the Department of Justice to prevent disclosure but was declassified in 2008 after a review undertaken as part of a FOIA lawsuit.[57] The initial classification was made because of purported national security concerns requiring secrecy.[58] This memorandum contained neither sensitive personal information nor details about specific intelligence-gathering programs, but its contents were also kept secret from the top lawyers for each branch of the military.[59]

Public knowledge of the abuses at the Abu Ghraib detention center in Iraq did not prevent the OLC from continuing to generate its body of secret law justifying torture. A nonpublic 2005 opinion authorized torture techniques, such as waterboarding, and the use of such techniques in combination with each other, for the interrogation of persons designated as enemy combatants.[60] A late 2005 opinion was drafted after Congress passed the Detainee Treatment Act of 2005, which specifically outlawed some harsh interrogation techniques.[61] This opinion confirmed that CIA practices were reconcilable with the Detainee Treatment Act's restrictions, once again providing legal cover for CIA interrogators against potential future prosecution.[62] Finally, a 2006 executive order, which was reviewed and approved by the OLC, confirmed authorization for the use of "enhanced" interrogation techniques.[63] Additional

56. *See id.*

57. *See* Press Release, American Civil Liberties Union, *Secret Bush Administration Torture Memo Released Today in Response to ACLU Lawsuit* (Apr. 1, 2008), http://www.aclu.org/safefree/torture/34747prs20080401.html.

58. *See* Eggen & White, *supra* note 55.

59. *See id.*

60. *See* Eggen & White, *supra* note 55. It was later revealed that certain members of Congress were briefed on the use of waterboarding of prisoners as early as 2002, but that they were forbidden from taking written notes on the brief, or from disclosing their knowledge to anyone, including their own staff members. Joby Warrick & Dan Eggen, *Hill Briefed on Waterboarding in 2002*, WASH. POST, Dec. 9, 2007, at A1. Rep. Jane Harman noted that she filed a classified letter objecting to the program, but was prevented from speaking publicly due to the rules of secrecy governing her role on an intelligence committee. *See id.*

61. Detainee Treatment Act of 2005, Pub. L. No. 109-148, 119 Stat. 2739.

62. Scott Shane et al., *Secret U.S. Endorsement of Severe Interrogations*, N.Y. TIMES, Oct. 4, 2007, at A1.

63. *Id.*

memoranda regarding interrogation techniques have been issued but not made public.[64]

Much of the substantive criticism of these memos at the time of the leaks turned on the expansive assertion of executive power[65] and the resulting erosion of due process and human rights protections for persons designated as "enemy combatants."[66] From a rule of law viewpoint, it was disturbing that the Bush administration was able to easily and readily exploit a structural flaw: it interpreted the lack of a requirement to disclose its legal policy as an affirmation that keeping its body of law secret was acceptable, insisting that secrecy was necessary to maintain the integrity of U.S. national security interests,[67] and arguing that information as to interrogation techniques would empower terrorists planning to attack the United States.[68] The Bush administration then used that secrecy to draft a series of memos providing legal comfort for arguably illegal actions under international and domestic law, all while claiming that it was abiding by its legal commitments. The private dictionary of the Bush administration when it came to the meaning of "torture" would not have become known but for leaks, press reporting, and FOIA litigation regarding the grotesque treatment of detainees. In the end, however, torture and the secret legal contortions undertaken by

64. *Id.*

65. Thomas Poguntke & Paul Webb, *The Presidentialization of Politics in Democratic Societies: A Framework for Analysis*, *in* THE PRESIDENTIALIZATION OF POLITICS: A COMPARATIVE STUDY OF MODERN DEMOCRACIES 1 (Thomas Poguntke & Paul Webb eds., 2005).

66. *See* Eggen & White, *supra* note 55; Editorial, *There Were Orders to Follow*, N.Y. TIMES (Apr. 4, 2008), http://www.nytimes.com/2008/04/04/opinion/04fri1.html. (noting that the Yoo Memorandum was "81 pages of twisted legal reasoning to justify President Bush's decision to ignore federal law and international treaties and authorize the abuse and torture of prisoners").

67. *See Wartime Executive Power and the National Security Agency's Surveillance Authority: Hearing Before the S. Comm. on the Judiciary*, 109th Cong. 264-320 (2007) [hereinafter *Wartime Executive Power*] (statement of Alberto R. Gonzales, Attorney General of the United States); Dawn E. Johnsen, *Faithfully Executing the Laws: Internal Legal Constraints on Executive Power*, 54 UCLA L. REV. 1559, 1565 (2007).

68. *See Wartime Executive Power*, *supra* note 67, at 107 (suggesting such revelations remind the enemy that they are being monitored); Carol D. Leonnig & Eric Rich, *U.S. Seeks Silence on CIA Prisons; Court Is Asked to Bar Detainees from Talking About Interrogations*, WASH. POST, Nov. 4, 2006, at A1. The Obama administration echoed this type of language when it attempted to justify the type of data gathering and surveillance that was exposed by Snowden, and which gave rise to the CJEU's invalidation of the Safe Harbor agreement in *Schrems*. *See* Jeremy Herb, *Intel Panel: DOD Report Finds Snowden Leaks Helped Terrorists*, THE HILL (Jan. 9, 2014), http://thehill.com/policy/defense/194937-intel-panel-dod-report-finds-snowden-leaks-helped.

the Bush administration to justify it undermined both international and domestic trust in the Bush administration for its remaining years.

B. Targeted Killings

When he took office in 2009, President Obama promised a return to the rule of law that would uphold national security interests, civil liberties, and the democratic value of governmental transparency. In some matters, he fulfilled his promise of cutting back on national security secrecy, such as reversing the Bush administration's FOIA policy to make access to some types of government information easier.[69] However, there were numerous areas where those aspirations were not met. In the context of the use of drones for targeted killings[70] of militants,[71] administration officials repeatedly emphasized the necessity, efficacy, and legality of targeted killings as a counterterrorism tool.[72] Administration officials resisted the idea that other branches of government and the public have the right to know the parameters of the drone strike program. The program prompted much debate over the threshold question of whether a systemic targeted killing program ought to exist,[73] the moral calculus of remote-control extrajudicial killings,[74] the legal authorities for such a program,[75] and the specific questions

69. *See* Presidential Memorandum for Heads of Executive Departments and Agencies Concerning the Freedom of Information Act, 74 Fed. Reg. 4683, 4683 (Jan. 21, 2009).

