MEMORANDUM

TO: Helen Dixon, Data Protection Commissioner

FROM: Morrison & Foerster LLP (Andrew B. Serwin)

DATE: November 30, 2016

RE: Review of Certain Causes of Action—Supplemental Memorandum

I. Introduction

This memorandum serves as a supplement to Morrison & Foerster's May 24, 2016 memorandum ("May 24, 2016 Memo"). The May 24, 2016 Memo and this supplement provide a non-exclusive overview of private remedies available to EU citizens, under federal law in the United States, against certain entities and individuals for alleged violations of data privacy arising from the gathering of personal information in the context of national security.[1,2]

This supplemental memorandum does not opine on the effectiveness of these remedies for purposes of Article 47 of the Charter of Fundamental Rights of the European Union, or on whether such causes of action would be appropriate in any particular circumstance. Where relevant, however, it identifies those factors that may be barriers to suit or otherwise limit recovery.

II. *Schuchardt v. President of the United States*

After the May 24, 2016 Memo was completed, a federal circuit court issued an opinion in *Schuchardt v. President of the United States* involving a constitutional challenge to an electronic surveillance program operated by the National Security Agency ("NSA").[3] The

[1] The May 24, 2016 Memo and this supplemental memorandum analyze only remedies under federal law, and do not discuss state law or regulatory provisions. Although application of state law is possible, it is unlikely to apply in a case brought by a foreign national for the alleged violations of data privacy analyzed by these memoranda. The doctrine of federal preemption originates from the Supremacy Clause of the U.S. Constitution. This doctrine provides that when state law conflicts with federal law, the state law is preempted and federal law applies. Additionally, the "dormant commerce clause" imposes an implicit limitation on the authority of states to enact laws affecting interstate commerce. 8 Witkin, *Summary of California Law* § 1300, p. 1000 (10th ed. 2005).

[2] In the preparation of the May 24, 2016 Memo and this supplemental memorandum, regard has been had to the assumed facts adopted by the Court of Justice of the European Union for the purpose of its analysis in its judgment in *Schrems v. Data Protection Commission*, Case No. C-362/14, 6 October 2015. These memoranda do not, however, review the facts of the *Schrems* case or make any factual finding or legal conclusion with respect to the *Schrems* case.

[3] *Schuchardt v. President of the United States,* 839 F.3d 336 (3d Cir. 2016).

case analyzes Article III standing in the context of a plaintiff who alleged that the United States Government was "intercepting, monitoring and storing the content of *all or substantially all* of the emails sent by American citizens," including presumably the plaintiff's.[4] The allegations made by the plaintiff were based in no small part upon the allegations made by Edward Snowden, which built upon prior public disclosures regarding alleged government monitoring.[5] In the context of a motion to dismiss, the United States Government argued that the plaintiff's allegation was insufficient to establish a claim.

For the purposes of a motion to dismiss, the court held that the plaintiff had adequately pleaded standing, but stated that its holding was narrow and the court explicitly stated that this did not mean that the plaintiff actually *had* standing to sue.[6] The court also noted that rulings on this question in other circuits varied depending on several factors, including the procedural posture of the case.[7] In other words, as noted in the cases cited in footnote 7 of this memorandum, the burden imposed upon the plaintiff to establish Article III standing varies depending on when in the case, and how, the defendant challenges standing, which is why the court noted that its holding was narrow. Thus, although this case may appear, at first blush, to indicate a lower threshold for pleading Article III standing in this circuit, it does not change the fact-intensive and circuit-specific nature of these determinations, and this does not alter the conclusion that a plaintiff must still meet his or her burden to show sufficient harm under Article III.

The plaintiff in *Schuchardt* also suggested that he was entitled to jurisdictional discovery, which is used to uncover jurisdictional facts.[8] The court, however, cautioned that "[j]urisdictional discovery is not a license for the parties to engage in a 'fishing expedition,' and that fact is particularly true in a case like this one, which involves potential issues of national security."[9] Notably, the plaintiff in *Schuchardt* based his claims on excerpts of classified materials that were the focus of public reports, some of the reports themselves, and affidavits filed in other cases.[10] These reports appeared to be important to the court analysis, and without such public disclosures regarding alleged surveillance, it could be more difficult for a plaintiff to bring suit.

