

Expert Report of Professor Neil M. Richards

I, Neil Michael Richards, declare as follows:

1. I am the Thomas and Karole Green Professor of Law at Washington University School of Law in St. Louis, Missouri, USA, where I have taught for over thirteen years, and where I co-direct the Washington University Institute for Genomic Medicine and the Law. I am an affiliate scholar with both the Stanford Center for Internet and Society and the Yale Information Society Project, and a Fellow with the Center for Democracy and Technology. I also teach each year in the international Summer Course on Privacy Law and Policy at the Institute for Information Law at the University of Amsterdam in the Netherlands.
2. I have been retained to provide an expert opinion on behalf of the Data Protection Commissioner (“DPC”) of Ireland respecting certain matters of United States law that affect the resolution of these Proceedings. Specifically, I have been instructed by Philip Lee, solicitors for the DPC, to opine on certain matters of US law as follows:
 - (1) The judicial remedies to which a citizen of the European Union may have recourse in the event that his or her personal data is transferred from the EU to the United States where it is accessed and/or processed by US security or intelligence agencies for national security purposes in a manner incompatible with the citizen’s data privacy rights as they apply under EU law;
 - (2) The constraints or limitations (if any) that may impair an EU citizen’s capacity to access such remedies in practice;
 - (3) In particular, whether, how and to what extent the doctrine of “standing” may constrain or limit access to such remedies by an EU citizen, or any of them;
 - (4) The nature and extent of the remedy (or remedies) that an EU citizen may access in the United States in the particular context at hand in the light of the adoption of the Privacy Shield mechanism.

In formulating my opinion on points (1), (2) and (3) above, I have been asked to examine, consider and comment upon a memorandum addressing those same matters of US law prepared by Mr. Andrew Serwin of Morrison Foerster LLP, dated 24 May 2016, and, to the extent that they likewise address the particular matters of US law first examined by Mr. Serwin, the

reports prepared on behalf of the First Named Defendant, Facebook Ireland Limited, by Mr. Stephen Vladeck, Mr. Peter Swire, and Mr. Geoffrey Robertson, respectively, in addition to the expert reports prepared by Ms. Ashley Gorski on behalf of Maximillian Schrems, and Mr. Alan Butler on behalf of *amicus curiae* Electronic Privacy Information Center.

3. I understand that my duty as an expert is to assist the Court as to matters within my field of expertise, and that this duty overrides any other duty or obligation that I may owe to the party by whom I have been engaged or by any party liable to pay my fees.

MATERIALS REVIEWED

4. In preparing this opinion, I have reviewed an extensive set of materials pertinent to this case, which I have appended to this Report as Appendix A.

SUMMARY OF OPINION

5. It is my opinion that there is substantial evidence to support the conclusions of the DPC Draft Decision and the Serwin Memorandum that EU citizens lack meaningful avenues of legal relief to remedy violations of their data protection and privacy rights in the US. Moreover, I believe these conclusions are correct interpretations of the state of US law at present. US privacy remedies are indeed fragmentary and suffer from individual deficiencies; they also have to surmount the general obstacle of standing doctrine, which appears to be becoming more stringent, especially in privacy cases. In addition, having reviewed the Privacy Shield framework, particularly the new Privacy Ombudsperson mechanism, I do not find that this program provides a legal remedy that changes my conclusion. All I can say at the present time is that it is distinct from a judicial redress scheme, and beyond that it is not possible to say what, precisely, it will deliver.

QUALIFICATIONS AND BACKGROUND

6. *Education and clerkships.* I am a 1997 graduate of the University of Virginia School of Law, from which I also graduated with a Master's Degree in Legal History. In law school, I was the Executive Editor of the *Virginia Law Review*, and was awarded several academic prizes, including the Order of the Coif. Following law school, I clerked twice for federal judges, first for Judge Paul V. Niemeyer of the United States Court of Appeals for the Fourth Circuit, and then for Chief Justice of the United States William H. Rehnquist. My clerkship with Chief Justice Rehnquist involved assisting

him during the impeachment trial of President William Jefferson Clinton in the United States Senate. Following my clerkships, I was the inaugural Hugo Black Fellow at the University of Alabama Law School, and then a Temple Bar Fellow with the Inns of Court in London. I then practiced law for a number of years with Wilmer, Cutler, and Pickering (now WilmerHale), in their Washington, DC Office. At Wilmer, my practice was split between privacy law and litigation.

7. *Professional experience.* Since I entered academia, I have been highly active in professional activities relating to privacy and technology law. I am elected member of the American Law Institute, and an Advisor on the ALI's project on the Principles of the Law of Data Privacy, a major element of which is the question of what constitutes "personal information." I am a member of the Advisory Board of the Future of Privacy Forum, a Washington, DC-based think-tank composed of privacy law experts in industry and academia that seeks to advance responsible data practices. I am also an elected trustee of the Freedom to Read Foundation. I have also consulted with law firms and companies about practical privacy issues. I have been an invited speaker by the Federal Trade Commission, and international organizations to speak on questions of data privacy and data protection. I also submitted a brief along with several other leading privacy law scholars in the Supreme Court's most recent privacy law standing case, *Spokeo v. Robins*, 135 S.Ct. 1892 (2016).
8. *Scholarship.* My written scholarship has been devoted almost entirely to questions of information privacy law. My article "The Dangers of Surveillance," which appeared in the *Harvard Law Review* in 2013, is one of the most-read articles in the field of privacy law in recent years. I am also the author of approximately twenty articles and numerous smaller essays, and my scholarship has appeared or is appearing in many of the leading law reviews, including the *Harvard Law Review*, *Yale Law Journal*, *Columbia Law Review*, *Virginia Law Review*, *California Law Review*, and the *Georgetown Law Journal*. I have been cited over five hundred times in law review articles. My first book, *Intellectual Privacy*, was published by Oxford University Press in 2015. I have also written extensively for a general audience about a range of privacy law issues, and my work has appeared in a wide variety of publications, including *The Guardian*, *Slate*, *Salon*, *MIT Technology Review*, and the *Chronicle of Higher Education*.
9. *Media.* I regularly appear in the media giving expert commentary on a wide range of consumer privacy and Internet law issues. I have appeared as a guest on television and radio programmes, including CNN, PBS, National Public Radio, the BBC, and Fox News, and have been quoted as an expert on privacy and constitutional law in newspapers such as the *Washington Post*,

Wall Street Journal, The Guardian (U.K.), the Chicago Tribune, and the Boston Globe.

SCOPE OF OPINIONS

10. As noted above, I have been retained by the DPC in this case to offer my opinions on (1) The judicial remedies available to citizens of the European Union if their personal data is transferred from the EU to the United States and it is accessed by the US government in a manner incompatible with the citizen's data privacy rights as they apply under EU law; (2) the constraints or limitations (if any) that may impair an EU citizen's capacity to access such remedies in practice; (3) in particular, how US "standing" doctrine may constrain or limit access to such remedies by an EU citizen, or any of them; and (4) the nature and extent of the remedy (or remedies) that an EU citizen may access in the United States in light of the adoption of the Privacy Shield mechanism. Based upon this brief, I have not sought to attempt an exhaustively comprehensive treatment and overview of all of the many points of US law which are at issue in this case. Instead, I have focused my attention on the specific issues that the DPC has asked me to address, which are most central to the analysis in the Draft Opinion of the DPC at issue in these Proceedings.
11. In the following paragraphs, I shall set out, by way of background, certain factual matters bearing upon the scope of the opinions I express in this report. For the avoidance of doubt, I would emphasise that, insofar as I refer to the ruling of the Court of Justice of the European Community in the first *Schrems* case, or instruments of EU law, I do not purport to express any opinion on any matter of EU law.
12. In its judgment in the initial *Schrems* case, the Court of Justice of the European Union ("CJEU") ruled, inter alia, that the European Commission's Safe Harbour Decision of 26 July 2000 was invalid. This decision had provided a legal basis for the transfer of data about EU citizens from the EU to organisations in the US. See Judgment of the CJEU, Maximilian Schrems v. Data Protection Commissioner ¶¶90-95 (Case C-362/14, 6 October 2015) ("*Schrems I*").
13. Central to the CJEU's judgment in *Schrems I* that the Safe Harbour Agreement was invalid were its conclusions (reached by reference to analyses presented by the European Commission in documents bearing reference numbers Communication COM(2013) 846 Final and Communication COM(2013) 847 Final) that (1) the US National Security Agency ("NSA") had the ability to access the data of Facebook-Ireland's

European subscribers in a manner incompatible with those subscribers' data protection rights guaranteed by European Law; that (2) those rights included the fundamental right to judicial protection enshrined in Article 47 of the Charter of Fundamental Rights of the European Union. *Schrems I* at ¶¶90, 95.

14. Following the CJEU's ruling in *Schrems I*, the case returned to the High Court, where Judge Hogan issued an order on 20 October 2015 remitting the case back to the Office of the DPC for further investigation. Maximilian Schrems v. Data Protection Commissioner, Order of the High Court, made on 20 October 2015.
15. Pursuant to her Office's investigation, the DPC issued a Draft Decision in this matter on 24 May 2016. Draft Decision of the Data Protection Commissioner, under Section 10(1)(b)(ii) of the Data Protection Acts, 1988 & 2003 ("DPC Draft Decision.")
16. In her Draft Decision, the DPC considered whether, following the invalidation of the Safe Harbour Decision, another of the derogations provided for under Article 26 of the EU Data Protection Directive of 1995 might be available to allow Facebook-Ireland to legitimately transfer the data of its EU subscribers to the US for processing under the Decisions of the European Commission approving standard contractual clauses for the transfer of personal data to third countries. DPC Draft Decision at pp. 1-3 & ¶¶1-10.
17. In her investigation, the DPC proceeded, as she put it, along "two distinct strands." DPC Draft Decision at ¶34. Strand One comprised a factual investigation regarding whether Facebook Ireland Limited (referred to in the Draft Decision and hereinafter as "FB-I") continued to transfer EU subscribers' personal data to the US following the CJEU Judgment in *Schrems I*. The DPC concluded that FB-I had, in fact continued to transfer data about its EU subscribers to its US-based parent company pursuant to the standard-form contractual clauses approved by the European Commission. DPC Draft Decision at ¶36.
18. Strand Two of the DPC's investigation comprised a legal investigation regarding the authority relied upon by FB-I to transfer personal data to the US. This inquiry itself had two dimensions: First, whether US law ensured "adequate" protection for the data protection rights of EU citizens; and second, if US law was not "adequate," whether the use of the standard contractual clauses offered "adequate safeguards with respect to the

protection of the privacy and fundamental rights and freedoms of individuals and as regards the exercise of their corresponding rights.” DPC Draft Decision at ¶37.

19. In the context of her examination of the ‘adequacy’ issue under Strand Two, the DPC obtained counsel from Mr Andrew Serwin of Morrison & Foerster LLP, a leading authority on US privacy law. Mr. Serwin produced a memorandum dated 24 May 2016 that provided 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.” Serwin Memorandum at p. 1.
20. The DPC noted that, while the CJEU did not determine explicitly that the US failed to ensure an adequate level of data protection within the meaning of Article 25(2) of the Directive, “[t]he Court appears to have inferred from the absence of any such findings in the Safe Harbour Decision that, under the laws of the US, the data protection rights of citizens whose data is transferred from the European Union to the US is, as a matter of fact, at risk of interference by US State entities on national security grounds and that such interference is not subject to the range of safeguards that would apply in the EU. It appears that, in drawing that inference, the Court relied, at least in part, on the findings contained in the ad hoc EU/US Working Group Report dated 27 November 2013.” DPC Draft Decision at ¶39-40. The DPC referred to the European Commission’s Communication [COM(2016)117 Final], observing that US law in this area had changed in three significant respects since 2013: (1) the Presidential Policy Directive 28 (“PPD-28”) (2014), (2) the USA-Freedom Act of 2015, and (3) the Judicial Redress Act of 2016. DPC Draft Decision at ¶41.
21. The DPC concluded that, having regard to the Serwin memorandum, and notwithstanding these reforms in US law and policy, “on the basis of my examination of these issues to date, it appears to me, at the current stage of my investigation, and subject to such further submissions as may be made, that, notwithstanding the above-referred changes in the US legal order, it remains the case that, even now, a legal remedy compatible with Article 47 of the Charter is not available in the US to EU citizens whose data is transferred to the US where it may be at risk of being accessed and processed by US State agencies for national security purposes in a manner incompatible with Articles 7 and 8 of the Charter.” DPC Draft Decision at ¶43.

22. The DPC thus based her judgment under Article 47 of the Charter, the “Right to an effective remedy and to a fair trial,” which provides in full that:

“Everyone whose rights and freedoms guaranteed by the law of the Union are violated has the right to an effective remedy before a tribunal in compliance with the conditions laid down in this Article. Everyone is entitled to a fair and public hearing within a reasonable time by an independent and impartial tribunal previously established by law. Everyone shall have the possibility of being advised, defended and represented.

Legal aid shall be made available to those who lack sufficient resources in so far as such aid is necessary to ensure effective access to justice.”

Charter of Fundamental Rights of the European Union, Art. 47.

23. In concluding that US law did not provide an “effective remedy” under Article 47 (and therefore did not ensure adequate protection for the data privacy rights of EU citizens), the DPC noted that “it is important to note that EU citizens are not completely without redress in the US, and that a number of remedial mechanisms are available under US law.” DPC Draft Decision at ¶44. However, she concluded that “by reference to EU law, there are both specific and general deficiencies in those remedial mechanisms:

“(1) From a specific perspective, the remedies are fragmented, and subject to limitations that impact on their effectiveness to a material extent; moreover, they arise only in particular factual circumstances, and are not sufficiently broad in scope to guarantee a remedy in every situation in which there has been an interference with the personal data of an EU data subject contrary to Articles 7 and 8 of the Charter. To that extent, the remedies are not complete.