70. Although targeted killing is not defined under international law, it is often considered to encompass "premeditated acts of lethal force employed by states in times of peace or during armed conflict to eliminate specific individuals outside their custody." Jonathan Masters, *Targeted Killings*, COUNCIL ON FOREIGN REL. (May 23, 2013), http://www.cfr.org/counterterrorism/targeted-killings/p9627. Although the governments that utilize targeted killings differentiate them from assassinations, critics view them as similar actions in terms of illegality. *Compare* Harold Hongju Koh, Legal Adviser, U.S. Dep't of State, Remarks at the Annual Meeting of the American Society of International Law: The Obama Administration and International Law (March 25, 2010) *with* Complaint at 5, Al-Aulaqi, et al. v. Panetta, No. 1:12-cv-01192-RMC (D.D.C. July 18, 2012).

71. *See Drone Wars Pakistan: Analysis*, NEW AM. FOUND., http://securitydata.newamerica.net/drones/pakistan-analysis.html (last visited Feb. 13, 2016) (detailing the number of drone strikes by the United States in Pakistan since 2004).

72. *See* Koh, *supra* note 70.

73. *See, e.g.*, Philip Alston (Special Rapporteur on Extrajudicial, Summary or Arbitrary Executions), *Study on Targeted Killings*, U.N. Doc. A/HRC/14/24/Add. 6 (May 28, 2010) (questioning the legality of the CIA drone program).

74. *See generally* Samuel Isaacharoff & Richard H. Pildes, *Drones and the Dilemma of Modern Warfare*, *in* DRONE WARS: TRANSFORMING CONFLICT, LAW, AND POLICY 388 (Peter Bergen & Daniel Rothenberg, eds.) (theorizing the moral dilemma of drone use in the context of individuated warfare).

75. *See* Alston, *supra* note 73, ¶¶ 28–92 (discussing international law of war principles with regard to targeted killings); Eric Holder, U.S. Attorney Gen., Speech at Northwestern

regarding the legality of its scope in terms of geographic location and citizenship of the target.[76] Despite these questions, the parameters of the targeted killing program remain largely secret, except for leaks and instances when it was self-serving to the Obama administration to make such information public.[77]

Occasional speeches by Obama administration officials from 2011 onward,[78] a classified Department of Justice memorandum leaked in early 2013,[79] and the Presidential Policy Guidance memorandum drafted in May 2013 and made public in August 2016 disclosed limited information.[80] The early 2013 leak may have prompted the Presidential Policy Guidance, and certainly prompted a May 2013 speech in which President Obama looked to both defend the legality of the targeted

---

University School of Law (Mar. 5, 2012) (outlining the parameters used by the Obama administration to determine whether a targeted killing comports with international and domestic legal obligations); Jeh C. Johnson, Gen. Counsel, Dep't of Def., Speech on National Security Law, Lawyers and Lawyering in the Obama Administration (Feb. 22, 2012) (echoing previous administration legal justifications for targeted killing); Koh, *supra* note 70 (arguing that the Obama administration's use of targeted killing as a counterterrorism tool complied with international and domestic legal obligations).

76. *See* Al-Aulaqi v. Obama, 727 F. Supp. 2d 1 (D.D.C. 2010) (dismissing, based on standing grounds, the suit of Nasser al-Aulaqi to enjoin the U.S. government from keeping his son, U.S. citizen Anwar al-Aulaqi, on its targeted killing list).

77. *See, e.g.*, David E. Pozen, *The Leaky Leviathan: Why the Government Condemns and Condones Unlawful Disclosures of Information*, 127 HARV. L. REV. 512 (2013); Stephanie Condon, *Obama: Anwar al-Awlaki's Death a "Major Blow" to al Qaeda and Affiliates*, CBSNEWS (Sept. 30, 2011, 4:40 PM), http://www.cbsnews.com/news/obama-anwar-al-awlakis-death-a-major-blow-to-al-qaeda-and-affiliates/ (relating comments by President Obama about the strategic importance of the targeted killing Anwar al-Awlaki, a U.S. citizen in Yemen).

78. *E.g.*, John O. Brennan, Assistant to the President for Homeland Security and Counterterrorism, Strengthening Our Security by Adhering to Our Values and Laws, Address at Harvard Law School (Sept. 16, 2011); Letter from Eric H. Holder, Jr., U.S. Att'y Gen., to Patrick J. Leahy, Chairman, Senate Comm. on the Judiciary (May 22, 2013) (detailing the administration's legal basis for the use of targeted killings against Anwar al-Aulaqi and other U.S. citizens overseas); Koh, *supra* note 70.

79. *See* U.S DEP'T OF JUSTICE, DEPARTMENT OF JUSTICE WHITE PAPER: LAWFULNESS OF A LETHAL OPERATION DIRECTED AGAINST A U.S. CITIZEN WHO IS A SENIOR OPERATIONAL LEADER OF AL-QA'IDA OR AN ASSOCIATED FORCE [hereinafter DOJ WHITE PAPER], *available at* http://msnbcmedia.msn.com/i/msnbc/sections/news/020413_DOJ_White_Paper.pdf (last accessed Mar. 5, 2017).

80. *Procedures for Approving Direct Action Against Terrorist Targets Located Outside the United States and Areas of Active Hostilities*, ACLU (May 22, 2013), https://www.aclu.org/sites/default/files/field_document/presidential_policy_guidance.pdf. This memo was disclosed as a result of Freedom of Information Act litigation brought by the American Civil Liberties Union.

killings program and the secrecy surrounding it.[81] At the same time that the administration discussed and leaked aspects of the program, it also relied upon the classified[82] nature of the program to shield itself from media inquiry[83] and from judicial accountability by using the standing doctrine and state secrets privilege to secure the dismissal of a suit challenging the constitutionality of the program.[84]

In his May 2013 speech, President Obama focused largely on the parameters for targeted killings, reiterating known positions of the administration, claiming that drone strikes were legal under international law standards[85] because they defended against "imminent" threats,[86] stating that U.S. citizenship is no protection against being targeted for a drone strike,[87] and making clear that he could keep as much

---

81. *See* President Barack Obama, Remarks by the President at the National Defense University (May 23, 2013), http://www.whitehouse.gov/the-press-office/2013/05/23/remarks-president-national-defense-university [hereinafter May 2013 NDU Speech].

82. *See generally* Jo Becker & Scott Shane, *Secret 'Kill List' Proves a Test of Obama's Principles and Will*, N.Y. TIMES, May 29, 2012, at A1 (discussing internal administration debates as to whether to declassify the legal justifications for the drone program, and noting that the administration decided not to do so); Charlie Savage, *Secret U.S. Memo Made Legal Case to Kill a Citizen*, N.Y. TIMES, Oct. 8, 2011, at A1 (offering details of a still-classified Office of Legal Counsel memorandum justifying the targeted killings of U.S. citizens).