---

[4] *Id.* at 341 (emphasis in original).
[5] *See id.* at 339.
[6] *Id.* at 353 ("Our decision today is narrow: we hold only that the Schuchardt's second amended complaint pleaded his standing to sue for a violation of his Fourth Amendment right to be free from unreasonable searches and seizures. This does not mean that he *has* standing to sue, as the Government remains free upon remand to make a factual jurisdictional challenge to Schuchardt's pleading.") (emphasis in original).
[7] *Id.* at 351 (comparing *ACLU v. Clapper*, 785 F.3d 787, 800 (2d Cir. 2015) (holding that plaintiffs had standing on motion to dismiss) and *Jewel v. NSA*, 673 F.3d 902, 906-07 (9th Cir. 2011) (same), with *Obama v. Klayman*, 800 F.3d 559, 568 (D.C. Cir. 2015) (opinion of Williams, J.) (finding that plaintiffs lacked standing to pursue preliminary injunction because there was no "substantial likelihood" that they could establish injury-in-fact) and *ACLU v. NSA*, 493 F.3d 644, 650-51, 667-70 (6th Cir. 2007) (finding that plaintiffs failed to establish injury-in-fact on summary judgment)).
[8] *Schuchardt*, 839 F.3d at 353-54.
[9] *Id.*
[10] *Id.* at 341.

The discussion of *Schuchardt* illustrates a broader point regarding Professor Vladeck's views of Article III and my views in the May 24, 2016 Memo. Professor Vladeck and I broadly agree on Article III, and to the extent there are differences in our views, they are differences that largely result from a difference in emphasis in which cases one relies upon, and what the procedural posture is of those cases (given the sliding scale of the burden on plaintiffs noted above). In discussing Article III standing, Professor Vladeck acknowledges *Clapper v. Amnesty International, USA*, in which the U.S. Supreme Court found that the plaintiffs lacked standing to challenge the constitutionality of FISA. He also expresses his personal concerns regarding this decision.

Both the May 24, 2016 Memo and this supplemental memorandum analyze *Clapper* and Article III standing in light of the recent Supreme Court decision in *Spokeo, Inc. v. Robins*, a case finding that a plaintiff in a case alleging a statutory violation of the Fair Credit Reporting Act could not establish standing, which is consistent with a narrower reading of *Clapper*.[11] It will remain to be seen what bearing *Spokeo*, which is not a national security case, has in the national security context on the Article III analysis.

In addition to the standing requirement, a plaintiff would have to consider the obligation to satisfy Federal Rule of Civil Procedure 11. Professor Vladeck's affidavit at page 29, footnote 28, asserts that the May 24, 2016 Memo conflates two distinct ideas—that Rule 11 "requires a good faith basis for the claims alleged in a proceeding," and that the fact of an EU citizen's surveillance "would likely be classified and difficult to prove." I respectfully submit that Professor Vladeck has misinterpreted the argument. The May 24, 2016 Memo simply notes that, particularly in a case where there has been no public disclosure regarding the alleged surveillance, it could be difficult for a plaintiff to argue that a good faith basis existed for their claim. The memo concludes: "It remains to be seen how the Rule 11 requirements in conjunction with the Judicial Redress Act will be implemented . . . .", and this remains all the more true in light of *Spokeo*.

The district court in *Schuchardt* essentially noted this issue when it assessed Article III standing: "On the other hand, courts have refused to find standing based on naked averments that an individual's communications must have been seized because the government operates a data collection program and the individual utilized the service of a large telecommunications company."[12] Simply put, if a case is simply based upon "naked averments," particularly where there is no public disclosure of a future data collection program, the pre-filing Rule 11 burdens must at least be considered before the case is filed.