(2) From a more general perspective, the “standing” admissibility requirements of the US federal courts operate as a constraint on all forms of relief available.”

DPC Draft Decision at ¶45.

24. On the specific objections, the DPC concluded that “[f]rom a specific perspective, the remedies are fragmented, and subject to limitations that impact on their effectiveness to a material extent; moreover, they arise only in particular factual circumstances, and are not sufficiently broad in scope to guarantee a remedy in every situation in which there has been an

interference with the personal data of an EU data subject contrary to Articles 7 and 8 of the Charter. To that extent, the remedies are not complete.” DPC Draft Decision at ¶45. The DPC went on to discuss several examples, including the Foreign Intelligence Surveillance Act (“FISA”), 50 U.S.C. §1801 et seq., the Electronic Communications Privacy Act, 18 U.S.C. § 2501 et seq., the Stored Communications Act, 18 U.S.C. § 2701 et seq., the Computer Fraud and Abuse Act, 18 U.S.C. § 1030, the Right to Financial Privacy Act, 12 U.S.C. § 3417, and the Freedom of Information Act, 5 U.S.C. § 552. DPC Draft Decision at ¶¶46-50. The DPC also considered the use of Executive Power to authorize surveillance, such as under Executive Order 12333, and concluded that because “the available remedies do not deal with certain legal bases available to US intelligence authorities to access and process data ... it is simply not possible to assess whether or not the remedies outlined above are sufficient to address the full extent of the activities of the intelligence authorities in question.” DPC Draft Decision at ¶51.

25. Turning to the general objection, the DPC found that “an overarching issue applying to all of these causes of actions is that arising from US constitutional ‘standing’ requirements, which are mandated by the ‘case or controversy’ condition of Article III of the US Constitution.” DPC Draft Decision at ¶52.
26. In assessing the compatibility of standing doctrine with Article 47, the DPC noted the judgment of the CJEU in *Schrems I*, that “... to establish the existence of an interference with the fundamental right to respect for private life, it does not matter whether the information in question relating to private life is sensitive or whether the persons concerned have suffered any adverse consequences on account of that interference (judgment in *Digital Rights Ireland and Others*, C 293/12 and C 594/12, EU:C:2014:238, paragraph 33 and the case-law cited).” DPC Draft Decision at ¶30 (quoting *Schrems I* at ¶78).
27. Based upon this ruling, the DPC concluded that “[t]he extent to which the ‘standing’ requirements applicable under US law would appear to operate to limit an individual’s capacity to access a remedy in this context in a manner incompatible with EU law is illustrated by the decision of the US Supreme Court in *Clapper v. Amnesty International* [133 S.Ct. 1138 (2013)]. In that case, the plaintiffs sought to pursue allegations that certain amendments to FISA were unconstitutional because of the plaintiffs’ stated belief that there was an objectively reasonable likelihood that their communications with foreign contacts would be intercepted in the future, or, alternatively, because they were already suffering injury because they found themselves having to

take costly and burdensome measures to protect the confidentiality of their international communications. The US Supreme Court held that the plaintiffs lacked standing because, inter alia, their fears were ‘highly speculative’ in nature, and because ‘they could not demonstrate that the future injury they purportedly fear is certainly impending and because they cannot manufacture standing by incurring costs in anticipation of non-imminent harm.’ I consider that such an approach is not reconcilable with that outlined in *Schrems* where the CJEU made it clear that a claimant cannot be required to demonstrate that harm has in fact been suffered as a result of the interference alleged.” DPC Draft Decision at ¶55.

28. The DPC also considered the remedies available to EU citizens to sue the US government under the Privacy Act of 1974, 5 U.S.C. § 552a, as expanded by the passage and entry into force of the Judicial Redress Act (“JRA”), Pub. L. No. 114-126 (2016), which extends certain of the remedies available to US citizens under the Privacy Act to EU citizens if certain conditions specified in the JRA are met. The DPC concluded that “[w]hilst, on the face of it, the JRA purports to open up access for EU citizens to remedies that were not previously available to them, the effectiveness of those remedies is subject to a number of important limitations and/or restrictions.” DPC Draft Decision at ¶57-59.
29. Accordingly, the DPC concluded that “at least on the question of redress, the objections raised by the CJEU in its judgment in *Schrems* have not yet been answered,” DPC Draft Decision at ¶60, and that “the safeguards purportedly constituted by the standard contract clauses ... do not address the CJEU’s objections concerning the absence of an effective remedy compatible with the requirements of Article 47 of the Charter, as outlined in *Schrems*. Nor could they. On their terms, the standard contract clauses in question do no more than establish a right in contract, in favour of data subjects, to a remedy against either or both of the data exporter and importer. Importantly for current purposes, there is no question but that the [European Commission’s Standard Contract Clause] Decisions are not binding on any US government agency or other US public body; nor do they purport to be so binding. It follows that they make no provision whatsoever for a right in favour of data subjects to access an effective remedy in the event that their data is (or may be) the subject of interference by a US public authority, whether acting on national security grounds, or otherwise. On this basis, I have formed the view, subject to consideration of such further submissions as may be filed by the Complainant and FB-I, that the protections purportedly provided by the standard contract clauses contained in the Annexes to the [European Commission’s Standard Contract Clause] Decisions are limited in their extent and in their application. So far as the question of access to an

effective remedy is concerned, it is my view that they cannot be said to ensure adequate safeguards for the protection of the privacy and fundamental rights and freedoms of EU citizens whose data is transferred to the US.” DPC Draft Decision at ¶61.

30. As a result, the DPC concluded that the European Commission’s Decisions legitimating the standard contractual clauses were likely to offend against Article 47 of the Charter, which required her to enter into the current Proceedings. As she put it in conclusion, “a legal remedy compatible with Article 47 of the Charter is not available in the US to EU citizens whose data is transferred to the US and whose personal data may be at risk of being accessed and processed by US State agencies for national security purposes in a manner incompatible with Articles 7 and 8 of the Charter. Against that backdrop, I consider that the [Standard Contract Clause] Decisions are likely to offend against Article 47 of the Charter insofar as they purport to legitimise the transfer of the personal data of EU citizens to the US notwithstanding the absence of a complete framework for any such citizen to pursue effective legal remedies in the US.” DPC Draft Decision at ¶64.

31. As I understand it, the DPC’s Draft Decision thus examined not whether US law is *adequate or not* in the broadest sense, and in all respects, but rather, whether US law is adequate in one particular respect, namely, whether US law provides an *effective remedy before a tribunal* to EU citizens to effectuate their substantive rights to privacy and data protection under EU law, particularly under Article 47 of the Charter of Fundamental Rights of the European Union. As is apparent from the Draft Decision, the DPC considered that her findings on that particular issue were determinative of the adequacy issue generally. Reflecting the DPC’s approach, I have likewise focused my report on this narrower legal question of remedies under US law, and not primarily on other, broader questions of adequacy, such as the legal and policy checks on government surveillance. These are interesting and complex legal questions, but they are beyond the scope of this Expert Report, except as they are relevant to address the question of availability of remedies, and except where noted below.

FINDINGS AND EXPERT OPINIONS

I. Data Protection Remedies Available to EU Citizens under US Law

32. The DPC Draft Decision noted that while EU citizens had some remedies under US law, “[f]rom a specific perspective, the remedies are fragmented,

and subject to limitations that impact on their effectiveness to a material extent; moreover, they arise only in particular factual circumstances, and are not sufficiently broad in scope to guarantee a remedy in every situation in which there has been an interference with the personal data of an EU data subject contrary to Articles 7 and 8 of the Charter. To that extent, the remedies are not complete.” DPC Draft Decision at ¶45. In this section of my report, I canvas what I believe to be the most important and most relevant judicial remedies, and discuss their contexts, elements, and limitations. In particular, insofar as the DPC Draft Decision reflects or takes account of the Serwin Memorandum, I have reviewed that Memorandum and its conclusions for accuracy and completeness.

33. As the DPC noted, unlike the EU and virtually all other industrialized Western democracies, the US does not have a comprehensive data protection statute. See, e.g., WILLIAM MCGEVERAN, *PRIVACY AND DATA PROTECTION LAW* 258 (2016) (“MCGEVERAN”). As Professors Solove and Schwartz put it in their leading casebook and treatise on privacy law, “Numerous statutes are directly and potentially applicable to the collection, use, and transfer of personal information by commercial entities. Congress’s approach is best described as “sectoral,” as each statute is narrowly tailored to particular types of businesses and services. The opposite of sectoral in this context is omnibus, and the United States lacks such a comprehensive statute regulating the private sector’s collection and use of personal information. Such omnibus statutes are standard in much of the rest of the world. All member nations of the European Union have enacted omnibus information privacy laws” DANIEL J. SOLOVE & PAUL M. SCHWARTZ, *INFORMATION PRIVACY LAW* 2 (7th ed. 2015) (“SOLOVE & SCHWARTZ”).
34. Data protection law in the United States is thus a complex web of, among other things, constitutional law rules binding the government, incomplete sector-specific federal statutes, state law statutes and common-law rules. SOLOVE & SCHWARTZ at 10-41. In my opinion, these facts support the DPC’s conclusion that US privacy law remedies are “fragmented” rather than general. Indeed, in my own scholarship I have argued that “American law governing surveillance is piecemeal, spanning constitutional protections such as the Fourth Amendment, statutes like the Electronic Communications Privacy Act of 1986 (ECPA), and private law rules such as the intrusion-into-seclusion tort. But the general principle under which American law operates is that surveillance is legal unless forbidden. ... Plaintiffs can only challenge secret government surveillance they can prove, but the government isn’t telling. Plaintiffs (and perhaps civil liberties) are out of luck.” Neil M. Richards, *The Dangers of Surveillance*, 126 HARV. L. REV. 1934, 1943-44 (2013). This paragraph, taken from the introduction of

an article I published two weeks before Edward Snowden's revelations about the US government's surveillance activities in June 2013, reaches essentially the same conclusion about remedies and standing under US law as the DPC Draft Decision of May, 2016. The review of the relevant US legal doctrines which follows explains this conclusion in greater detail.

A. Constitutional Law

35. There are at least two rights recognized under the US Constitution that could provide avenues for relief for EU citizens whose personal data has been gathered in the context of national security by the US government: the Fourth Amendment and the constitutional right of information privacy. I note that my analysis on these points goes beyond that of the Serwin Memorandum, which was directed to federal statutory causes of action.

1. The Fourth Amendment

36. The Fourth Amendment to the US Constitution provides that

“The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.”

U.S. CONST. AMD. IV.

37. The Fourth Amendment applies, among other things, to protect the privacy of communications and electronic data. *Katz v. United States*, 389 U.S. 347 (1967); *Riley v. California*, 573 U.S. ___ (2014). However, the Supreme Court has suggested it applies with less force in the foreign national security context. See *United States v. United States District Court*, 407 U.S. 297 (1972). In these areas, the Foreign Intelligence Surveillance Act is usually considered to serve as the regulation and remedy of first instance. SOLOVE & SCHWARTZ at 420-21.
38. Another obstacle to Fourth Amendment relief is the so-called “Third-Party Doctrine.” This is the highly-controversial idea that information loses its Fourth Amendment protection when it is shared with a third party such as a telephone company, *Smith v. Maryland*, 442 U.S. 735 (1979) (phone numbers dialed), or a bank, *United States v. Miller*, 425 U.S. 435 (1976); The doctrine remains a matter of substantial criticism and debate, and at least

one Justice on the current Supreme Court has called for the Court to re-examine it. *E.g.*, *United States v. Jones*, 132 S. Ct. 945 (Sotomayor, J., concurring in the judgment).

39. With respect to the third party doctrine, the federal government has long maintained that stored emails, which are communications shared with a telecommunications company, are within the third-party doctrine, though this proposition was flatly rejected by a federal appeals court in 2010. *United States v. Warshak*, 631 F.3d 266 (6th Cir. 2010). The federal government did not seek to appeal that case to the Supreme Court, and as a result, the rule in *Warshak* is only binding in the handful of American states governed by the ruling of that regional court (Kentucky, Michigan, Ohio and Tennessee). Whilst I believe that the Supreme Court would likely ratify the result in *Warshak* were it to hear a case squarely presenting the issue, the constitutional protection of emails in the United States remains unclear at present. (I agree with the Vladeck Report at ¶27 in this respect).
40. When the Fourth Amendment has been violated by the government, the normal remedy is the exclusion of evidence obtained in violation of the Constitutional rule from a criminal trial. However, since Fourth Amendment violations can happen outside the context of the investigation of criminals, the Supreme Court has also held that there exists an implied private right of action to protect all Americans against deprivations of Fourth Amendment rights by the federal government. *Bivens v. Six Unknown Named Agents*, 403 U.S. 388 (1971).
41. It remains unclear, however, whether a Fourth Amendment *Bivens* action is available to foreign claimants who lack substantial connections to the United States. *United States v. Verdugo-Urquidez*, 494 U.S. 259 (1990). As Professor Vladeck points out, “U.S. courts have been hostile to *Bivens* claims in the national security context—so that such remedies may be *formally* available to individuals with Fourth Amendment rights, but have at least thus far proven almost categorically unavailable to them in practice. See, e.g., Stephen I. Vladeck, *The New National Security Canon*, 61 AM. U. L. REV. 1295 (2012). But see *Turkmen v. Hasty*, 789 F.3d 218 (2d Cir. 2015) (recognizing a *Bivens* claim arising out of the allegedly unlawful conditions of confinement of immigration detainees in a national security case), cert. granted, No. 15-1363, 2016 WL 2653655 (U.S. Oct. 11, 2016).” As Professor Vladeck further notes, the Supreme Court’s grant of certiorari in *Turkmen v. Hasty* may resolve this important question. At present, however, a *Bivens* claim under the Fourth Amendment does not seem to be one which is broadly open to EU citizens to effectuate privacy and data protection rights under Articles 7 and 8 of the European Charter against the US government.