83. *See, e.g.*, N.Y. Times Co. v. U.S. Dep't of Justice, 915 F. Supp. 2d 508 (S.D.N.Y. Jan. 3, 2013) (dismissing requests made under the Freedom of Information Act for documents regarding the targeted killing program, based on the administration's claim of necessary secrecy surrounding counterterrorism programs); Milena Sterio, *The Covert Use of Drones: How Secrecy Undermines Oversight and Accountability*, 8 ALB. GOV'T L. REV. 129, 134-35 (2015) (detailing the selective and utilitarian disclosures surrounding the covert CIA drone program); Jameel Jaffer, *Selective Disclosure About Targeted Killing*, JUST SECURITY (Oct. 7, 2013), https://www.justsecurity.org/1704/selective-disclosure-targeted-killing/.

84. *See generally* Al-Aulaqi v. Obama, 727 F. Supp. 2d 1 (D.D.C. 2010) (dismissing the suit brought by the father of U.S. citizen Anwar al-Awlaki, which sought an injunction against the targeted killing of his son, based on a lack of standing and administration claims of necessary secrecy surrounding counterterrorism programs). Anwar al-Awlaki was killed by a drone strike in September 2011. Charlie Savage, *Court Releases Large Parts of Memo Approving Killing of American in Yemen*, N.Y. TIMES (June 23, 2014), http://www.nytimes.com/2014/06/24/us/justice-department-found-it-lawful-to-target-anwar-al-awlaki.html.

85. *Compare* May 2013 NDU Speech, *supra* note 81, *with* Holder, *supra* note 78, *and* Koh, *supra* note 70 (President Obama articulated proportionality and distinction principles that largely reflected the standards offered by Attorney General Holder and State Department Legal Adviser Koh in previous speeches).

86. *Compare* May 2013 NDU Speech, *supra* note 81, *with* Holder, *supra* note 78, *and* Koh, *supra* note 70 (arguing the legality of ordering a targeted killing when, among other factors, an undefined "imminence" standard was met).

87. *Compare* May 2013 NDU Speech, *supra* note 81 (noting that "the high threshold that we've set for taking lethal action applies to all potential terrorist targets, regardless of whether or not they are American citizens"), *with* Holder, *supra* note 78.

of the drone program secret as he wished.[88] This defense of the drone program sparked criticism on numerous grounds, including the lack of clarity over what constituted an "imminent" threat in the view of the Obama administration.[89] Despite years of FOIA litigation and other attempts to understand more fully the parameters of the targeted killing program, the question remains how the Obama administration's private dictionary defined "imminence."[90]

The idea of basing the decision to use force against an enemy on the question of imminence is not new; in fact, it is quite common in discussions of law of war principles governing the preemptive or anticipatory use of force as a matter of self-defense.[91] The real question was how the standard of "imminence" was being interpreted by the Obama administration. Was it a well-understood and traditional interpretation of the term, such as dealing with an immediate and concrete threat that created the overwhelming need to use force because there is no time for deliberation?[92] Was it a definition of "imminence" grounded in the international human rights principles of necessity and proportionality, such that lethal force is only justifiable if the attack is unavoidable but for the use of that lethal force against the threat?[93] From the information made available through leaks and disclosures, it seems as though neither of these definitions of "imminence" governed the Obama administration's decision making regarding targeted killings. In fact, a 2011 Justice Department White Paper specifically noted that an imminent threat "does not require the United States to have clear evidence that a specific attack on U.S. persons and interests will take place in the immediate future."[94]

The human toll of drone strikes, the U.S definition of the theater of war as encompassing the entire world,[95] the 2013 government prediction that the U.S. efforts against al-Qaeda would last another ten to twenty

88. *See* May 2013 NDU Speech, *supra* note 81.

89. *E.g.*, Fred Kaplan, *Obama's Post-9/11 World*, SLATE (May 23, 2013, 6:25 PM), http://www.slate.com/articles/news_and_politics/war_stories/2013/05/barack_obama_national_defense_university_speech_nothing_new_about_drones.html (noting that the administration's definition of an imminent threat meant that "'imminent' doesn't really mean '*imminent*'").

90. *See* Anna Diakun, *Fighting to Bring the Drone Program into the Light*, ACLU (Oct. 25, 2016), https://www.aclu.org/blog/speak-freely/fighting-bring-drone-program-light.

91. *See* Rosa Brooks, *Drones and the International Rule of Law*, 28 J. ETHICS & INT'L AFF. 83, 93 (2014).

92. *Id.*

93. *See* Sinnar, *supra* note 37, at 1601.

94. DOJ WHITE PAPER, *supra* note 79, at 7.

95. Spencer Ackerman, *Pentagon Spec Ops Chief Sees '10 to 20' More Years of War Against Al-Qaida*, WIRED (May 16, 2013, 11:49 AM), http://www.wired.com/dangerroom/2013/05/decades-of-war/.

years,[96] and the administration's defense of the legality of the program, should beget calls for more accountability measures. Congress and/or the judiciary should assert themselves to protect against and provide redress for arbitrary or abusive decision making in the process of extrajudicial killings. Yet Congress has expressed little will to set meaningful parameters on the program, and the judiciary has shied away from adjudicating the legality of placing targets for extrajudicial killings on a government list, even if those targets are U.S. citizens who are not "imminently" attacking the United States in any conventional sense of the word.[97] Actual protection of rights would necessitate more than rhetoric about the efficacy and legality of the drone program that cannot actually be examined and verified because of national security secrecy. As in the case of torture, the legally operative understandings used by the Obama administration were unknown and may very well have been in violation of public commitments to international and domestic law.

C. The NSA's Metadata Program

Legal constraints on intelligence gathering were loosened significantly in the wake of the September 11 attacks. The Bush and Obama administrations interpreted the USA Patriot Act as authorizing the collection and storage of domestic telephony and internet metadata[98] and the collection and content searches of substantial amounts of foreign telephone and internet communications.[99] This gave the intelligence

96. *Id.*

97. *See generally* Al-Aulaqi v. Obama, 727 F. Supp. 2d 1 (D.D.C. 2010) (dismissing the suit brought by the father of U.S. citizen Anwar al-Awlaki, which sought an injunction against the targeted killing of his son, based on a lack of standing and administration claims of necessary secrecy surrounding counterterrorism programs).

98. The telephony metadata authorized for collection is defined as:

> [I]nclud[ing] comprehensive communications routing information, including but not limited to session identifying information (e.g., originating and terminating telephone number, International Mobile Subscriber Identity (IMSI) number, International Mobile station [sic] Equipment Identity (IMEI) number, etc.), trunk identifier, telephone calling card numbers, and time and duration of call. Telephony metadata does not include the substantive content of any communication . . . or the name, address, or financial information of a subscriber or customer.

See Primary Order at 3 n.1, *In re* Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things From [Redacted] (FISA Ct. 2013), http://www.dni.gov/files/documents/PrimaryOrder_Collection_215.pdf.http://www.dni.gov/files/documents/PrimaryOrder_Collection_215.pdf.