III. Administrative Procedure Act ("APA")

Professor Vladeck asserts in his affidavit that the May 24, 2016 Memo should have addressed a claim under Section 702 of the Administrative Procedure Act. [13] The APA has

[11] *Spokeo, Inv. v. Robins*, 136 S. Ct. 1540 (2016).
[12] *Schuchardt v. Obama*, No. 14-705, 2015 WL 5732117, at *6 (W.D. Pa. Sept. 30, 2015).
[13] *See* Affidavit of Stephen I. Vladeck ¶ 81. The affidavit of Peter Swire does not appear to discuss Section 702 of the APA as a potential civil remedies against the United States Government.

been used in certain cases, notably *ACLU v. Clapper*, and that case is important to consider as an illustration of the APA Section 702 claim.

It is first important to note that remedies under APA Section 702 exist only for "[a]gency action made reviewable by statute and final agency action for which there is no other adequate remedy in a court . . . ."[14] The APA was not "designed to expand the jurisdictional foundations of the federal courts. Rather, [it] merely provide[s] additional remedies and procedures where jurisdiction has already been conferred by statute."[15] Where other statutes provide adequate remedies, the APA is unavailable.[16] The alternate remedy "need not provide relief identical to relief under the APA, so long as it offers relief of the 'same genre.'"[17]

While the APA Section 702 claim has been used in cases where individuals directly seek relief, it is a claim that has faced some mixed results for plaintiffs in the national security context. As discussed below, courts have found that they are precluded from reviewing at least some claims involving intelligence gathering practices by the United States Government. Furthermore, circuit courts have had mixed views on whether a plaintiff in the national security context can establish that monitoring is "final agency action" under the APA, which in one case precluded relief against the United States government for allegedly intercepting oversees communications.[18]

The case cited by Professor Vladeck, *ACLU v. Clapper*, presented a unique fact pattern in which the ACLU and other non-profit civil rights organizations challenged a telephone metadata program that was being conducted pursuant to 50 U.S.C. § 1861.[19] Section 1861

---

[14] 5 U.S.C. § 704. Indeed, one court referred to a claim brought pursuant to the APA as an "umbrella claim" where the plaintiff also brought causes of action under three surveillance statutes—ECPA, FISA, and SCA. *See Jewel v. Nat'l Sec. Agency*, 673 F.3d 902, 908 (9th Cir. 2011).

[15] *First Nat'l Bank of Scotia v. United States*, 530 F. Supp. 162, 168 n.5 (D.D.C. 1982).

[16] *See, e.g., Turner v. Sec'y of U.S. Dept. of Housing & Urban Dev.*, 449 F.3d 536 (3d Cir. 2006) (plaintiff was precluded from bringing a cause of action under the APA because there were other adequate remedies available); *Town of Sanford v. United States*, 140 F.3d 20, 23 (1st Cir. 1998) ("A legal remedy is not inadequate for purposes of the APA because it is procedurally inconvenient for a given plaintiff, or because plaintiffs have inadvertently deprived themselves of an opportunity to pursue that remedy"). Courts have dismissed APA claims brought against the U.S. Government for failure to produce documents in response to FOIA requests, concluding that FOIA provides an adequate remedy. *See Elec. Privacy Info. Ctr. v. Nat'l Sec. Agency*, 795 F. Supp. 2d 85, 94-96 (D.D.C. 2011) (dismissing APA claim where FOIA provided an adequate alternative remedy for the relief sought); *Manna v. U.S. Dep't of Justice*, No. 15-794 (BAH), 2016 WL 4921394, at *4 (D.D.C. Sept. 15, 2016) (same).

[17] *Garcia v. Vilsack*, 563 F.3d 519, 522 (D.C. Cir. 2009) (citation omitted). As noted in the May 24, 2016 Memo, as well as this supplemental memorandum, I have not opined on the effectiveness of these remedies for purposes of Article 47 of the Charter of Fundamental Rights of the European Union, or on whether such causes of action would be appropriate in any particular circumstance, but I would note that courts in the United States might have to engage in this analysis now if an APA claim is brought in these circumstances.