Moreover, the Supreme Court will also hear a case this Term regarding the extraterritorial application of the Fourth Amendment stemming from a police shooting that occurred across the US-Mexican border, see *Hernandez v. Mesa*, No. 15-118, 2016 WL 5897576 (U.S., Oct. 11, 2016). It is thus fair to say that US law is unclear at present regarding whether an EU citizen (who is not a permanent resident of the United States) can bring a constitutional action for an alleged violation of her Fourth Amendment rights.

2. The Constitutional Right of Information Privacy

42. Another potential remedy for EU citizens might lie in the federal constitutional right of information privacy, which is a controversial offshoot of the even more controversial constitutional right of privacy recognized by the Supreme Court in *Griswold v. Connecticut*, 381 U.S. 479 (1965), and *Roe v. Wade*, 410 U.S. 113 (1973). In the case of *Whalen v. Roe*, 429 U.S. 589 (1977), the Supreme Court seemed to recognize such a right in *obiter dictum* in the context of a state database of prescription records, and while some lower federal courts have recognized the right, its existence to this day is a matter of some scholarly and judicial debate. In its two subsequent cases raising the doctrine, the Supreme Court has assumed without deciding the existence of the right, but then found that the right was not violated under the facts of each particular case. Accordingly, it declined to recognize the right explicitly. *Nixon v. Administrator of Gen. Servs.*, 433 U.S. 425 (1977); *NASA v. Nelson*, 131 S.Ct. 746 (2010).

B. Federal Statutory Law

43. There are several federal statutes that could potentially provide avenues of relief for EU citizens challenging the collection, use, and disclosure of their data by the federal government for national security purposes.

1. The Privacy Act/Judicial Redress Act

44. Although as noted above, the United States does not have a general data protection statute, it does have a sectoral data protection statute governing information held by the federal government. The Privacy Act of 1974 applies broadly to “records” about an “individual” held in a “system of records” 5 U.S.C. § 552a(g)(1)(D), which are protected by (among other things) a rule of nondisclosure, 5 U.S.C. § 552a(b). Violations of the Privacy Act are enforced by a variety of civil remedies, including injunctive relief, 5 U.S.C. § 552a(g)(3), and in the case of an “intentional or willful” violation, actual damages with a minimum recovery of \$1,000, costs, and reasonable attorney fees, 5 U.S.C. § 552a(g)(4).

45. The Serwin Memorandum explains the remedies available under the Privacy Act (pp. 4-5), as extended to non-US persons under the Judicial Redress Act (pp. 5-9). I have read and examined the analysis set out in the Memorandum and its conclusions. I am satisfied that its analysis is both complete and well-founded, and I agree with its conclusions. I also concur with the views expressed in the Memorandum to the effect that the remedies to be accessed under the Judicial Redress Act, in particular, are subject to limitations (both actual and potential) that are material in their nature and extent. I offer the following additional observations on those remedies.
46. One point in which I would like to amplify the Serwin Memorandum's discussion is its reference on page 5 to the Supreme Court's cutting back on the damages remedy under the Privacy Act in recent years. In *Doe v. Chao*, 540 U.S. 614 (2004), the Supreme Court held in a case involving a Privacy Act claim that "actual damages" under the Privacy Act needed to be proven in order for a plaintiff to recover the statutory minimum damages of \$1,000. In the more recent case of *FAA v. Cooper*, 132 S.Ct. 1441 (2012), however, the Court held that as a matter of statutory interpretation, the Privacy Act remedy for "actual damages" could not include damages claims for mental and emotional harm, and that plaintiffs seeking Privacy Act damages must show "pecuniary harm" in order to recover. This was the case, in the Court's view, because the Privacy Act, by authorizing damages actions against the sovereign, constitutes a waiver of sovereign immunity, which must be strictly construed in favor of the government and against private plaintiffs. The decision occasioned a passionate (and to my mind, legally correct) dissent by three Justices led by Justice Sotomayor, but after *Cooper*, it is clear that the Supreme Court does not appear inclined to expand damage claims under the Privacy Act. As I interpret the majority opinion in *Cooper*, I have further doubts whether that Court would recognize the deprivation of European fundamental rights of privacy as "actual damages" under the Privacy Act, on the ground that they were dignitary rather than pecuniary.¹

¹ I note in passing in connection with *Cooper* that I agree with Professor Vladeck's observation that this strict limitation on the availability of *damages* does not disturb the availability of *injunctive relief* against the federal government under the Act. Vladeck Report at ¶97. However, in my opinion, this does not invalidate the DPC's specific conclusion in ¶59(9) of her Draft Decision that these developments mean that "a requirement to prove pecuniary loss or damage will also operate as a precondition to the availability of particular remedies under the JRA." DPC Draft Decision at ¶59(9) Many violations of the rights of privacy and data protection under both the European (as I understand them) and traditional American views are nonpecuniary, but *Cooper* seems to foreclose them almost entirely.

47. The Privacy Act's general rule of nondisclosure is subject to twelve statutory exceptions, 5 U.S.C. § 552a(b)(1)-(12), three of which I would like to highlight. First, the Act exempts "routine uses" of data by an agency. This allows the disclosure of a record for any "routine use" if disclosure is "compatible" with the purpose for which the agency collected the information in the first place. 5 U.S.C. § 552a(a)(7) & (b)(3). This is a very broad exception that, in the minds of many distinguished scholarly and practical commentators on privacy law, has the potential to be the proverbial exception that swallows the rule. For example, Paul Schwartz has noted that "Federal agencies have cited this exemption to justify virtually any disclosure of information without the individual's permission." Paul M. Schwartz, *Privacy and Participation: Personal Information and Public Sector Regulation in the United States*, 80 IOWA L. REV. 553, 585 (1995). Robert Gellman is even more critical of the routine use exemption, suggesting that

"The [Privacy A]ct limits use of personal data to those officers and employees of the agency maintaining the data who have a need for the data in the performance their duties. This vague standard is not a significant barrier to the sharing of personal information within agencies. . . . No administrative process exists to control or limit internal agency uses. Suits have been brought by individuals who objected to specific uses, but most uses have been upheld. . . . The legislation left most decisions about external uses to the agencies, and this created the biggest loophole in the law. An agency can establish a 'routine use' if it determines that a disclosure is compatible with the purpose for which the record was collected. This vague formula has not created much of a substantive barrier to external disclosure of personal information. . . . Later legislation, political pressures, and bureaucratic convenience tended to overwhelm the law's weak limitations. Without any effective restriction on disclosure, the Privacy Act lost much of its vitality and became more procedural and more symbolic."

Robert Gellman, *Does Privacy Law Work?* in TECHNOLOGY AND PRIVACY: THE NEW LANDSCAPE (Philip E. Agre & Marc Rotenberg eds., 1997).

48. A second statutory exception in the Privacy Act disclosure bar is that for law enforcement. The Act excludes disclosures "to another agency or to an instrumentality of any governmental jurisdiction within or under the control of the United States for a civil or criminal law enforcement activity if the activity is authorized by law, and if the head of the agency or instrumentality has made a written request to the agency which maintains

the record specifying the particular portion desired and the law enforcement activity for which the record is sought” 5 U.S.C. § 552a(b)(7).

49. A third exception to the rule of nondisclosure in the Privacy Act allows individual agencies to follow a procedure to exempt systems of records if those records are (a) kept by the Central Intelligence Agency or (b) “maintained by an agency or component thereof which performs as its principal function any activity pertaining to the enforcement of criminal laws.” As the Serwin Memorandum details, the NSA has taken advantage of this procedure, and further exempted records classified under its collection powers authorized by Presidential executive orders. Serwin Memorandum at pp. 4-5. Quoting a blog post by former Bush White House Official Tim Edgar, the Vladeck Report explains that this provision makes sense in that it would be counter-productive to allow domestic or international criminals and terrorists the ability to access their own NSA files. Vladeck Report at ¶68 (quoting Tim Edgar, *Redress for NSA Surveillance: The Devil is in the Details*, LAWFARE, Oct. 19, 2015, <https://www.lawfareblog.com/redress-nsa-surveillance-devil-details>). I agree with this conclusion, with the caveat that there is a difference between keeping targeted surveillance secret, and keeping entire surveillance programmes secret. It is my opinion that, under the best traditions of American constitutionalism, a democratic citizenry should have the right to know and consent to the broad contours of government surveillance that are engaged in by the state in their name. See, e.g., Neil M. Richards, *The Dangers of Surveillance*, 126 HARV. L. REV. 1934, 1959-61 (2013).
50. As it was originally enacted in 1974, the Privacy Act (and thus its remedies) only applied to US persons. The definition of “individual” in the statute is “a citizen of the United States or an alien lawfully admitted for permanent residence.” 5 U.S.C. § 552a(a)(2). By its terms, then, the Privacy Act does not apply to EU citizens who are resident in Europe.
51. The Judicial Redress Act, signed by President Obama on February 24, 2016, has the potential to expand the remedies available to US “individuals” to EU citizens. Judicial Redress Act of 2016, Pub. L. No. 114-126. The Serwin Memorandum explains the remedies available under the Judicial Redress Act at pp. 5-9 and offers opinions on its limited utility. I am satisfied that the analysis in the Serwin Memorandum is both complete and well-founded, and I agree with its conclusions. The Judicial Redress Act grants the US Secretary of State the functional power to designate foreign nationals as US “individuals” within the meaning of the Privacy Act, and thus to open up its remedies to those foreign nationals, including, in some cases, damages. *Id.* To my knowledge, neither the EU (nor any Member State) has to date been

so designated. However, even were such a designation to be made in the future (which I believe is quite possible, at least in part), because the Privacy Act is a limited statute due to its many exceptions, and because many of the records potentially at interest in these Proceedings have been exempted by administrative processes from its coverage, it is difficult for me to envision that the Judicial Redress Act would be a vehicle for the kinds of effective litigation contemplated by the CJEU and the DPC under Article 47 of the European Charter, at least as I understand the meaning of those terms in *Schrems I*.

52. In particular, the exemption of government surveillance records from the Privacy Act discussed above makes the Privacy Act a very poor vehicle for EU citizens to vindicate their fundamental rights under Articles 7, 8, and 47 of the European Charter. As Mr. Edgar continues in the blog post quoted above, “[p]retending that providing Privacy Act rights to EU citizens responds to European concerns about redress for targets of PRISM and other intelligence programs is not going to fool anyone. It will take more fundamental – and much more difficult – changes to surveillance law to address the EU’s concerns about redress.” quoting Tim Edgar, *Redress for NSA Surveillance: The Devil is in the Details*, LAWFARE, Oct. 19, 2015, <https://www.lawfareblog.com/redress-nsa-surveillance-devil-details>.

2. The Electronic Communications Privacy Act/Stored Communications Act

53. The Fourth Amendment to the U.S. Constitution, as noted earlier, protects the privacy of communications and other areas of human activity against unreasonable searches and seizures by the state. Although the Supreme Court initially held, for example, that telephone calls were not protected by the Fourth Amendment because wiretapping was a non-physical intrusion, *Olmstead v. United States*, 277 U.S. 438, 466 (1928), the Supreme Court reversed this position four decades later, holding in *Katz v. United States*, 389 U.S. 347 (1967) that wiretaps required a warrant. The following year, Congress passed the federal Wiretap Act as Title III of the Omnibus Crime Control and Safe Streets Act of 1968, which implemented this holding by providing detailed regulation of wiretapping and the bugging of oral communications.

54. A few years later, the Supreme Court decided the case of *United States v. United States District Court*, 407 U.S. 297 (1972).² In this case, involving a warrantless wiretap of alleged domestic terrorists, the Court held that the Fourth Amendment applied to regulate investigation of domestic threats to national security, though it held out the possibility that Congress might be able to create different rules than Title III for intelligence-gathering cases that might nevertheless satisfy the Fourth Amendment.
55. The Electronic Communications Privacy Act, 18 U.S.C. § 2501 et seq. (“ECPA”) was passed in 1986 to update the old Wiretap Act of 1968.
56. The Serwin Memorandum explains the remedies available under ECPA on pp. 9-10. I am satisfied that its analysis is both complete and well-founded, and I agree with its conclusions. I will offer a few additional thoughts on ECPA’s context and remedies.
57. ECPA is a detailed and highly complex statute, but its relevant provisions can be summarized succinctly. Title I of ECPA provides for extensive protection of the “contents” of wire, oral, and electronic communications against both government and private interceptions.³ Title I of ECPA requires the government to obtain a warrant to intercept the contents of communications, has minimization procedures, and violations of Title I are enforceable by criminal prosecution and civil penalties including a private right of action for substantial damages. The ordinary private right of action is not available against the United States, 18 U.S.C. § 2520 (providing for a right of action for “any *person* whose wire, oral, or electronic communication is intercepted, disclosed, or intentionally used in violation of this chapter may in a civil action recover from the person or entity, other than the United States, which engaged in that violation”). Title I also has a statutory exclusionary rule for illegally-intercepted wire or oral (but not electronic) communications. 18 U.S.C. § 2518(10)(a); see also SOLOVE & SCHWARTZ at 353-54.

² Due to its generic name, this decision is usually called the “Keith” decision after the name of the district judge in the case. In the interests of keeping my analysis concise, I have not adopted the colloquial name for the case in this Report.

³ A confusing point of American privacy law is that the Wiretap Act was itself Title III of a broader law, the “Crime Bill” of 1968, entitled the Omnibus Crime Control and Safe Streets Act of 1968. Even today, lawyers routinely call Title I of ECPA “Title III,” which was the shorthand lawyers used to describe the old Wiretap Act before the passage of ECPA.