99. *See* Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001, Pub. L. No. 107-56, § 215, 115 Stat. 272, 287 [hereinafter PATRIOT Act] (arguably authorizing the collection and storage of bulk metadata); FISA Amendments Act of 2008, Pub. L. No. 110-261, § 702, 122 Stat. 2436, 2438

community a much larger haystack of information from which to attempt to glean details of emerging and ongoing terrorist threats.[100] This shift generated critiques from civil libertarians and lawmakers.[101] But until late 2013, critics were largely unable to secure significant victories in curtailing surveillance powers or even understanding the parameters of what was authorized under existing law.[102] The tenor of the public debate became more contentious in June 2013 when Edward Snowden began revealing classified documents detailing the scope of NSA surveillance on foreign and U.S. persons in order to prompt public scrutiny and debate over the programs. Snowden disclosed, among many other things, that the NSA was engaged in the practice of collecting and retaining the metadata of all U.S. telephone customers for five years, and had been running searches through that metadata when there was a "reasonable, articulable suspicion" that a particular telephone number was associated with potential terrorist activity.[103] Further disclosures indicated that additional surveillance targeted Muslim community leaders in the

---

(2008) (codified as amended at 50 U.S.C. § 1881a (2015) (authorizing the targeted collection of data, including content, from overseas targets). When various provisions of the Patriot Act were up for renewal in 2010, debates on the utility, invasiveness, and potential abuse of the surveillance provisions ended in congressional reauthorization of the Act without alternation. *See* David Kravets, *Lawmakers Punt Patriot Act to Obama*, WIRED (Feb. 26, 2010, 3:52 PM), http://www.wired.com/2010/02/lawmakers-renew-patriot-act/.

100. *See* Gil Press, *The Effectiveness of Small vs. Big Data Is Where the NSA Debate Should Start*, FORBES (June 12, 2013), http://www.forbes.com/sites/gilpress/2013/06/12/the-effectiveness-of-small-vs-big-data-is-where-the-nsa-debate-should-start (discussing need to understand whether a larger or smaller "haystack" of data better enables intelligence-gathering and analysis efforts).

101. *See, e.g.*, Felicia Sonmez, *Harry Reid, Rand Paul Spar over Patriot Act on Senate Floor*, WASH. POST (May 25, 2011), http://www.washingtonpost.com/blogs/2chambers/post/harry-reid-rand-paul-spar-over-patriot-act-on-senate-floor/2011/05/25/AGcgWRBH_blog.html (describing objections by Senators Rand Paul and Tom Udall to data-gathering provisions being debated for renewal as part of the Patriot Act).

102. *See, e.g.*, Clapper v. Amnesty Int'l, 133 S. Ct. 1138 (2013) (holding that plaintiffs alleging unconstitutional and illegal surveillance lacked standing to bring their complaint because they had no publicly available proof of their surveillance). Cases that challenge these surveillance programs on constitutional and statutory grounds are still being litigated.

103. *See* Glenn Greenwald, *NSA Collecting Phone Records of Millions of Verizon Customers Daily*, GUARDIAN (June 6, 2013 06.05 PM), http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order.

United States who had not engaged in any suspicious activity, other than the apparent red flag of being Muslim.[104]

The broad scope, lack of particularized suspicion, and lengthy duration of data retention raised substantive concerns.[105] From a transparency perspective, concerns arose on two fronts. First, the purported legitimacy of the program was based on the fact that its parameters and details had been approved in a nonpublic opinion by the Foreign Intelligence Surveillance Court, a nonadversarial body that operates largely in secret and has approved virtually every government request for surveillance authority that it has considered.[106] Second, the general structure and details of the program were hidden from most members of Congress and the public until the Snowden disclosures began. Together, these concerns raised the question of whether the NSA's metadata collection program was, in fact, based on secret laws and without any meaningful understanding of how the government was interpreting its surveillance authority.

One example of problematic interpretation stems from a Senate oversight hearing on March 12, 2013, in which Senator Ron Wyden specifically asked Director of National Intelligence James Clapper if the NSA was systematically collecting information on the communications of millions of Americans.[107] Clapper denied this, yet later disclosures confirmed that the scope of the NSA's data collection included metadata for telephonic communications, as well as content data for e-mails, texts, and other such writings.[108] After public discussion of the discrepancy in

104. *See* Glenn Greenwald & Murtaza Hussain, *Meet the Muslim-American Leaders the FBI and NSA Have Been Spying on*, INTERCEPT (July 9, 2014, 12:01 AM), https://theintercept.com/2014/07/09/under-surveillance/.

105. The U.S. intelligence community has engaged in numerous programs involving warrantless surveillance, and this analysis only considers the bulk metadata collection that was arguably authorized under Section 215 of the Patriot Act. Other warrantless surveillance—of non-U.S. persons or on non-U.S. territory—falls under the auspices of other authorities, such as Executive Order 12333 or Section 702 of the Foreign Intelligence Surveillance Act. The structural accountability problems raised here with regard to the NSA Metadata Program can be extrapolated to consider other domestic surveillance questions based on common legal and political frameworks.

106. The Foreign Intelligence Surveillance Court is discussed in detail in Chapter 3.

107. Glenn Kessler, James Clapper's 'Least Untruthful' Statement to the Senate, WASH. POST (June 12, 2013), http://www.washingtonpost.com/blogs/fact-checker/post/james-clappers-least-untruthful-statement-to-the-senate/2013/06/11/e50677a8-d2d8-11e2-a73e-826d299ff459_blog.html. Senator Wyden posed the following question: "[D]oes the NSA collect any type of data at all on millions or hundreds of millions of Americans?" Clapper responded, "No, sir." Id.

108. *See* Siobhan Gorman & Jennifer Valentino-DeVries, *New Details Show Broader NSA Surveillance Reach*, WALL ST. J. (Aug. 20, 2013, 11:31 PM), http://online.wsj.com/article/SB10001424127887324108204579022874091732470.html (describing how seventy-five percent of email traffic, including the content of emails, sent or received by United States persons is captured by various NSA programs).

his testimony, Clapper noted that he and the NSA used a 1982 Defense Department regulation to define the word "collect" to mean the point at which searches through the stored data provide results and those results are analyzed by a person.[109] Using this definition, Clapper was able to argue that "collection" does not occur at the point at which the data is gathered or even when algorithms are used to sort the data for relevance, even though a plain reading would suggest otherwise. In fact, common understanding suggests that "collection" occurred at any number of points earlier in the NSA's data gathering and sorting process, particularly since humans were actively querying the database of information.

Although Wyden and others tasked with oversight theoretically could have found the 1982 regulatory definition and used it to ask follow up questions of Clapper, it seems that if Wyden had used a synonym for "collect" that was not an obscurely defined term of art, such as "gather," or "intake and store," Clapper might not have been able to mislead Congress in his March 2013 testimony. In that sense, Clapper engaged in constructive secrecy: the legally operative meaning of "collection" was theoretically not a secret, but the administration did not volunteer the meaning that it was relying upon and the operative definition was not made clear to oversight bodies. Until subsequent disclosures helped clarify the dissonance between the publicly understood parameters of the NSA's metadata program and the legally operative parameters, the administration could retain secrecy around its policy while denying that it was secret at all.