[18] *Compare ACLU v. Nat'l Sec. Agency*, 493 F.3d 644, 677-79 (6th Cir. 2007) (holding that plaintiffs had not alleged the necessary "agency action" in claiming that NSA intercepted overseas communications and failed to comply with FISA's warrant requirements and minimization procedures) *with ACLU v. Clapper*, 785 F.3d 787, 810 (2d Cir. 2015) (holding that plaintiffs challenging NSA's telephone metadata program had a right of action under the APA).

[19] *ACLU v. Clapper*, 785 F.3d 787 (2d Cir. 2015).

"allows the Director of the FBI or his designee to 'make an application for an order requiring the production of any tangible things . . . for an investigation to obtain foreign intelligence information not concerning a United States person or to protect against international terrorism or clandestine intelligence activities.'"[20] The plaintiffs only became aware of the government order in this case when a newspaper published a leaked government order directing the production of appellant's call records.[21]

The court considered whether the plaintiffs were precluded from bringing suit to challenge the telephone metadata program via the APA.[22] Although the APA establishes a right of judicial review of administrative action, it does not apply where statutes preclude judicial review.[23] The court noted that 18 U.S.C. § 2712, the first cause of action I examine in the May 24, 2016 Memo, explicitly withdrew the right to sue under the APA for certain government actions involving surveillance.[24] Because the specific cause of action alleged by the plaintiffs in *Clapper* was not mentioned in Section 2712, and because the legislative history did not explicitly withdraw the right to sue the United States Government under this section, the court found that the plaintiffs had a right of action under the APA. Highlighting the unique circumstances of this case, the court further stated that in enacting Section 1861, "Congress assumed, in light of the expectation of secrecy, that persons whose information was targeted by a § 215 order would rarely ever know of such orders, and therefore that judicial review at the behest of such persons was a non-issue."[25] Nonetheless, under the circumstances of this case where the Section 1861 order was leaked to the public, judicial review came into question. The court vacated the lower court's judgment dismissing the complaint, but declined to conclude that a preliminary injunction was required.[26]

In contrast, at least one other court considering this same issue found that it lacked jurisdiction to hear plaintiffs' APA claim challenging the Section 1861 order. The court there concluded that Congress *did* intend to preclude APA claims in these circumstances.[27] In holding that judicial review was precluded, the court stated that Congress had "created a closed system of judicial review of the government's domestic foreign intelligence-gathering" under the FISA provisions in question, and that this system "include[d] no role for third parties."[28]

---

[20] *Id.* at 795 (quoting 50 U.S.C. § 1861(a)(1)).
[21] *Id.*
[22] *Id.* at 803-10.
[23] *Id.* at 803.
[24] *Id.* at 809-10. ("Section 2712, moreover, *explicitly* withdraws the right to challenge the specific government actions taken under specific authorization, in connection with *extending* an explicit cause of action for monetary damages in connection with such actions. . . . § 2712 manifestly does not create a cause of action for damages for violations of § 215, as it does with respect to those statutes of which it does preclude review under the APA.") (emphasis in original).
[25] *Id.* at 810.
[26] *Id.* at 826.
[27] *See Klayman v. Obama*, 957 F. Supp. 2d 1, 21 (D.D.C. 2013), *remanded on other grounds by Obama v. Klayman*, 800 F.3d 559 (D.C. Cir. 2015).
[28] *Id.* ("Stated simply, Congress created a closed system of judicial review of the government's domestic foreign intelligence-gathering, generally, 50 U.S.C. § 1803, and of Section 1861 production orders, specifically,

As demonstrated by the varying opinions issued by United States courts, the APA Section 702 claim faces several challenges beyond the Article III challenges that resulted in the dismissal of the complaint in *Clapper v. Amnesty International, USA.* Moreover, it is important to note that the cases permitting APA claims under Section 702 in these circumstances *predated* the Judicial Redress Act ("JRA").[29] As noted in the May 24, 2016 Memo, the JRA extends certain remedies under the Privacy Act to EU citizens, and these remedies were not available for EU citizens at the time of *Clapper*, and the other published APA Section 702 cases, including the ability to bring suit in federal district court for certain Privacy Act violations by the U.S. federal government relating to the sharing of law enforcement information.[30] It is beyond the scope of this supplemental memorandum to assess the adequacy of remedies, but a U.S. court certainly could consider whether the enactment of the JRA provides sufficient relief "of the same genre" to make relief under APA Section 702 inappropriate.