58. Title II of ECPA, the “Stored Communications Act,” provides for government access to stored communications and telecommunications company customer data under a variety of standards. Unlike Title I, however, Title II has a private right of action, which provides that “[a]ny person who is aggrieved by any willful violation of this chapter or of chapter 119 of this title or of sections 106(a), 305(a), or 405(a) of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.) may commence an action in United States District Court against the United States to recover money damages. In any such action, if a person who is aggrieved successfully establishes such a violation of this chapter or of chapter 119 of this title or of the above specific provisions of title 50, the Court may assess as damages (1) actual damages, but not less than \$10,000, whichever amount is greater; and (2) litigation costs, reasonably incurred.” 18 U.S.C. § 2712(a). See also Vladeck Report at ¶26.
59. Title II of ECPA also allows the government the ability to obtain the contents of stored wire and electronic communications from a telecommunications company without notice to the customer who is the subject of surveillance if it obtains a warrant. 18 U.S.C. § 2703(b). Delayed notice is also available under 18 U.S.C. § 2705. In April 2016, Microsoft Corporation filed a lawsuit against the federal government challenging these provision for secret notice on First and Fourth Amendment grounds. It argued that it had received over 2,500 secret orders over the previous 18 months, and that 68 per cent of these orders called for indefinite secrecy of the search. The case is currently pending in federal district court in Seattle, Washington. *Microsoft Corporation v. United States Department of Justice*, No. 2:16-cv-00538-JLR (W.D. Wash. 2016). (In full disclosure, I should note that I signed an amicus brief on behalf of a group of law professors supporting Microsoft’s claim that the Stored Communication Act provisions at issue in this case are unconstitutional). Microsoft brought the lawsuit in this case in part on behalf of its customers, because government’s orders obtained pursuant to the secrecy provisions of the Stored Communications Act purportedly prevent those customers from ever learning about the surveillance, much less seeking a remedy against it, except perhaps when they might be prosecuted for illegal activity discovered through the surveillance. See generally Microsoft Corporation, *Keeping Secrecy the Exception, Not the Rule*, DigitalConstitution.com, April 14, 2016, available at <https://digitalconstitution.com/2016/04/keeping-secrecy-exception-not-rule/>.
60. ECPA was a remarkably far-sighted statute passed by Congress to (in effect) regulate e-mail before most people had even heard of the technology. However, thirty years on, ECPA is showing its age, as many of the

technological assumptions that undergirded the statute have changed. This can lead to some absurd results. The Microsoft litigation just discussed illustrates one such case. Another example is that the Stored Communications Act provides for lower protection for the contents of electronic communications stored for over 180 days. 18 U.S.C. § 2703(a). In an age of telephone answering machines, modems, and magnetic tape, this distinction might have made some sense, but in the age of cloud computing and storage and instantaneous networking, it is not only problematic, but also arguably inconsistent with the Fourth Amendment. It is my opinion that most American lawyers working in this field agree that ECPA needs to be reformed, but cannot agree on the standards that should regulate privacy and law enforcement access to electronic information. In any event, the over-use of secret orders makes it hard for people whose electronic data is accessed under ECPA to challenge it (especially the majority of people who are not charged with crimes), and the “willfulness” requirement in its remedy against the government is a material obstacle to relief.

3. FISA & Foreign Surveillance Law

61. The Foreign Intelligence Surveillance Act (“FISA”), 50 U.S.C. § 1801 et seq., was enacted in 1978. The law was the product of two developments. The first of these was the Supreme Court’s invitation to Congress (discussed above) in *United States v. United States District Court*, 407 U.S. 297 (1972), to develop different procedures than ECPA for national security intelligence gathering. The second of these was the report of a special post-Watergate Senate commission known as the “Church Committee,” which documented extensive warrantless surveillance and other abuses by the Nixon Administration. These included “COINTELPRO,” a Federal Bureau of Investigation (“FBI”) programme to investigate, disrupt, and “neutralize” dissident political groups. MCGEVERAN at 562; SOLOVE & SCHWARTZ at 419-420. These groups included a variety of dissident political and other groups, including the Black Panthers, the anti-Vietnam War movement, and the Ku Klux Klan. MCGEVERAN at 562. As the Church Committee’s final report itself concluded,

“Too many people have been spied upon by too many Government agencies and too much information has been collected. The Government has often undertaken the secret surveillance of citizens on the basis of their political beliefs, even when those beliefs posed no threat of violence or illegal acts on behalf of a hostile foreign power. The Government, operating primarily through secret informants, but also using other intrusive techniques such as wiretaps, microphone “bugs,” surreptitious mail opening, and break-ins, has swept in vast amounts of information about the personal lives, views, and

associations of American citizens. . . . Groups and individuals have been harassed and disrupted because of their political views and their lifestyles. Investigations have been based upon vague standards whose breadth made excessive collection inevitable. . . . The FBI's COINTELPRO — counterintelligence program — was designed to “disrupt” groups and “neutralize” individuals deemed to be threats to domestic security. The FBI resorted to counterintelligence tactics in part because its chief officials believed that existing law could not control the activities of certain dissident groups, and that court decisions had tied the hands of the intelligence community. Whatever opinion one holds about the policies of the targeted groups, many of the tactics employed by the FBI were indisputably degrading to a free society. . . . Since the early 1930's, intelligence agencies have frequently wiretapped and bugged American citizens without the benefit of judicial warrant. . . . There has been, in short, a clear and sustained failure by those responsible to control the intelligence community and to ensure its accountability.”

Intelligence Activities and the Rights of Americans (Vol. 2), FINAL REPORT OF THE SELECT COMMITTEE TO STUDY GOVERNMENT OPERATIONS WITH RESPECT TO INTELLIGENCE ACTIVITIES 5, 10, 15 (Apr. 26, 1976).

62. FISA was intended to address these concerns, Pub.L. No. 95-511, codified at 50 U.S.C. § 1801 et seq., and established a set of standards and procedures governing national security investigations – ones in which (at least after the standard was liberalized by the USA-PATRIOT Act of 2001) foreign intelligence gathering is a “significant purpose” of the investigation. 50 U.S.C. § 1804(a)(6)(B); § 1823(a)(7)(B). FISA also created the Foreign Intelligence Surveillance Court, a special court of federal district judges appointed by the Chief Justice who hear foreign intelligence surveillance order applications in secret, ex parte proceedings.
63. The Serwin Memorandum explains the remedies available under FISA at pp. 2-3. I am satisfied that its analysis is both complete and well-founded, and I agree with its conclusions. I will offer a few additional thoughts on these conclusions.
64. There are several causes of action for the unlawful use or disclosure of information obtained by a FISA surveillance order, which are laid out in the Serwin Memorandum. To this description I would add only three additional comments. First, these causes of action do not cover unlawful collection (although ECPA does regulate unlawful collection of electronic information generally). Second, in order to be actionable, an unlawful use or disclosure

(or for that matter, a collection) must be known, which can be a challenge when dealing with secret government electronic surveillance. This challenge is compounded by the fact that the Supreme Court has recognized in its standing doctrine cases (discussed below in Part III) that separation of powers considerations have led to a stricter application of standing requirements in the foreign affairs context. *Clapper v. Amnesty International*, 133 S.Ct. 1138, 1147 (2013). Third, the causes of action only apply to unlawful uses or disclosures that are “willful,” which is still an uncertain standard, despite the fact that the statutes have been on the books for years. Cf. Serwin Memorandum at p. 2 & n.7.

65. The expert reports adduced by Facebook in this case explain at length the sources of authority for US government surveillance of personal data of Europeans and the legal and policy safeguards that exist in the United States concerning this data. E.g., Vladeck Report at ¶¶54-78; Swire Report at Chapters 1, 3-5. In particular, they explain that while the scope and authority of NSA electronic surveillance is broad, there exist numerous limitations and safeguards under US law. For example, the Vladeck Report notes seven such constraints:

“Legal constraints on collection, including built-in limits and those required by the Fourth Amendment, Executive Order 12,333, and PPD-28;

Legal constraints on the use and retention of collected information, including built-in limits and those required by the Fourth Amendment, Executive Order 12,333, PPD-28, and federal statutes such as the Privacy Act;

Robust internal constraints on access to the collected data;

Internal oversight through agency Inspector General and Privacy and Civil Liberties Offices;

External oversight by the PCLOB;

External oversight by the House and Senate Intelligence and Judiciary Committees; and

Ex ante and ongoing judicial supervision through judicial review.”

Vladeck Report at ¶78

The Swire Report also goes into great detail regarding US privacy law. Swire Report at Chapters 1, 3-5. The Vladeck and Swire Reports thus provide substantial evidence to support their contention that US Government surveillance is not unconstrained, and exists within the rule of law. By contrast, the Gorski and Butler Reports acknowledge these legal structures but have a more pessimistic conclusion about the level of constraint they impose in practice. Gorski Report at ¶¶49-59; Butler Report at *passim*.

66. Given the scope of the opinion I have been asked to give in these Proceedings, I do not wish to wade into this debate in this Report because, in my opinion, this issue is complex, nuanced, but critically, it is not directly responsive to the question of remedies that I have been asked to address. Article 47 of the Charter guarantees European citizens a “right to an effective remedy before a tribunal[.]” In my mind, external and internal safeguards are a very important element of law in general and privacy law in particular, but (in US constitutional law at least) they are analytically distinct from fundamental rights.
67. There is one substantive observation, however, I would like to make about the safeguards which operate to constrain government surveillance in the United States. In their reports, professors Vladeck and Swire articulate and explain, in great detail, the various legal and policy safeguards that constrain surveillance by the US government. However, it is important to note that many of these safeguards are contingent on the discretion of the President of the United States or other officials in the Executive Branch. Thus, while I agree with Professors Vladeck and Swire that American surveillance law has become more privacy-protective since the Snowden Revelations of June 2013, many of these protections are merely administrative rules, and a significant portion of these are politically contingent and thus quite fragile. For example, the President must appoint and the Senate must confirm a new Chair of the Privacy and Civil Liberties Oversight Board who is committed to civil liberties (which was an unfilled position from 2007-13 and is currently once again empty after the its first chair, David Medine, stepped down in July 2016). The current or a future President also has the ability to amend, expand, or repeal executive orders such as Executive Order 12,333 and the Presidential Policy Directive 28. In the American system of government as (so I understand) in the European, fundamental rights are not fundamental if they are contingent on the discretion of elected officials. (See, in agreement, the Robertson Report at ¶¶29, 60). I am reminded of the conclusion of Chief Justice John Roberts in the Supreme Court’s most recent digital privacy case, in which he agreed that privacy-protective agency procedures by law enforcement were “[p]robably a good idea, but the Founders did not fight a revolution to gain the right to government agency protocols.” *Riley v. California*, 134 S.Ct. 2473, 2491 (2014). In that case, the Supreme Court went on to extend the protection of the Fourth Amendment – a true fundamental right – to the contents of mobile phones seized incident to arrest.

4. Other Potential Federal Causes of Action

68. The Serwin Memorandum discussed several other potential federal causes of action, including the Freedom of Information Act, 5 U.S.C. § 552; the Computer Fraud and Abuse Act, 18 U.S.C. § 1030; and the Right to Financial Privacy Act, 12 U.S.C. § 3401 et seq. I am satisfied that its analysis is both complete and well-founded, and I agree with its conclusions.

II. Standing Doctrine under the Law of the United States

69. In addition to the specific objection that remedies for privacy violations are “fragmented” under US law, the DPC Draft Decision noted a more general objection to relief under US law. As the DPC put it, “From a more general perspective, the “standing” admissibility requirements of the US federal courts operate as a constraint on all forms of relief available.” DPC Draft Decision at ¶45. In this section of my report, I want to explain what standing doctrine is, why it exists in US law, how it applies to privacy litigation, and also explain what I believe to be the effect of several recent privacy cases on the availability of relief for EU citizens who believe that their privacy and data protection rights have been violated by US security and/or intelligence agencies.
70. As I understand the DPC’s “general objection,” it is that Article 47 of the Charter requires that an effective remedy before a tribunal exists. Further, I understand that the DPC’s interpretation of European law is that because an individual remedy under US Law requires a plaintiff to satisfy the elements of standing doctrine, “these requirements appear to be incompatible with EU law in circumstances where, as a matter of EU law, it is not necessary to demonstrate an adverse consequence as a result of an interference with Articles 7 and 8 of the Charter in order to secure redress of a violation of the said articles. DPC Draft Decision at ¶54 (quoting *Schrems I*, ¶87 (“To establish the existence of an interference with the fundamental right to respect for private life, it does not matter whether the information in question relating to private life is sensitive or whether the persons concerned have suffered any adverse consequences on account of that interference.”))).
71. In the 2013 *Harvard Law Review* article (as noted above, published shortly before the Snowden disclosures of June of that year) about the dangers that unregulated and under-regulated government surveillance poses to democracy, I argued at the outset that, from an American perspective “[a]lthough we have laws that protect us against government surveillance,

secret government programs cannot be challenged until they are discovered. And even when they are, our law of surveillance provides only minimal protections. Courts frequently dismiss challenges to such programs for lack of standing, under the theory that mere surveillance creates no harms. The Supreme Court recently reversed the only major case to hold to the contrary, in *Clapper v. Amnesty International, USA*, finding that the respondents' claim that their communications were likely being monitored was 'too speculative.'" Neil M. Richards, *The Dangers of Surveillance*, 126 HARV. L. REV. 1934, 1934-35 (2013).