In late 2013 and the years following, the Obama administration increased its public willingness to improve protections of privacy and civil liberties and improve transparency when those goals were compatible with intelligence gathering interests.[110] For example, in early 2016 the

---

109. *See* DEP'T OF DEF., PROCEDURES GOVERNING THE ACTIVITIES OF DOD INTELLIGENCE COMPONENTS THAT AFFECT UNITED STATES PERSONS, DoD 5240.1-R (1982). This regulation defines "collection" as follows: "Information shall be considered as 'collected' only when it has been received for use by an employee of a [Department of Defense] intelligence component in the course of his official duties . . . . Data acquired by electronic means is 'collected' only when it has been processed into intelligible form." *Id.* § C2.2.1, at 15.

110. *See* President Barack Obama, Remarks by the President at the United States Military Academy Commencement Ceremony (May 28, 2014, 10:22 AM), http://www.whitehouse.gov/the-press-office/2014/05/28/remarks-president-west-point-academy-commencement-ceremony ("Our intelligence community has done outstanding work, and we have to continue to protect sources and methods. But when we cannot explain our efforts clearly and publicly, we face terrorist propaganda and international suspicion, we erode legitimacy with our partners and our people, and we reduce accountability in our own government . . . . [W]e're putting in place new restrictions on how America collects and uses intelligence—because we will have fewer partners and be less effective if a perception takes hold that we're conducting surveillance against ordinary citizens."). In February 2015,

NSA's Civil Liberties and Privacy Office issued a newly mandated transparency report.[111] Among other things, this report clarified that newly imposed limitations on data gathering practices were being interpreted by the NSA and Congress in the same way, thus alleviating some concerns that the NSA was engaging in the type of constructive secrecy that had previously allowed misleading statements, like Clapper's, to be made to Congress.[112]

The primary message from the Obama administration from 2013 onward was that the Snowden disclosures were unnecessary, illegal, and counterproductive to both intelligence-gathering programs and national security.[113] Yet, no evidence suggests that any of the accountability measures championed by the administration and Congress would have existed or gained significant purchase but for the Snowden disclosures.[114] To the contrary, some within the NSA actively attempted to avoid oversight by the Department of Justice.[115] Other oversight mechanisms, such as the Office of the Inspector General for the NSA,[116] are well-suited

---

the Director of National Intelligence announced new limits to the scope of Section 215 surveillance and intelligence-gathering that largely reflected the type of limitations suggested by President Obama in 2014. *See* ODNI General Counsel Robert Litt's As Prepared Remarks on Signals Intelligence Reform at the Brookings Institute (Feb. 4, 2015), http://icontherecord.tumblr.com/post/110632851413/odni-general-counsel-robert-litts-as-prepared.

111. NSA CIVIL LIBERTIES AND PRIVACY OFFICE, TRANSPARENCY REPORT: THE USA FREEDOM ACT BUSINESS RECORDS FISA IMPLEMENTATION (2016), https://fas.org/irp/nsa/ufa-2016.pdf.

112. *See id.* at 4–7 (including definitions and the applications of the parameters of the USA Freedom Act).

113. *See, e.g.*, President Barack Obama, Remarks by the President on Review of Signals Intelligence (Jan. 17, 2014, 11:15 AM), http://www.whitehouse.gov/the-press-office/2014/01/17/remarks-president-review-signals-intelligence.

114. Snowden provided written testimony to the European Parliament stating that he had attempted to discuss his concerns with regard to various aspects of NSA surveillance with superiors within the NSA prior to his public disclosure, but that his efforts were either ignored or rebuffed. *See* Edward J. Snowden, *Answers to Written Questions from the European Parliament*, EUR. PARL. 1, 5 (March 7, 2014), http://www.europarl.europa.eu/document/activities/cont/201403/20140307ATT80674/20140307ATT80674EN.pdf.

115. *See* Barton Gellman, *NSA Broke Privacy Rules Thousands of Times per Year, Audit Finds*, WASH. POST (Jan. 8, 2007), http://www.washingtonpost.com/world/national-security/nsa-broke-privacy-rules-thousands-of-times-per-year-audit-finds/2013/08/15/3310e554-05ca-11e3-a07f-49ddc7417125_story.html (explaining how NSA operatives requesting permission to extend surveillance to a new target were instructed to limit the information disclosed to Justice Department "overseers").

116. Commentators have suggested that an independently appointed and overseen Inspector General for the NSA would provide a better avenue for accountability. *See* Britt Snider & Charles Battaglia, *National Security Agency Needs an Independent Inspector General*, WASH. POST (Sept. 26, 2013), https://www.washingtonpost.com/opinions/national-

to deal with allegations of statutory and policy compliance violations, but not with a large-scale systemic and philosophical complaint about privacy rights such as that of Snowden.[117] Other potential avenues for accountability, such as the Office of the Inspector General for the Defense Department, were rendered impotent by the lack of access to the relevant information.[118] The extreme secrecy that surrounded these surveillance programs, even within the Obama administration, suggests that many existing oversight mechanisms were, in the time before the Snowden disclosures, not effective and succeeded only in giving a veneer of accountability over a program that lacked it.

D. Contextualizing Private Interpetations

The fact that so many accountability measures were theoretically in place but easily avoidable until the fallout of the Snowden disclosures goes to the heart of what concerned the CJEU in *Schrems* and was part of the reason that the CJEU came down so hard on the old Safe Harbor agreement. It was not that Schrems or the CJEU could point to a series of specific violations of the Safe Harbor agreement that actually undercut the fundamental privacy rights of an EU citizen. Instead, the CJEU's decision was founded on the understanding that, as of 2013, the United States was likely maneuvering around the privacy protections and oversight mandated in the Safe Harbor agreement by not abiding by public understandings of those protections and instead relying on its privately held legal interpretations of its obligations.

In each of the contexts discussed in this Part, the Bush and Obama administrations secretly reinterpreted and, therefore, subverted commonly understood, ordinary definitions of terms in order to conduct a national security related program in a way that arguably violated

---

security-agency-needs-an-independent-inspector-general/2013/09/26/ae37d7fc-25f4-11e3-ad0d-b7c8d2a594b9_story.html?utm_term=.2d5870d0aad1.