In conclusion, the APA Section 702 claim has had a mixed history in the national security context. It will remain to be seen whether, or what kind of, role it has going forward given the existing remedies, the extension of certain of the Privacy Act remedies to EU citizens under the JRA, as well as the new redress available under Privacy Shield, which is discussed below.

IV. Privacy Shield

After the May 24, 2016 Memo was prepared, the United States and the European Union entered into the *EU-U.S. Privacy Shield.*[31] Since other experts have covered Privacy Shield in some detail, I will focus my comments on the creation of an Ombudsperson. I would also note that Privacy Shield is not directly within the scope of my opinions, since they are, as noted above and in the May 24, 2016 Memo, confined to "non-exclusive overview of private remedies available to EU citizens, under federal law in the United States." Privacy Shield was significant enough, however, that I felt that it should be covered in some manner.

Professor Swire correctly observes that "[t]he EU-US Privacy Shield created new remedies against the US government available to EU persons. The Privacy Shield creates an Ombudsman within the US Department of State who can hear complaints from EU data subjects related to US government actions."[32] Professor Swire is also correct when he observes that the Ombudsperson is intended to be independent of the U.S. national security

---

§ 1861(f). This closed system includes no role for third parties, such as plaintiffs here, nor courts besides the FISC, such as this District Court. Congress's preclusive intent is therefore sufficiently clear.").

[29] Pub. L. No. 114-126, 130 Stat. 282. The Judicial Redress Act was signed by President Obama on February 24, 2016.

[30] *See id.*

[31] *See The EU-U.S. Privacy Shield*, EUROPEAN COMMISSION, http://ec.europa.eu/justice/data-protection/international-transfers/eu-us-privacy-shield/index_en.htm.

[32] *See* Affidavit of Peter Swire ¶ 53.

services and, notably, that the Ombudsman has authority not just under Privacy Shield regarding these matters, but also under BCRs, as well as SCCs.[33]

As noted in Annex A: EU-U.S. Privacy Shield Ombudsperson Mechanism, the Ombudsperson is intended to undertake a number of functions, including:

- Effective Coordination--the Privacy Shield Ombudsperson will be able to effectively use and coordinate with the oversight bodies, described below, in order to ensure that the Ombudsperson's response to requests from the submitting EU individual complaint handing body is based on the necessary information. When the request relates to the compatibility of surveillance with U.S. law, the Privacy Shield Ombudsperson will be able to cooperate with one of the independent oversight bodies with investigatory powers.
- Receive complaints from the EU individual complaint handling body and then conduct an initial review, track the status of requests and provide appropriate updates, as well as provide a timely and appropriate response to the submitting EU individual complaint handling body, as more fully discussed in Exhibit A.[34]

There is also a process that permits requests for further action where a request alleges a violation of law or other misconduct.[35]

The scheme establishes new avenues by which a complainant can seek redress. It will remain to be seen how these new remedies will operate once implemented, particularly since Privacy Shield offers redress that appears to be in some ways different than the more traditional judicial remedies.

---

[33] *Id. See also* Annex A: EU-U.S. Privacy Shield Ombudsperson Mechanism, https://www.privacyshield.gov/servlet/servlet.FileDownload?file=015t00000004q0g.
[34] Annex A: EU-U.S. Privacy Shield Ombudsperson Mechanism, https://www.privacyshield.gov/servlet/servlet.FileDownload?file=015t00000004q0g.
[35] *Id.*