A. Basic Overview of Standing Doctrine

72. The US Constitution divides the legal power of the sovereign into three powers – legislative (the creation of law), executive (the execution and enforcement of law), and judicial (the adjudication and interpretation of law). The Constitution separates these powers by allocating each to a branch of government in the first three Articles of the Constitution. U.S. Const. Arts. I-III. Under American law, standing doctrine is one of a series of doctrines associated with the federal judicial power that are categorized under the heading of “justiciability.” This is an important corollary to (and limitation upon) the power of judicial review established in the foundational case of *Marbury v. Madison*, 5 U.S. (1 Cranch) 137 (1803).
73. Article III of the Constitution deals with the federal Judiciary. Section One provides that “The judicial Power of the United States, shall be vested in one supreme Court, and in such inferior Courts as the Congress may from time to time ordain and establish. The Judges, both of the supreme and inferior Courts, shall hold their Offices during good Behaviour, and shall, at stated Times, receive for their Services, a Compensation, which shall not be diminished during their Continuance in Office.” This vests the judicial power in a separate judiciary, and protects that judiciary’s independence by providing for judicial life tenure and guaranteed salary to protect the judges from political interference.
74. The second section of Article III begins by providing that “[t]he judicial Power shall extend to all Cases, in Law and Equity, arising under this Constitution, the Laws of the United States, and Treaties made, or which shall be made, under their Authority;—to all Cases affecting Ambassadors, other public ministers and Consuls;—to all Cases of admiralty and maritime Jurisdiction;—to Controversies to which the United States shall be a Party;—to Controversies between two or more States;—between a State and Citizens of another State;—between Citizens of different States;—between Citizens of the same State claiming Lands under Grants of different States,

and between a State, or the Citizens thereof, and foreign States, Citizens or Subjects.” U.S. CONST, ART III § 2.

75. In addition to standing, several other justiciability doctrines are derived from these provisions. These other doctrines include the prohibitions on advisory opinions and deciding “political questions,” as well as the doctrines of ripeness and mootness. These doctrines limit the ability of the federal courts to hear particular claims that are hypothetical, untimely or textually committed to the political process, and they are justified under a variety of theories, including the separation of powers, conservation of judicial resources, improving decision-making by limiting federal cases to ones in which adverse parties with a stake in the outcome are before the court, and the promotion of fairness by preventing the litigation of rights held by parties not before the court. See generally, ERWIN CHEMERINSKY, CONSTITUTIONAL LAW: PRINCIPLES AND POLICIES §2.3 (5th ed. 2015).
76. Standing doctrine is derived from the textual commitment in Art. III §2 of the judicial power to (and as interpreted only to) enumerated classes of “Cases” and “Controversies.” In order to ensure that a suit before the court presents a case and controversy and that the plaintiff has “standing” to bring a claim before the court that the court is able to adjudicate, the doctrine requires that the plaintiff establish three elements. In the absence of any one of these elements, the court lacks jurisdiction to entertain the claim because (so the logic goes) it would not be deciding a “case or controversy.” In his leading treatise on constitutional law, Dean Erwin Chemerinsky explains further:
- “The [Supreme] Court has said that some of these requirements are constitutional; that is, they are derived from the Court’s interpretation of Article III and as constitutional restrictions they cannot be overridden by statute. Specifically, the Supreme Court has identified three constitutional standing requirements. First, the plaintiff must allege that he or she has suffered or imminently will suffer an injury. Second, the plaintiff must allege that the injury is fairly traceable to the defendant’s conduct. Third, the plaintiff must allege that a favorable federal court decision is likely to redress the injury.”
- ERWIN CHEMERINSKY, CONSTITUTIONAL LAW: PRINCIPLES AND POLICIES §2.5 (5th ed. 2015).
77. These three constitutional standing requirements – injury in fact, causation, and redressability – are reflected in the DPC Draft Decision ¶53.

78. I must explain at the outset that beyond stating this three-part test, identifying coherent principles that run through the American law of standing can be very difficult. The doctrine is frequently confusing and indeterminate and open to charges that the Justices (and lower court judges) are in practice if not in intent manipulating what is supposed to be a procedural doctrine in order to affect the substantive merits of legal disputes. Dean Chemerinsky explains this charge in greater detail:

“Standing frequently has been identified by both justices and commentators as one of the most confused areas of the law. Professor Vining wrote that it is impossible to read the standing decisions ‘without coming away with a sense of intellectual crisis. Judicial behavior is erratic, even bizarre. The opinions and justifications do not illuminate.’ Thus, it is hardly surprising that standing has been the topic of extensive academic scholarship and that the doctrines are frequently attacked. Many factors account for the seeming incoherence of the law of standing. The requirements for standing have changed greatly in the past 40 years as the Court has formulated new standing requirements and reformulated old ones. The Court has not consistently articulated a test for standing; different opinions have announced varying formulations for the requirements for standing in federal court. Moreover, many commentators believe that the Court has manipulated standing rules based on views of the merits of particular cases.”

ERWIN CHEMERINSKY, *CONSTITUTIONAL LAW: PRINCIPLES AND POLICIES* §2.5 (5th ed. 2015).

79. In making this observation (and quoting Prof. Chemerinsky), I am not attempting to suggest that standing doctrine is incoherent (though, to be fair, a substantial number of critics of the doctrine do believe this). My point is merely that, beyond the broad conceptual outlines of the doctrine, the standing cases in privacy law as elsewhere in American law can be difficult to predict or restate. This is as much a challenge for litigants presenting claims that push near the boundaries of the doctrines as it is for academics, practicing attorneys, and judges who seek to understand or apply it.

B. Standing Doctrine in Privacy Cases

80. Standing doctrine frequently implicates cases that bring claims in which the legal wrong sought to be remedied is new or involves a remedy for intangible harm, particularly where the harm alleged departs from traditional common law notions of physical or pecuniary harm. It is thus no surprise that earlier

leading privacy cases drew heavily from environmental law and cases raising theories of environmental or aesthetic harm with complex causation, e.g., *Lujan v. Defenders of Wildlife*, 504 U.S. 555 (1992); *Massachusetts v. EPA*, 549 U.S. 497 (2007), while newer ones seem to increasingly involve privacy law, with their emphasis on psychological or dignitary injuries.

81. In lower court litigation across the field of privacy law, litigation of “privacy harm” is an important issue, and numerous privacy claims have been dismissed for want of standing. As Professor McGeveran puts it well discussing class action litigation against private companies, “developments in privacy law, particularly standing doctrine, have also increased the obstacles to private suits, including class actions.” MCGEVERAN at 199. To be sure, standing doctrine is not a complete obstacle – McGeveran notes that “privacy class action suits will remain a significant legal threat to companies for the foreseeable future,” *id.*, but standing doctrine remains a real obstacle to privacy litigation by plaintiffs across the board in the United States, whether they are suing companies or the government. Professors Solove and Schwartz seem to concur with this assessment, see, e.g., SOLOVE & SCHWARTZ at 811, 967, as do I.
82. Two recent Supreme Court standing cases have involved privacy claims, and are worthy of closer examination. In *Clapper v. Amnesty International*, 133 S.Ct. 1138 (2013), lawyers, journalists, and human rights activists who spoke frequently with non-US clients and contacts about sensitive topics brought a challenge to Section 702 of FISA. The plaintiffs argued that section 702 harmed them by violating their First and Fourth Amendment rights. The plaintiffs argued that because their communications were with people that the government considered suspicious, they reasonably believed that those communications were being monitored. They also claimed that in order to protect their privacy and other fundamental rights, they had spent substantial amounts of both time and money, including traveling out of the United States to speak with their clients rather than using telephones or emails that the government was likely monitoring. *Id.* at 1145-46. Nevertheless, a majority of the Supreme Court dismissed their claim on standing grounds under the first prong of the analysis for failure to allege a constitutionally-sufficient injury in fact. After explaining the “cases and controversies” requirement that is rooted in the separation of powers, and noting that “we have often found a lack of standing in cases in which the Judiciary has been requested to review actions of the political branches in the fields of intelligence gathering and foreign affairs,” *id.* at 1147, the Court explained the governing test:

“To establish Article III standing, an injury must be ‘concrete, particularized, and actual or imminent; fairly traceable to the challenged action; and redressable by a favorable ruling. Although imminence is concededly a somewhat elastic concept, it cannot be stretched beyond its purpose, which is to ensure that the alleged injury is not too speculative for Article III purposes—that the injury is certainly impending. Thus, we have repeatedly reiterated that threatened injury must be certainly impending to constitute ‘injury in fact,’ and that [a]llegations of possible future injury are not sufficient.” *Id.* (citations and quotations omitted).

83. Applying this test, the Court concluded that the plaintiffs had not alleged a constitutionally-sufficient injury because it was speculative about whether the government would “imminently target” their communications under section 702, they had no actual knowledge of the government’s targeting practices, and that even if their being targeted was imminent, they could not prove that the targeting was being authorized by Section 702 (which they were challenging), rather than another of the various methods of government surveillance (which they were not). *Id.* at 1148-49. The Court also rejected the plaintiffs’ alternative argument that they had incurred costs to avoid surveillance on the ground that they could not “manufacture standing merely by inflicting harm on themselves based on their fears of hypothetical future harm that is not certainly impending. Any ongoing injuries that respondents are suffering are not fairly traceable to § [702].” *Id.* at 1151. Because their injuries were thus neither “imminent” nor “fairly traceable” to section 702, they lacked an injury in fact that could be redressed by a favourable ruling and thus standing to challenge the government’s surveillance programme.
84. One of the great ironies about *Clapper* is that much of the speculation about the government’s targeting practices could have been resolved if the government had disclosed (including confidentially to the Court) whether the plaintiffs’ communications were being monitored, and what targeting or minimization procedures were being used. See Neil M. Richards, *The Dangers of Surveillance*, 126 HARV. L. REV. 1934, 1944 (2013). This suggestion was actually made to the Court at oral argument, but the Court rejected it in its opinion on what were apparently national security grounds. The Court explained that “it is not the Government’s burden to disprove standing by revealing details of its surveillance priorities. Moreover, this type of hypothetical disclosure proceeding would allow a terrorist (or his attorney) to determine whether he is currently under U.S. surveillance simply by filing a lawsuit challenging the Government’s surveillance program. Even if the terrorist’s attorney were to comply with a protective

order prohibiting him from sharing the Government’s disclosures with his client, the court’s post-disclosure decision about whether to dismiss the suit for lack of standing would surely signal to the terrorist whether his name was on the list of surveillance targets.” *Id.* at 1149 n. 4.

85. The second recent Supreme Court decision to discuss standing doctrine in the privacy context is one decided this past summer, *Spokeo v. Robins*, 136 S.Ct. 1550 (2016). *Spokeo* involved a claim made by a consumer that a data broker had violated the Fair Credit Reporting Act of 1970, 15 U.S.C. § 1681 et seq., a federal consumer protection statute that imposes a data protection regime on consumer reporting agencies. The plaintiff consumer alleged that the data broker had reported false information about him, but the data broker had countered that because the false information was favourable to the consumer, there was no injury and thus no standing to sue. The Supreme Court held for the data broker on standing grounds – specifically under the rationale that the consumer had failed to allege an injury in fact that was both “concrete” and “particularized.” The Court explained that “[f]or an injury to be ‘particularized,’ it must affect the plaintiff in a personal and individual way. Particularization is necessary to establish injury in fact, but it is not sufficient. An injury in fact must also be concrete.... A ‘concrete’ injury must be ‘de facto’; that is, it must actually exist. When we have used the adjective ‘concrete,’ we have meant to convey the usual meaning of the term—‘real,’ and not ‘abstract.’ Concreteness, therefore, is quite different from particularization.” *Id.* at 1548 (citations and some quotations omitted).
86. The Court in *Spokeo* went on to explain what it meant by the concept of “concreteness.” In somewhat confusing language, it explained that

“‘Concrete’ is not, however, necessarily synonymous with ‘tangible.’ Although tangible injuries are perhaps easier to recognize, we have confirmed in many of our previous cases that intangible injuries can nevertheless be concrete. In determining whether an intangible harm constitutes injury in fact, both history and the judgment of Congress play important roles. Because the doctrine of standing derives from the case-or-controversy requirement, and because that requirement in turn is grounded in historical practice, it is instructive to consider whether an alleged intangible harm has a close relationship to a harm that has traditionally been regarded as providing a basis for a lawsuit in English or American courts. In addition, because Congress is well positioned to identify intangible harms that meet minimum Article III requirements, its judgment is also instructive and important. Thus, we said in *Lujan* that Congress may ‘elevat[e] to the status of legally cognizable injuries concrete, de facto injuries that were previously

inadequate in law.’ Similarly, Justice Kennedy’s concurrence in that case explained that ‘Congress has the power to define injuries and articulate chains of causation that will give rise to a case or controversy where none existed before.’” *Id.* at 1149 (citations omitted).

87. Applying these new principles to the case at hand, the Court held that to satisfy the constitutional minimum of standing, plaintiffs must have suffered concrete harm and not a “bare procedural violation,” which would be constitutionally insufficient to allow a remedy. As the Court explained,

“In the context of this particular case, these general principles tell us two things: On the one hand, Congress plainly sought to curb the dissemination of false information by adopting procedures designed to decrease that risk. On the other hand, Robins cannot satisfy the demands of Article III by alleging a bare procedural violation. A violation of one of the FCRA’s procedural requirements may result in no harm. For example, even if a consumer reporting agency fails to provide the required notice to a user of the agency’s consumer information, that information regardless may be entirely accurate. In addition, not all inaccuracies cause harm or present any material risk of harm. An example that comes readily to mind is an incorrect zip code. It is difficult to imagine how the dissemination of an incorrect zip code, without more, could work any concrete harm.” *Id.* at 1550.