117. *See* Interviews with NSA officials (various dates, on file with author) (discussing the fact that the job of the NSA Inspector General would not have been to discuss the "philosophical differences" that Snowden had with the NSA's programmatic and policy choices). However, the Inspector General for the NSA has publicly stated that if Snowden had complained to the Inspector General, his allegations would have been investigated thoroughly. Darren Samuelsohn, *NSA Watchdog Talks Snowden*, POLITICO (Feb. 25, 2014, 6:37 PM), http://politi.co/NvvjAE. But it seems quite likely that the extent of the Inspector General's inquiry would have been to examine the program against the existing statutory authority and find that the bulk data collection was statutorily authorized.

118. *See* Spencer Ackerman, *Pentagon Watchdog 'Not Aware' of NSA Bulk Phone Data Collection*, GUARDIAN (Mar. 18, 2014, 3:36 PM), http://www.theguardian.com/world/2014/mar/18/pentagon-watchdog-nsa-bulk-phone-collection (saying that the Defense Department Deputy Inspector General was unaware of the bulk data collection until learning about it through the June 2013 Snowden leaks).

international and/or domestic law. Each administration was somewhat successful in doing so because the domestic control mechanisms in place—internal review within the Executive Branch, Congress, Article III courts, and the Foreign Intelligence Surveillance Court—failed to demand transparency and accountability in how the government was interpreting and implementing its obligations under various laws and treaties.

The Privacy Shield emerges in a different context: the control mechanisms described in the Privacy Shield, such as the ombudsperson, are domestic. However, because the Privacy Shield is a transnational agreement, it can be held to account in a more rigorous manner because it had to be validated by EU regulators, will be reviewed annually by U.S. and EU regulators, and can be invalidated by courts outside of the United States. EU regulators do not have to wait for the CJEU to consider whether the Privacy Shield's protections for the privacy rights of EU citizens are adequate. In the interim, EU regulators involved in overseeing the implementation of the Privacy Shield can take an active role in making sure that the United States is not using its own private dictionary in interpreting its obligations under the Privacy Shield.

III. POTENTIAL CONSTRAINTS AGAINST CONSTRUCTIVE SECRECY

It is possible that the Trump administration will engage in constructive secrecy with the Privacy Shield along the lines of what the Bush and Obama administrations did in the contexts of torture, targeted killings, and surveillance. As of this writing, it is unclear what kind of transparency and rights-protective commitments the Trump administration will make and whether it will abide by those commitments once they are made. If the Trump administration does engage in interpretation that subverts the Privacy Shield, then the legally operative interpretation under which the administration acts would likely be kept secret from the public, even as public assurances suggest compliance with the constraints that most people, including EU regulators, believe is part of the agreement.

The Privacy Shield may be particularly vulnerable to this problem for several reasons. First, the same expansive carve-out regarding national security that existed in the Safe Harbor agreement is also included in the Privacy Shield.[119] Second, the 2016 commitments by the Office of the Director of National Intelligence include a description of the six types of data collection that the United States will be entitled to collect in the name of national security under the Privacy Shield: detecting and

119. *See Privacy Shield*, *supra* note 7, § I.5.

countering certain activities of foreign powers, counterterrorism, counter-proliferation, cybersecurity, detecting and countering threats to the United States or allied armed forces, and combatting transnational criminal threat, including sanctions evasion.[120] Based on current U.S. definitions of terrorism and security,[121] these categories are broad enough to encompass tremendous swaths of data in a manner that may violate EU privacy rights.[122] Third, the agency letters affirming that the U.S. interpretation of the parameters of the Privacy Shield adheres to the privacy-oriented aspirations of the framework are not legal commitments; they are simply a statement of how an agency plans to act.[123]

As discussed in Part II, reliance on the good faith interpretations of the U.S. government regarding national security matters sometimes resulted in dissonance between the operative legal definition and the public commitment made by the Bush and Obama administrations. Under the Trump administration, it is wholly unclear what those public commitments would be or whether they would be interpreted consistently for internal purposes. If such interpretive dissonance were to occur, the privacy rights that the CJEU looked to preserve in *Schrems* could be violated regardless of the external commitments that the United States has made in the Privacy Shield or accompanying letters.

These interpretative concerns, among others, motivated the September 2016 suit filed by the privacy activist group, Digital Rights Ireland, seeking annulment of the Privacy Shield by the CJEU.[124] In its complaint, the plaintiff alleges that the Privacy Shield does not comport

120. *See* Letter from Robert S. Litt, *supra* note 33, at 4.

121. *See generally* Sudha Setty, *What's in a Name? How Nations Define Terrorism Ten Years After 9/11*, 33 U. PA. J. INT'L L. 1 (2011) (addressing the extreme broad definitions of terrorism in the United States and elsewhere).

122. *See* Eur. Comm'n Press Release, Article 29 Working Party Statement on the Decision of the European Commission on the EU-U.S. Privacy Shield (July 26, 2016), http://ec.europa.eu/justice/data-protection/article-29/press-material/press-release/art29_press_material/2016/20160726_wp29_wp_statement_eu_us_privacy_shield_en.pdf (expressing concerns that the Privacy Shield would technically allow for mass collection of signals intelligence, as was authorized when the Safe Harbor was in effect) [hereinafter Article 29 Working Party Statement]; Katie Bo Williams, *US, EU Face Blowback on Data Deal*, HILL (Feb. 29, 2016, 8:06 PM), http://thehill.com/policy/cybersecurity/271233-us-eu-face-blowback-on-data-deal (discussing concerns that the Privacy Shield likely would not withstand scrutiny by the CJEU).

123. *See* Peter Teffer, *EU and US Agree Data 'Privacy Shield'*, EUOBSERVER (Feb. 2, 2016, 7:21 PM), https://euobserver.com/justice/132109 (quoting Sophie in 't Veld, a Liberal Member of the European Parliament, as expressing concern that "[t]he assurances seem to rely exclusively on political commitment, instead of legal acts. So any change in the political constellation in the US may undo the whole thing").

124. *See* Complaint, Case T-670/16, Digital Rights Ireland Ltd. v. Comm'n, 2016 O.J. (C 410) 26 (filed Sept. 16, 2016) [hereinafter Digital Rights Complaint].

with the requirements of Article 25 of the Data Protection Directive, which allows for commercial data transfers so long as there is "an adequate level of protection . . . by reason of its domestic law or of the international commitments it has entered into . . . for the protection of the private lives and basic freedoms and rights of individuals."[125] The plaintiff argues that U.S. domestic law does not adequately protect the privacy rights of Europeans and that the Privacy Shield does not rise to the level of an "international commitment" such that the standard articulated in Article 25 would be satisfied.[126]

Absent another Snowden-like leak, litigation as in *Schrems*, or the CJEU getting involved again as requested in the new Digital Rights Ireland case, the EU regulators tasked with reviewing the Privacy Shield should consider how to constrain the U.S. executive branch from relying on secret interpretations that undermine the objective meaning of the agreement. One viable option would be to use the annual review in 2017 to formalize the norms and methodology used to interpret the Privacy Shield, bringing it to the level of an "international commitment" under the standard of Article 25 of the Data Protection Directive, instead of simply trusting the U.S. government to interpret the limitations of the Privacy Shield in a manner that comports with EU privacy standards. Interpretive norms coming out of international law, international guidance, and other transnational commitments offer useful guidance.