88. *Spokeo* certainly made standing doctrine stricter in general, especially in privacy cases, yet it was actually greeted with relief by some advocates and academics among the US privacy community. One of the great fears in the community was that there was a substantial risk that the Supreme Court might hold not only that Robins (the plaintiff in that case) would lose, but more broadly that standing doctrine might be interpreted to substantially limit the ability of Congress to authorize private rights of action to remedy privacy wrongs. Because of this fear, several leading privacy law scholars (including myself) filed an *amicus curiae* brief in the Supreme Court. Our brief did not take a position on Mr. Robins’ narrow dispute with *Spokeo*, but addressed instead what we saw as the real threat to privacy law that the case presented, the risk that privacy causes of action might get limited through standing doctrine across the board in ways analogous to the way the Supreme Court recently read the Privacy Act “actual damages” requirement so narrowly in *FAA v. Cooper*, 132 S.Ct. 1441 (2012). In our brief, we argued that the federal Fair Credit Reporting Act’s procedures were important to the integrity of the consumer credit system, and that more generally, the private rights of action in the FCRA and other statutes were an important part of protecting consumers and their information. I can recall teaching

privacy law while the case was pending last year, and having to repeatedly tell my students that significant chunks of the course material might be rendered unconstitutional if the Court accepted all of Spokeo's arguments in that case. As a result, when the Supreme Court returned only a modest judgment for Spokeo, many privacy scholars were pleased that the Supreme Court had not gutted (figuratively speaking) US privacy law. But the case shows how close the Supreme Court could have come to placing even more substantial obstacles in the path of plaintiffs seeking redress for nonpecuniary privacy harms under American law. And the fact that even a further, modest tightening of standing rules for privacy plaintiffs was considered something of a victory shows how substantial an obstacle standing doctrine really is to plaintiffs under US law.

89. Perhaps because it did not originate in the national security context, I note that the other expert reports in this case have not really addressed *Spokeo*. (I believe that neither the Swire nor Vladeck reports even cite the case, for example). However, because standing doctrine applies to every lawsuit brought before a federal court, the Court's tightening of standing doctrine in *Spokeo* to make the concreteness requirement stricter and to forbid Congress authorizing "bare procedural violations" through private rights of action represents a higher obstacle for US privacy plaintiffs in general, whether they seek redress against companies, the government, or both.
90. Where do these developments in standing law leave privacy litigation in the United States? As explained previously, the classic definition of injury in fact under American standing doctrine is that an injury must be both (1) "concrete and particularized" as well as (2) "actual and imminent, not conjectural and hypothetical." *Lujan v. Defenders of Wildlife*, 504 U.S. 555 (1992). The two most recent Supreme Court privacy standing cases make each of these requirements more difficult for claimants to satisfy. In *Clapper*, the Court tightened up the "actual and imminent" prong in a surveillance case in which there may have been an injury to fundamental civil liberties, but the government was not required to tell, while in *Spokeo*, the Court tightened up the "concrete and particularized" prong in a data protection case involving the processing of personal data, which rejected "procedural violations" as being adequate to support a remedy in the absence of demonstrable injury. As noted, *Spokeo* also seems to reject Congress's ability to authorize private rights of action that remedy a "bare procedural violation" of privacy or data protection standards. From this perspective, the DPC's conclusion that standing doctrine represents a general obstacle to data protection claims brought by EU citizens seems eminently correct, DPC Draft Opinion at ¶55, particularly where (as I understand it), the *Schrems I* court seems to allow a substantially lower threshold for a remediable injury

than US standing doctrine does. DPC Draft Opinion at ¶30 (quoting *Schrems I* at ¶87).

91. The Vladeck Report acknowledges that the *Clapper* decision is substantively unsatisfying, but it suggests that the DPC Draft opinion “errs” in concluding that “US law thereby requires a claimant ‘to demonstrate that a harm has in fact been suffered as a result of the interference alleged.’” Vladeck Report at ¶90 (quoting DPC Draft Opinion at ¶55). I do not agree with this critique. In my opinion, the DPC Draft Opinion correctly states this basic principle of standing law – that the Constitution requires each federal court plaintiff to demonstrate that an *injury in fact* (harm) has been suffered that was *caused* by the defendant and which can be *redressed* by a favourable decision of the court. Moreover, in the case of a privacy violation, the *Spokeo* decision makes clear that not all regulatory ‘harms’ will satisfy the constitutional minimum. *Spokeo* requires that injuries must be concrete, which in that case meant more than a “bare procedural violation.” *Spokeo*, 135 S.Ct. at 1550.
92. The Vladeck Report also cites a number of lower court cases subsequent to *Spokeo* to suggest that “[g]iven how much more is publicly known today about U.S. government surveillance authorities—especially Section 702 of FISA—it seems far more likely that an EU citizen could demonstrate a ‘substantial risk’ that his communications will be unlawfully collected by the U.S. government today than it would have appeared to the Supreme Court in *Clapper*.” Vladeck Report at ¶93. I sincerely hope that he is correct about this, but this conclusion is merely speculative. Those cases are in any event factually distinguishable,⁴ and are of course not binding on the Supreme Court.⁵
93. The Vladeck Report notes further on this point that some lower court cases have rejected challenges to standing, but concludes that

“As these cases illustrate, there is significant uncertainty in the lower courts over exactly when *Clapper* does and does not foreclose standing,

⁴ For example, though I agree that the Second Circuit’s finding of standing in *ACLU v. Clapper*, 785 F.3d 787 (2015), was correctly decided, that was a bulk collection case that avoided the problem of speculative harm identified in the Supreme Court’s *Clapper v. Amnesty International* case because there was no speculation about whether the plaintiffs were being spied on, since the section 215 bulk collection was targeting essentially everyone. *ACLU v. Clapper*, 785 F.3d at 801.

⁵ Both *Clapper* decisions in the Court of Appeals were authored not only by the same appellate court – the New York-based United States Court of Appeals for the Second Circuit, but both Second Circuit opinions were written by the same judge, Judge Gerard E. Lynch.

and I do not mean to suggest otherwise. The critical point for present purposes is that this uncertainty is not nearly as categorically hostile to standing as suggested in the DPC Draft Decision, and instead is more reflective of the case-specific vagaries of individual lawsuits. Thus, based on the cases surveyed above, it is my view that, where EU citizens can marshal plausible grounds from which it is reasonable to believe that the U.S. government has collected, will collect, and/or is maintaining, records relating to them in a government database, they will likely have standing to sue even in light of the Supreme Court's *Clapper* decision."

Vladeck Report at ¶¶ 94-95. I would agree that there is great uncertainty on this point in the US Courts, but my reading of the DPC Draft Decision is slightly different. I understand the DPC to have concluded that standing law is a general obstacle to EU citizens bringing suit, and that "[o]n their terms, I consider that these requirements appear to be incompatible with EU law in circumstances where, as a matter of EU law, it is not necessary to demonstrate an adverse consequence as a result of an interference with Articles 7 and 8 of the Charter in order to secure redress of a violation of the said Articles." DPC Draft Decision at ¶54. In my opinion, the DPC is correct that standing is a general obstacle to all litigants, and particularly correct that American standing doctrine's injury in fact requirement always requires the demonstration of actual injury, particularly since *Spokeo*'s strengthening of the concreteness requirement eliminates the possibility that "bare procedural violations" can produce the requisite level of constitutional injury.

94. On the subject of lower-court cases, the Gorski report notes the ACLU's litigation representing a group of human rights and educational groups (including Wikimedia, which runs the Wikipedia online encyclopedia) challenging Section 702 "Upstream" surveillance, and how that case was dismissed in district court under the Supreme Court decision in *Clapper*. See *Wikimedia v. NSA*, 143 F.Supp.3d 344, 356 (D.Md 2015). I should note that I joined a brief with other First Amendment Law Professors seeking to have the dismissal overturned on appeal. I agree with Ms. Gorski both in the hope that this ruling will be reversed on appeal, and that (in her words) "the district court's opinion illustrates the difficulties that plaintiffs face in establishing standing, even at the outset of a case, when a plaintiff's allegations must merely be plausible." Gorski Report at ¶54. I would amplify this point by noting that if these difficulties are substantial for one of the world's most popular websites represented by the most famous civil liberties group in the world, they would likely be even more pronounced for ordinary EU citizens.

95. The Vladeck Report also takes issue with the Serwin Memorandum's discussion of Rule 11 of the Federal Rules of Civil Procedure. See Vladeck Report at ¶96; Serwin Memorandum at pp. 16-17. As the Vladeck Report explains, Rule 11 is a requirement in all civil litigation before federal courts requiring essentially that litigants filing motions before the court are not engaged in frivolous or vexatious litigation. I do not see a material difference between the Vladeck Report and the Serwin Memorandum on this point. The DPC Draft Decision does conclude with the statement that "[t]aken with the analysis adopted by the Court in *Clapper* in connection with the making of 'speculative' claims regarding alleged violations of data privacy rights, the Federal Rules of Procedure would appear to preclude the bringing of precisely the kind of complaint now before me." DPC Draft Decision at ¶56. Professor Vladeck is correct that Rule 11 does not preclude claims, but rather authorizes sanctions on the abuse of process. Insofar as the statement in the DPC's Draft Decision might be interpreted in isolation as suggesting that Rule 11 would preclude bringing a speculative claim identical to the one rejected in *Clapper*, such an interpretation of US law would not be correct. However, I do not believe that this is the best way to read the DPC Draft Decision's interpretation of US law. On the contrary, when one reads ¶56 of the DPC Draft Opinion in connection with the preceding ¶55, the DPC's conclusion seems to be different and correct as a matter of US law. Under this reading, substantive standing doctrine can operate to bar speculative claims alleging unlawful surveillance. On balance, I think that this latter reading is a more faithful reading of the DPC Draft Decision. Moreover, I could envision that a claim that is more "speculative" than *Clapper* could not only be barred by the developments in the recent privacy law standing cases, but could also run the risk of Rule 11 sanctions as well. In any event, even if this statement by the DPC could fairly be said to be erroneous, it would be at most a misreading of Serwin that I do not see as undermining the DPC's overall US law argument under Article 47 of the Charter as to US standing doctrine.
96. The Swire Report also considers the issue of standing. Swire Report pp. 7-38 to 7-40. Professor Swire agrees with the DPC's conclusion to the extent that standing is a generally-applicable requirement for all litigants in federal court, but notes that *Clapper* "should not, however, be read to create a *per se* ban on cases involving US foreign intelligence or counterterrorism programs," citing lower court cases that have found litigants with standing to challenge other surveillance programmes. Swire Report at 7-39 ¶88 (citing *ACLU v. Clapper*, 785 F.3d 787, 801 (2d Cir. 2015) (finding that standing existed to challenge the Section 215 metadata programme where the bulk collection necessarily included plaintiffs' phone records); *Klayman v.*

Obama, 142 F.Supp.3d 172, 186 (D.D.C. 2015) (same); *Shearson v. Holder*, 725 F.3d 588, 593 (6th Cir. 2013) (holding that individual had standing to challenge her suspected placement on the terrorist watch list, even though the court found “it is impossible for [her] to prove that her name remains on that list,” but where she had proven indicia of being on the watch list). It is both correct and encouraging that lower Courts after *Clapper* have allowed civil liberties challenges to surveillance to go forward. However, as I understand both the Swire Report and the DPC Draft Opinion, there is no disagreement that standing is an obstacle to relief, particularly where there is no injury in fact. Under EU law as I understand it, particularly as the CJEU interpreted Article 47 in *Schrems I*, a stringent requirement of injury-in-fact akin to that required by the US Supreme Court in *Clapper* and *Spokeo* is not always required. This could represent a bar to a significant chunk of such claims by EU citizens that US law would leave unredressed. This barrier seems higher, as the *Clapper* court noted, in national security cases. And it also would now have to satisfy the more stringent “concreteness” requirement for injuries in fact after *Spokeo*. Thus, while standing doctrine is not a complete bar to relief in surveillance cases, it is still frequently a substantial and frequently unsatisfying one (see Vladeck Report at ¶90). I agree here with scholarly work by Professor Vladeck in which he has argued that “perhaps the most important takeaway from [*Clapper*] is the extent to which the Supreme Court’s Article III standing jurisprudence interposes substantial obstacles to judicial review of secret surveillance programs (if not all secret government conduct) on the merits.” Stephen I. Vladeck, *Standing and Secret Surveillance*, 10 I/S: J. L. & POL. FOR INFO. SOC. 551, 565-66 (2014). Moreover, this is also how I read (and concur with) the DPC Draft Decision’s findings on US law – that standing doctrine is a general obstacle to relief of this sort that, while not necessarily fatal, is nevertheless substantial and jurisdictional.

97. In conclusion regarding the potential remedies, it is my opinion that EU citizens seeking legal relief to remedy violations of their data protection and privacy rights in the US face substantial obstacles at the specific level of causes of action, and at the general levels of standing doctrine and the practical difficulties in learning about surveillance in the first place.
98. The other four experts on US law who have filed reports in these Proceedings also take positions on this question. The Swire Report is quite optimistic about the availability of remedies in US legal proceedings. It

argues that the “fragmentation” of US remedies is not a vice but rather a virtue, and explains that there is a lot of substance to US privacy law, contrary to the belief of some foreign observers. Swire Report at p. 7-1. The Swire report offers five categories of remedies for privacy violations under US law – (1) judicial remedies against the government, including laws regulating violations of privacy laws by individuals, (2) non-judicial remedies available against US government surveillance, (3) individual remedies against US companies, (4) privacy enforcement under US state law, and (5) standing. Swire Report at p. 7-2.