The Vienna Convention on the Law of Treaties[127] offers a straightforward framework for interpreting treaty language, emphasizing in Article 31 that "a treaty shall be interpreted in good faith in accordance with the ordinary meaning to be given to the terms of the treaty in their context and in the light of its object and purpose."[128] Article 31 also affirms that interpretation of a treaty should take into account its context, purpose, supplemental documentation, subsequent agreements regarding interpretation, subsequent practices regarding interpretation, and any relevant rules of applicable international law.[129] In Article 32,

125. *See* Directive 95/46/EC, *supra* note 13, art. 25(6).

126. *See* Digital Rights Complaint, *supra* note 124, at 27 ("Third plea in law, alleging that the 'privacy principles' and/or the official (US) 'representations and commitments' . . . do not constitute 'international commitments' within the meaning of Article 25(6) of Directive 95/46.").

127. Vienna Convention on the Law of Treaties, May 23, 1969, 1155 U.N.T.S. 331 [hereinafter "Vienna Convention"].

128. *Id.* art. 31.

129. *See id.*

the Vienna Convention goes further to offer additional guidance on means of interpretation, noting that:

> Recourse may be had to supplementary means of interpretation, including the preparatory work of the treaty and the circumstances of its conclusion, in order to confirm the meaning resulting from the application of article 31, or to determine the meaning when the interpretation according to article 31 . . . leaves the meaning ambiguous or obscure; or . . . leads to a result which is manifestly absurd or unreasonable.[130]

Together, the language in these two Articles would go some distance in constraining the executive branch from creating secret and legally operative definitions that vary significantly from public commitments based on national security related concerns. If added to the language of the Privacy Shield, they may even serve to signal to the CJEU and other constituencies that the United States is heightening its commitment to the protections guaranteed under the Privacy Shield, and that those commitments are not subject to the changing whims of an agency, administration, or the intelligence community.

The commitments of Articles 31 and 32 cannot simply be inferred; indeed, they would need to be adopted explicitly in the annual review of the Privacy Shield, or through another amendment mechanism. The Vienna Convention is not legally binding on the parties to the Privacy Shield for a number of reasons. First, the Privacy Shield is not a treaty, but is a framework applying to private and government actors in two jurisdictions (the United States and the European Union) that are subject to regulatory and judicial scrutiny.[131] Second, the United States is a signatory to the Vienna Convention but has not ratified it, although the U.S. State Department has noted that it accepts many provisions of the Vienna Conventions as constituting customary international law on the

130. *Id.* art. 32.

131. *See* U.S. DEP'T OF COMMERCE, THE EU-U.S. PRIVACY SHIELD FRAMEWORK FAQS (2016), https://www.commerce.gov/sites/commerce.gov/files/media/files/2016/faqs-eu-us_privacy_shield_7-16_sc_cmts.pdf (clarifying the nature of the Privacy Shield as a "framework" as opposed to "treaty" or other legal instrument).

law of treaties.[132] Third, the Vienna Convention has a relatively narrow scope and only applies to treaties between states.[133]

Yet the interpretive standards in the Vienna Convention could provide an important touchstone to help formalize and make uniform the type of interpretation that the parties to the Privacy Shield purport to want.[134] In statements by U.S. and EU negotiators during the development of the Privacy Shield, as well as in the letters provided by U.S. regulators when the Privacy Shield was made public, the United States promised to act in good faith to uphold privacy standards that would pass the scrutiny of the CJEU. If that is truly the case, then explicitly tying those commitments to the Vienna Convention's interpretive standard should be uncontroversial.

Explicit incorporation of the interpretive standards of the Vienna Convention would be particularly apt because the same standards articulated in the Vienna Convention have long been considered useful and necessary in a number of public international and transnational contexts, private transnational contexts, the canons of U.S. statutory interpretation, and the laws and guidance surrounding U.S. contract interpretation. The International Law Commission has looked to the Vienna Convention in considering how to manage the expansion and fragmentation of international law,[135] and the American Law Institute has articulated similar interpretive standards for international agreements.[136] Other agreements, like the widely used and relied on Covenant for the International Sale of Goods (CISG),[137] are often interpreted using analogous principles that rely upon ordinary and

---

132. *See Vienna Convention on the Law of Treaties*, U.S. DEP'T OF STATE, http://www.state.gov/s/l/treaty/faqs/70139.htm (last visited Mar. 4, 2017).

133. *See* Vienna Convention, *supra* note 127, art. 1 ("The present Convention applies to treaties between States.").

134. *See* ANTHONY AUST, MODERN TREATY LAW AND PRACTICE 207–17 (3d ed. 2013) (explaining the utility of Articles 31 and 32 of the Vienna Convention).

135. *E.g.*, Int'l Law Comm'n, *Fragmentation of International Law: Difficulties Arising from the Diversification and Expansion of International Law*, U.N. Doc. A/CN.4/L.682 (2006). Like the Vienna Convention, the Fragmentation Report notes that treaties are not to be applied and interpreted in a vacuum. *Id.* ¶ 120. The Report notes that "all international law exists in a systemic relationship with other law" and, therefore, no treaty application can occur without placing the relevant instrument in its contextual environment, which suggests that ordinary meanings within the negotiated context must apply when interpreting the obligations under an agreement. *Id.* ¶ 423.

136. RESTATEMENT (THIRD) OF FOREIGN RELATIONS LAW OF THE UNITED STATES § 325(1) (AM. LAW INST. 1987) ("An international agreement is to be interpreted in good faith in accordance with the ordinary meaning to be given to its terms in their context and in the light of its object and purpose.").

137. U.N. Conference on Contracts for the International Sale of Goods, *Official Records: Documents of the Conference and Summary Records of the Plenary Meetings and of the Meetings of the Main Committees*, at 178–90, U.N. Doc. A/CONF 97/19 (Apr. 11, 1980).

common understandings of terms.[138] Such an interpretive methodology is also common in U.S. domestic contract law[139] and judicial interpretation of statutes.[140] Therefore, using the interpretive standards articulated in Articles 31 and 32 of the Vienna Convention should not only be uncontroversial as a matter of transnational norm creation, but also as a matter of substance because the norm in domestic law is to give ordinary meanings to words in contracts and statutes.