99. I agree with the Swire Report that the US does have real privacy law, and that there is a lot of it. However, the fact that US privacy law is substantial is not directly responsive, in my opinion, to the questions I have been asked to address in this report, such as the availability of judicial remedies to EU citizens who wish to challenge unlawful data processing by the US government once their data has been transferred to the US. From the perspective of that question, of the five categories of law described in the Swire Report, only part of category (1) and category (5) are relevant, as they are the only ones that bear on legal redress against the United States government for surveillance that violates EU fundamental rights. With respect to category (2), non-judicial remedies are by definition non-judicial. Category (3) remedies against companies are not remedies against the government. And privacy enforcement under US state law, though it has been overlooked by many until recently, does not provide redress against the national government. As for category (5), I have already explained at length above why I believe that standing doctrine is a substantial obstacle, and I will not repeat that discussion here.
100. This leaves category (1), which are “US Civil Judicial Remedies.” In this category, the Swire Report includes some other remedies, such as those under the “Umbrella Agreement,” the Privacy Shield Ombudsperson mechanism, standard contractual clauses, and Privacy Shield alternative dispute resolution. I respectfully disagree that these are judicial remedies, though I address the potential and limitations of the Ombudsperson mechanism in Part III, below. With respect to Privacy Shield alternative dispute resolution, which is separate from the Ombudsperson mechanism, I do not see how a civil arbitration scheme between a company and its customers could provide relief for government privacy violations. Finally, Litigation under the standard contractual clauses is a judicial remedy, but I also do not see how it could provide relief for government privacy violations.
101. The Swire Report also discusses under category (1) “US Criminal Judicial Remedies” brought by the US Department of Justice against people

(including government officials) who violate ECPA, FISA, and the Privacy Act. Swire Report at p. 7-10. These criminal prosecutions could not of course be brought by EU citizens, and although they could certainly punish people who have violated federal privacy law, to my mind this is not the same as the redress of a violation of a fundamental right. The Swire Report does discuss under category (1) the Privacy Act/Judicial Redress Act, the Electronic Communications Privacy Act, and FISA. I have already discussed these causes of action and some of their specific limitations above.

102. In contrast to the Swire Report, the Gorski and Butler Reports are more pessimistic as to remedies. The Butler Report explains that “EU citizens whose personal data has been transferred to the U.S. have limited remedies available where their claims arise from access to, use of, or dissemination of their private communications or other personal data.... None of these statutory remedies provide a means of redress for bulk surveillance conducted under Section 702 or EO 12333.” Butler Report at ¶61. The Gorski report goes further, concluding that “U.S. Surveillance law is extremely permissive, as the government claims broad authority to acquire the communications and data of non-U.S. persons located abroad. For the vast majority of individuals subject to Section 702 and EO 12333 surveillance, there has to date been no viable avenue to obtain meaningful redress for the rights violations resulting from this surveillance.” Gorski Report at ¶64. Indeed, earlier in her report, Ms. Gorski explains that due to the obstacles facing litigants, “no civil lawsuit challenging Section 702 or EO 12333 surveillance has ever produced a U.S. court decision addressing the lawfulness of that surveillance.” Gorski Report at ¶56.
103. In between these positions is the Vladek Report, which concedes some of the objections raised by the DPC Draft Report, as well as some of those raised by the Gorski Report, the Butler Report, and the Serwin Memorandum – many of which I have already discussed in this Report. At two points in his report, Professor Vladek notes that relief is problematic, but then argues that it is not as problematic as the other opinions on this question (with the exception of Prof. Swire) conclude. At paragraph 98 of his Report, he states that “although there *are* shortcomings in the existing U.S. legal regime with regard to redress of unlawful government data collection, I do not believe that they are nearly as comprehensive —or that standing is as categorical an obstacle—as the DPC Draft Decision or the [Serwin] Memo suggest.” At paragraph 103 of his Report, he concludes that in his opinion the DPC Draft Decision’s assessment of current U.S. remedies for unlawful collection of EU citizens’ data from U.S. companies is significantly incomplete, that its analysis of the obstacles posed by “standing” doctrine is substantially overstated....”

104. It is my expert opinion that the DPC Draft Decision does not significantly overstate the specific or general difficulties faced by EU citizens seeking relief for violations of their EU fundamental privacy and data protection rights in US courts. For the reasons given in this report, I thus respectfully disagree with Professors Swire and Vladeck on this point, and agree with the ultimate conclusions to the contrary on this point reached by the Serwin Memorandum, the Gorski Report, the Butler Report, and the DPC Draft Decision.

III. THE PRIVACY SHIELD FRAMEWORK

105. The Privacy Shield Framework is a recently-negotiated agreement designed to replace the Safe Harbour Agreement invalidated by the CJEU in the *Schrems* case. After negotiations between the government of the US, the European Commission, and other interested parties, the European Commission issued a decision on 12 July 2016 providing a derogation for adequate processing of personal data pursuant to Article 25 of the EU Data Protection Directive for US companies that satisfy the “Privacy Shield” requirements and follow its rules. Commission Implementing Decision of 12.7.2016, pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-US Privacy Shield (2016) (“Commission Implementing Decision of 12.7.2016.”)
106. Under the Privacy Shield Framework, as under the predecessor Safe Harbour Agreement, US companies can self-certify online to the Department of Commerce and publicly commit to adhere to and comply with the Framework’s requirements. U.S. Department of Commerce, Privacy Shield Overview, available at <https://www.privacyshield.gov/Program-Overview>.
107. The Privacy Shield Principles, like the predecessor Safe Harbour principles, are derived from Fair Information Practice Principles (FIPPs) common throughout international privacy law. They are the *Notice Principle*, the *Data Integrity and Purpose Limitation Principle*, the *Choice Principle*, the *Security Principle*, the *Access Principle*, the *Accountability for Onward Transfer Principle*, and the *Recourse, Enforcement and Liability Principle*. Commission Implementing Decision of 12.7.2016, at ¶¶19-29.
108. The *Recourse, Enforcement and Liability Principle* requires organizations under the Privacy Shield Framework to provide recourse (including an effective remedy) to the individuals whose data they hold under the framework in cases of non-compliance with the other principles. The Commission Implementing Decision envisions seven different possible

sources of recourse for such individuals. First, they can pursue cases of non-compliance directly with the company that is self-certified to the Privacy Shield Framework. Second, they can bring a complaint to a company-designated “independent dispute resolution body. Third, they can bring their complaint to their national Data Protection Authority. Fourth, they can bring complaints to the US Department of Commerce. Fifth, companies that self-certify to the Privacy Shield Framework must also be subject to the Federal Trade Commission’s investigatory and enforcement powers, including the ability to obtain consent decrees in cases of alleged unfair and deceptive trade practices. Sixth, there is the availability of binding arbitration by a “Privacy Shield Panel” of arbitrators constituted under the Framework. Seventh, there is always the possibility of individuals bringing legal claims under US state law. Commission Implementing Decision of 12.7.2016, at ¶¶38-60.

109. Based upon the seven possible avenues of redress against Privacy Shield self-certifying companies, the European Commission found in its implementing decision that “that the Principles issued by the U.S. Department of Commerce as such ensure a level of protection of personal data that is essentially equivalent to the one guaranteed by the substantive basic principles laid down in Directive 95/46/EC.” Commission Implementing Decision of 12.7.2016, at ¶61.
110. Nevertheless, because the adequacy of Safe Harbor was invalidated in *Schrems I* on the basis of access to EU personal data held in the US by the US government, the Commission considered the state of US surveillance law in light of the reforms that have been implemented in the wake of the Snowden revelations of June 2013. In negotiations with the US government, the Commission received detailed submissions from the US government about its collection programmes and limitations. It also received a commitment by the US government to create a new “Privacy Shield Ombudsperson,” to be housed in the Department of State. Commission Implementing Decision of 12.7.2016, at ¶65. U.S. Dept. of State, EU - U.S. Privacy Shield Ombudsperson, <http://www.state.gov/e/privacyshield/ombud/index.htm>.
111. The role of the Ombudsperson is set out in a letter (“the Kerry Letter”) from the US Secretary of State to the European Commission, which was considered by the Commission in its adequacy determinations for the Privacy Shield. In the letter, Secretary of State John F. Kerry designated Under Secretary of State Catherine Novelli, the Under Secretary of States for Economic Growth, Energy, and the Environment, to serve as the

Ombudsperson. He also stated that “Under Secretary Novelli is independent from the U.S. intelligence community, and reports directly to me.” Letter from U.S. Secretary of State John Kerry to the European Commission, July 7, 2016, available at Commission Implementing Decision of 12.7.2016, at Annex III.

112. The Kerry Letter sets out the Ombudsperson mechanism in a six-page Memorandum, which was attached to the Letter as Annex A. This memorandum described the Ombudsperson’s role as follows:

1. The Privacy Shield Ombudsperson. The Senior Coordinator will serve as the Privacy Shield Ombudsperson and designate additional State Department officials, as appropriate to assist in her performance of the responsibilities detailed in this memorandum. [] The Privacy Shield Ombudsperson will work closely with appropriate officials from other departments and agencies who are responsible for processing requests in accordance with applicable United States law and policy. The Ombudsperson is independent from the Intelligence Community. The Ombudsperson reports directly to the Secretary of State who will ensure that the Ombudsperson carries out its function objectively and free from improper influence that is liable to have an effect on the response to be provided.

2. 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.

a. The Privacy Shield Ombudsperson will work closely with other United States Government officials, including appropriate independent oversight bodies, to ensure that completed requests are processed and resolved in accordance with applicable laws and policies. In particular, the Privacy Shield Ombudsperson will be able to coordinate closely with the Office of the Director of National Intelligence, the Department of Justice, and other departments and agencies involved in United States national security as appropriate, and Inspectors General, Freedom of

Information Act Officers, and Civil Liberties and Privacy Officers.

b. The United States Government will rely on mechanisms for coordinating and overseeing national security matters across departments and agencies to help ensure that the Privacy Shield Ombudsperson is able to respond within the meaning of Section 4(e) to completed requests under Section 3(b).

c. The Privacy Shield Ombudsperson may refer matters related to requests to the Privacy and Civil Liberties Oversight Board for its consideration.

Annex A, Letter from U.S. Secretary of State John Kerry to the European Commission, July 7, 2016, available at Commission Implementing Decision of 12.7.2016, at Annex III.

113. The Kerry Letter also provides a mechanism by which EU citizens can submit requests to the Ombudsperson via their National Data Protection Authorities, and through the DPAs to an “EU Individual Complaint Handling Body” that will verify and standardize requests to the Ombudsperson.
114. Notably, in a departure from the standing requirements that apply to private litigants in US federal courts, the Kerry Letter provides that “To be completed for purposes of further handling by the Privacy Shield Ombudsperson under this memorandum, the request need not demonstrate that the requester’s data has in fact been accessed by the United States Government through signal intelligence activities.”
115. The Kerry Letter also provides a procedure for the Ombudsperson’s investigation. The Ombudsperson is required to acknowledge receipt of the request to the “EU Individual Complaint Handling Body,” and conduct an initial review to ensure completeness of the request and see if more information is needed from the “EU Individual Complaint Handling Body,” including having it contact the complaining individual. The Kerry Letter then provides three additional requirements:
- “e. Once a request has been completed as described in Section 3 of this Memorandum, the Privacy Shield Ombudsperson will provide in a timely manner an appropriate response to the submitting EU individual complaint handling body, subject to the continuing obligation to protect information under applicable laws and policies.

The Privacy Shield Ombudsperson will provide a response to the submitting EU individual complaint handling body confirming (i) that the complaint has been properly investigated, and (ii) that the U.S. law, statutes, executives [sic] orders, presidential directives, and agency policies, providing the limitations and safeguards described in the ODNI letter, have been complied with, or, in the event of non-compliance, such non-compliance has been remedied. The Privacy Shield Ombudsperson will neither confirm nor deny whether the individual has been the target of surveillance nor will the Privacy Shield Ombudsperson confirm the specific remedy that was applied. As further explained in Section 5, FOIA requests will be processed as provided under that statute and applicable regulations.

f. The Privacy Shield Ombudsperson will communicate directly with the EU individual complaint handling body, who will in turn be responsible for communicating with the individual submitting the request. If direct communications are part of one of the underlying processes described below, then those communications will take place in accordance with existing procedures.

g. Commitments in this Memorandum will not apply to general claims that the EU-U.S. Privacy Shield is inconsistent with European Union data protection requirements. The commitments in this Memorandum are made based on the common understanding by the European Commission and the U.S. government that given the scope of commitments under this mechanism, there may be resource constraints that arise, including with respect to Freedom of Information Act (FOIA) requests. Should the carrying-out of the Privacy Shield Ombudsperson's functions exceed reasonable resource constraints and impede the fulfillment of these commitments, the U.S. government will discuss with the European Commission any adjustments that may be appropriate to address the situation.”

Annex A, Letter from U.S. Secretary of State John Kerry to the European Commission, July 7, 2016, available at Commission Implementing Decision of 12.7.2016, at Annex III.

116. Finally, the Privacy Shield Ombudsperson procedures outlined in the Kerry Letter provide that “A request alleging violation of law or other misconduct will be referred to the appropriate United States Government body, including independent oversight bodies, with the power to investigate the respective request and address non-compliance.” This envisions the involvement of two kinds of oversight officials: (1) “Inspectors General,” US

agency officials whose job it is to conduct internal investigations, audits, and review, and also to recommend “corrective action” and (2) Privacy and Civil Liberties officers and oversight boards with review and reporting requirements.

117. Based upon its review of the procedures and commitments outlined in the Kerry Letter, the European Commission determined that “the United States ensures effective legal protection against interferences by its intelligence authorities with the fundamental rights of the persons whose data are transferred from the Union to the United States under the EU-U.S. Privacy Shield.” Commission Implementing Decision of 12.7.2016, at ¶123. It also determined that the objection of the CJEU in *Schrems I* regarding effective remedies under Article 47 of the European Charter. It determined that this objection had been satisfied, based upon a combination of both the current remedies available under US law to EU citizens and the new Ombudsperson mechanism, which it deemed to provide “for independent oversight with investigatory powers.” Commission Implementing Decision of 12.7.2016, at ¶124.
118. The European Commission proceeded from these determinations to conclude that the Privacy Shield provided an adequate level of legal protection under Article 25 of the Directive, as interpreted in light of the European Charter by the CJEU in *Schrems I*. Commission Implementing Decision of 12.7.2016, at ¶141.
119. I have been asked to consider “The nature and extent of the remedy (or remedies) that an EU citizen may access in the United States in the particular context at hand in the light of the adoption of the Privacy Shield mechanism.” Before I do this, I must make three initial caveats. First, while the privacy principles and redress mechanisms against private companies seem stronger under Privacy Shield than under Safe Harbour, I offer no firm opinion on this point because it seems largely irrelevant to the question that produced the judgment in *Schrems I*, law enforcement and intelligence services access to EU personal data transferred to the US. Second, consistent with my instructions in this case and my own expertise in US rather than EU privacy law, I offer no determination about the correctness or not of the European Commission’s determination of Privacy Shield’s legal adequacy under the Directive. Third, since the Ombudsperson mechanism is new and the Privacy Shield Framework is still being built up, it is difficult to draw any firm conclusions about how useful the mechanism will be in practice. Any analysis at this stage by anyone with knowledge of the mechanism will be speculative by its very nature.