This is not to suggest that such explicit incorporation of interpretive norms would resolve all of the current concerns involving the Privacy Shield. Indeed, the complaint in the new *Digital Rights Ireland* case alleges many substantive and procedural failures in the Privacy Shield, many of which echo the concerns voiced by the Article 29 Working Party of data protection commissioners in EU member states reviewing the Privacy Shield.[141] Yet, dealing with the problem of potential interpretive dissonance in a manner that follows international, transnational, and domestic precedent provides a simple path to improving the Privacy Shield and, perhaps, resolving one of the issues that privacy rights groups and the CJEU have justifiably raised in the past.

CONCLUSION

One of the key problems of constructive secrecy is the creation of public commitments that appear to adequately hold the U.S. government to account, but the reality is that those commitments present only a

138. *See, e.g.*, Frank Diedrich, *Maintaining Uniformity in International Uniform Law via Autonomous Interpretation: Software Contracts and the CISG*, 8 PACE INT'L L. REV. 303, 317–18 (1996) (noting that the Vienna Convention's interpretive methodology and reliance on common and ordinary meanings of terms is used to resolve disputes in textual meaning).

139. *See, e.g.*, RESTATEMENT (SECOND) OF CONTRACTS § 203(a) (AM. LAW INST. 1981) ("[A]n interpretation which gives a reasonable, lawful, and effective meaning to all terms is preferred to an interpretation which leaves a part unreasonable, unlawful, or of no effect . . . ."); U.C.C. § 1-303 (AM. LAW INST. & UNIF. LAW COMM'N 2001) ("[T]he express terms of an agreement and any applicable course of performance, course of dealing, or usage of trade must be construed whenever reasonable as consistent with each other.").

140. *See* Connecticut Nat'l Bank v. Germain, 503 U.S. 249, 253–54 (1992) ("[C]anons of construction are no more than rules of thumb that help courts determine the meaning of legislation, and in interpreting a statute a court should always turn first to one, cardinal canon before all others . . . . [C]ourts must presume that a legislature says in a statute what it means and means in a statute what it says there. When the words of a statute are unambiguous, then, this first canon is also the last: 'judicial inquiry is complete.'") (citations omitted); Caminetti v. United States, 242 U.S. 470, 471 (1917) (establishing the plain meaning rule of statutory construction).

141. *See* Article 29 Working Party Statement, *supra* note 122.

façade of accountability because the legally operative, private commitments made by the government are substantially different. These legal "grey holes" provide a dangerous false comfort regarding government accountability, transparency, and the maintenance of the rule of law.[142] Time and again in the last fifteen years, the U.S. government has invoked national security concerns to provide such false comfort in reassuring the public that it is upholding its domestic and international legal commitments, only for subsequent disclosures to make clear that those reassurances were either definitely or arguably ill-founded. The concerns expressed by the CJEU in *Schrems* reflect its discomfort with the U.S. reliance on constructive secrecy and the false sense of comfort it provides. The Privacy Shield attempts to remedy that situation by increasing oversight of U.S. companies conducting transnational data transfers and by seeking overt commitments from U.S. government agencies that the privacy protections for EU citizens will rise to a level that would likely survive subsequent scrutiny by the CJEU.

Perhaps the CJEU will uphold the Privacy Shield as satisfying the Data Protection Directive, but the September 2016 suit brought by Digital Rights Ireland highlights the doubts as to whether the language in the Privacy Shield adequately constrains the U.S. government. Further, the CJEU continues to make it clear in its jurisprudence that it will enforce the privacy rights of EU citizens even in the face of strong arguments about the need for potentially intrusive data collection in the name of national security.[143]

The CJEU may also be skeptical of the efficacy of the Privacy Shield based on a lack of transparency and concerns as to how the Trump administration will interpret its privacy commitments under the agreement. A January 25, 2017 Executive Order requires federal agencies to limit privacy protections for non-U.S. citizens,[144] an action that immediately led European lawmakers to express uncertainty regarding the U.S. commitment to the Privacy Shield.[145] Other comments

---

142. *See* David Dyzenhaus, Schmitt v. Dicey: *Are States of Emergency Inside or Outside the Legal Order?*, 27 CARDOZO L. REV. 2005, 2026 (2006).

143. *See Tele2*, *supra* note 12, ¶¶ 72–73 (reasoning that invocations of national security did not justify the type of bulk data collection at issue in the case).

144. President Donald J. Trump, Executive Order: Enhancing Public Safety in the Interior of the United States (Jan. 25, 2017), https://www.whitehouse.gov/the-press-office/2017/01/25/presidential-executive-order-enhancing-public-safety-interior-united ("Agencies shall, to the extent consistent with applicable law, ensure that their privacy policies exclude persons who are not United States citizens or lawful permanent residents from the protections of the Privacy Act regarding personally identifiable information.").

145. *E.g.*, Jeff John Roberts, *U.S. Tech Industry Wants Trump to Calm EU Data Fears*, FORTUNE (Feb. 2, 2017) http://fortune.com/2017/02/02/trump-privacy-shield/ (describing

made by members of the Trump administration calling for a reduction of privacy protections in the name of national security have further increased skepticism as to whether the Privacy Shield will be enforced as written.[146] In fact, in early April 2017, the European Parliament passed a resolution asking the European Commission to undertake its upcoming 2017 review of the Privacy Shield with an eye toward better understanding how the United States has thus far interpreted its obligations under the agreement.[147]

None of these developments will reassure the CJEU that the Privacy Shield is an adequate framework to protect the privacy rights of EU citizens. The precarity of the Privacy Shield undermines confidence in both the enforcement of fundamental privacy protections and the viability of businesses that depend on data transfers. This makes it all the more important for the United States to make the interpretative methodology of the Privacy Shield a matter of public record, an international commitment, and a subject of external accountability. Doing so would not ameliorate all of the concerns surrounding the Privacy Shield, but it would strengthen the U.S. government's argument that it ought to be trusted in this context.

---

concerns of a former Federal Trade Commissioner that the executive order could make European lawmakers skittish about the U.S. application of the Privacy Shield); Natasha Lomas, *Trump Order Strips Privacy Rights from Non-U.S. Citizens, Could Nix EU-US Data Flows*, TECH CRUCNH (Jan. 26, 2017), https://techcrunch.com/2017/01/26/trump-order-strips-privacy-rights-from-non-u-s-citizens-could-nix-eu-us-data-flows/ (noting concerns of a Member of the European Parliament as to the uncertain enforcement of the Privacy Shield in light of the executive order).

146. *See* Melanie Teplinsky, *Opinion: Will Trump Sink Privacy Shield?*, CHRISTIAN SCI. MONITOR (Feb. 24, 2017), http://www.csmonitor.com/World/Passcode/Passcode-Voices/2017/0224/Opinion-Will-Trump-sink-Privacy-Shield.

147. *See* Catherine Stupp, *MEPs Want Commission to Toughen up Privacy Shield Under Trump*, EURACTIV (Apr. 7, 2017), http://www.euractiv.com/section/data-protection/news/meps-want-commission-to-toughen-up-privacy-shield-under-trump/.