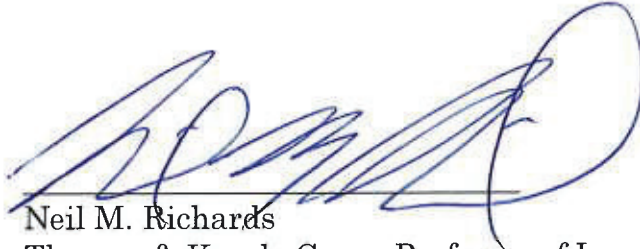
120. In my opinion, the Privacy Shield Ombudsperson mechanism offers a potential opportunity for relief for EU citizens who are concerned that their data protection rights are not being observed through the Privacy Shield-enabled transfers of their data to the US. The mechanism offers an opportunity to have a government official investigate claims, and that official seems to have access to a number of internal investigators and civil liberties lawyers and professionals within the US government intelligence bureaucracies. By providing that a complaint can be investigated without the complainant proving that their data has been accessed by the US government, the mechanism potentially side-steps the obstacle of “injury in fact” that makes a litigation remedy in federal court so difficult to achieve for many privacy plaintiffs. The Ombudsperson is also, by reporting to the Secretary of State, nominally independent from the US intelligence apparatus. I note that both the Gorski Report and the Robertson Report disagree with this assertion on the grounds that the Department of State is entangled in the US intelligence community. See Gorski Report at ¶62 & n.50; Robertson Report at ¶98.
121. Nevertheless, there are several features about the Ombudsperson mechanism that strike me as very different from a judicial remedy. First, the Ombudsperson is not a disinterested judge, but a political appointee who appears to serve at the pleasure of another very senior political appointee, the US Secretary of State. Second, even in cases in which the Ombudsperson’s investigation discovers a violation, she has no formal power to order it to be fixed. Third, even when a violation is discovered and fixed internally, the Ombudsperson cannot tell the EU citizen complainant whether or not they were a target of unlawful surveillance or what if any problems were fixed. Fourth, the Ombudsperson does not tell an EU citizen complainant anything, as her role is insulated from the complainant by two levels of DPA bureaucracy at the European and national levels. And fifth, any response given to the “EU Individual Complaint Handling Body” appears to be qualified both by being an “appropriate response” and by remaining “subject to the continuing obligation to protect information under applicable laws and policies.” These would seem to be bureaucratic refuges that could be used to do very little.
122. The Swire Report expresses optimism that the Privacy Ombudsperson mechanism envisioned by the Privacy Shield Framework could represent an alternative form of relief to EU citizens. The Swire Report makes reference to the Ombudsperson mechanism in Chapter 7, but I do not see anything in this report that causes me to decide that the Ombudsperson mechanism solves the difficulties faced by EU citizens who might desire a legal remedy for privacy violations.

123. In connection with this debate about the effectiveness of Ombuds mechanisms, I note that the Robertson Report concludes that, at least in the European experience with them, Ombuds oversight over intelligence services is limited. The Robertson Report cites with approval the Nov. 15 report of the European Agency for Fundamental Rights, which concludes (in Mr. Robertson's words) that "ombudsmen, although theoretically useful as a means of circumventing legal rules about standing, can only offer non-binding recommendations in cases of maladministration." Robertson Report at ¶53. In my opinion, this critique would seem to apply to the new US Privacy Shield Ombudsperson mechanism as well, to the extent we can anticipate how it will operate in fact. With respect to Mr. Robertson's assessment of the Privacy Shield Ombudsperson, I note that he offers only "provisional approbation," in part because the Kerry Letter was "deficient in detail," and in part because "[i]t is unclear whether it can even order compensation for an individual when it finds that his data has been misused." Robertson Report at ¶98. The Robertson Report concludes that its real potential benefit seems to be along the lines of the kinds of "below the waterline," (i.e., non-litigation) safeguards that are outside the scope of this report. Report at ¶99.
124. In sum, while I believe that the Privacy Ombudsperson mechanism has the potential to be a useful reform, it looks to me far more like a complaint resolution scheme than something approaching a judicial remedy, at least as that notion is understood within the US system with which I am expert. This is not to denigrate the mechanism, which I see as both a reform and an improvement, but the Privacy Shield, in my mind, does not substantially change the legal remedies available to EU citizens, at least not in the way that legal remedies are typically understood in the United States. I note that the Gorski report is substantially in agreement with this interpretation of the Ombudsperson mechanism as well. See Gorski Report at ¶¶60-63.

CONCLUSION

125. In sum, it is my opinion that there is not only substantial evidence to support the conclusions of the DPC Draft Decision and the Serwin Memorandum that EU citizens lack meaningful avenues of legal relief to remedy violations of their data protection and privacy rights in the US, but that I believe these conclusions are correct interpretations of the state of US law at present. US privacy remedies are indeed fragmentary and suffer from individual deficiencies, as well as having to surmount the general obstacle of standing doctrine, which appears to be becoming more stringent, especially in privacy cases. In addition, having reviewed the Privacy Shield framework,

particularly the new Privacy Ombudsperson mechanism, I do not find that this program provides a legal remedy that changes my conclusion.

A handwritten signature in blue ink, appearing to read 'Neil M. Richards', is written over a horizontal line.

Neil M. Richards
Thomas & Karole Green Professor of Law
Washington University in St. Louis
1st December 2016

Appendix A

List of Sources Consulted

I. Public Sources

A. EU Legislation

- 126. The Data Protection Acts, 1988 & 2003 (consolidated)
- 127. Directive 95/46/EC
- 128. Charter of the Fundamental Rights of the European Union
- 129. General Data Protection Regulation (EU) 2016/679
- 130. Commission Decision 2010/87/EC (Standard Contractual Clauses)
- 131. Commission Implementing Decision C(2016) 4176 (the “Privacy Shield” arrangements)

B. US Legislation

- 132. Computer Fraud and Abuse Act, 18 U.S.C. § 1030.
- 133. Electronic Communications Privacy Act, 18 U.S.C. § 2501 et seq.,
- 134. Freedom of Information Act, 5 U.S.C. § 552.
- 135. Judicial Redress Act (“JRA”), Pub. L. No. 114-126 (2016).
- 136. Foreign Intelligence Surveillance Act (“FISA”), 50 U.S.C. §1801 et seq.
- 137. Right to Financial Privacy Act, 12 U.S.C. § 3417.
- 138. Stored Communications Act, 18 U.S.C. § 2701 et seq.

C. US Executive Materials

- 139. Executive Order 12,333.
- 140. Letter from U.S. Secretary of State John Kerry to the European Commission, July 7, 2016.
- 141. Presidential Policy Directive 28.
- 142. U.S. Department of Commerce, Privacy Shield Overview, available at <https://www.privacyshield.gov/Program-Overview>.

D. US Cases

- 143. *ACLU v. Clapper*, 785 F.3d 787 (2d Cir. 2015).
- 144. *Bivens v. Six Unknown Named Agents*, 403 U.S. 388 (1971).
- 145. *Clapper v. Amnesty International*, 133 S.Ct. 1138 (2013).
- 146. *Doe v. Chao*, 540 U.S. 614 (2004).

147. *FAA v. Cooper*, 132 S.Ct. 1441 (2012).
148. *Griswold v. Connecticut*, 381 U.S. 479 (1965).
149. *Hernandez v. Mesa*, No. 15-118, 2016 WL 5897576 (U.S., Oct. 11, 2016).
150. *Katz v. United States*, 389 U.S. 347 (1967).
151. *Klayman v. Obama*, 142 F.Supp.3d 172 (D.D.C. 2015).
152. *Lujan v. Defenders of Wildlife*, 504 U.S. 555 (1992).
153. *Marbury v. Madison*, 5 U.S. (1 Cranch) 137 (1803).
154. *Massachusetts v. EPA*, 549 U.S. 497 (2007).
155. *Microsoft Corporation v. United States Department of Justice*, No. 2:16-cv-00538-JLR (W.D. Wash. 2016).
156. *NASA v. Nelson*, 131 S.Ct. 746 (2010).
157. *Nixon v. Administrator of Gen. Servs.*, 433 U.S. 425 (1977).
158. *Olmstead v. United States*, 277 U.S. 438 (1928).
159. *Riley v. California*, 134 S.Ct 2473 (2014).
160. *Roe v. Wade*, 410 U.S. 113 (1973).
161. *Shearson v. Holder*, 725 F.3d 588, 593 (6th Cir. 2013).
162. *Smith v. Maryland*, 442 U.S. 735 (1979).
163. *Spokeo v. Robins*, 135 S.Ct. 1892 (2016).
164. *Turkmen v. Hasty*, 789 F.3d 218 (2d Cir. 2015), cert. granted, No. 15-1363, 2016 WL 2653655 (U.S. Oct. 11, 2016).
165. *United States v. Jones*, 132 S. Ct. 945, 565 U.S. ____ (2012).
166. *United States v. Miller*, 425 U.S. 435 (1976).
167. *United States v. United States District Court*, 407 U.S. 297 (1972).
168. *United States v. Verdugo-Urquidez*, 494 U.S. 259 (1990).
169. *Whalen v. Roe*, 429 U.S. 589 (1977).
170. *Wikimedia v. NSA*, 143 F.Supp.3d 344 (D.Md 2015).

II. Materials Relating to the *Schrems* Litigation

A. Documents relating to the first *Schrems* judgment

171. Original complaint of Maximillian Schrems to the Irish Data Protection Commissioner, dated 25 June 2013
172. Judgment of Mr Justice Hogan dated 18 June 2014
173. Reference to the CJEU, dated 17 July 2014
174. Judgment of the CJEU, Maximillian Schrems v Data Protection Commissioner (Case C-362/14, 6 October 2015)
175. Order of the High Court, made on 20 October 2015
176. Letter from the Office of the Data Protection Commissioner to Facebook Ireland Limited notifying them of the commencement of an investigation, 3 November 2015

177. Reformulated Complaint of Maximillian Schrems against Facebook Ireland Limited dated 1 December 2015

B. The Draft Decision of 24 May 2016 & Associated Documents

178. Memorandum of Andrew Serwin of Morrison Foerster LLP, dated 24 May 2016
179. Draft Decision of the Data Protection Commissioner, dated 24 May 2016
180. Report of the EU Co-chairs: ad hoc EU/US Working Group, dated 27 November 2013
181. European Commission's Communication to the European Parliament and the Council on the Functioning of the Safe Harbour, published on 27 November 2013 Pleadings (present action)
182. Statement of Claim delivered on 31 May 2016
183. Commission Implementing Decision of 12.7.2016, pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-US Privacy Shield (2016).
184. High Court Order dated 25 July 2016 (procedural directions)
185. Defence of Facebook Ireland Limited, delivered on 23 September 2016
186. Defence of Maximillian Schrems, delivered on 9 September 2016
187. Plaintiffs Reply to the First Named Defendant's Defence, dated 30 September 2016
188. Plaintiffs Reply to the Second Named Defendant's Defence, dated 30 September 2016

C. Expert Reports/Evidence

1. For Mr Schrems

189. Affidavit of Maximillian Schrems, sworn on 14 October 2016
190. Report of Ashley Gorski, dated 14 October 2016

2. For Facebook Ireland Limited

191. Report of Stephen Vladeck, dated 2 November 2016
192. Report of Peter Swire, dated 3 November 2016
193. Report of Geoffrey Roberston SC, dated 7 November 2016
194. Report of John DeLong, dated 2 November 2016
195. Affidavit of Andrea Scheley, sworn on 3 November 2016
196. Report of Peter Ratzel, dated 3 November 2016
197. Report of Joshua P Meltzer, dated 3 November 2016
198. Affidavit of Chris Bream, sworn 3 November 2016

199. Affidavit of Yvonne Cunnane, 3 November 2016
200. Report of Michael Clarke, dated 11 November 2016

3. For EPIC

201. Report of Alan Butler, dated 9 November 2016

4. For BSA/Software Alliance

202. Affidavit of Thomas Boue, sworn 17 November 2016

5. For Digital Europe

203. Report of John Higgins sworn 18 November 2016

III. Secondary Sources

204. Brief of Amicus Curiae Information Privacy Law Scholars, *Spokeo v. Robins*, 135 S.Ct. 1892 (2016), available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2656482.
205. Erwin Chemerinsky, *Constitutional Law: Principles and Policies* §2.3 (5th ed. 2015).
206. Tim Edgar, *Redress for NSA Surveillance: The Devil is in the Details*, *LAWFARE*, Oct. 19, 2015, <https://www.lawfareblog.com/redress-nsa-surveillance-devil-details>.
207. William McGeeveran, *Privacy and Data Protection Law* (2016).
208. Robert Gellman, *Does Privacy Law Work?* in *TECHNOLOGY AND PRIVACY: THE NEW LANDSCAPE* (Philip E. Agre & Marc Rotenberg eds., 1997).
209. Neil M. Richards, *The Dangers of Surveillance*, 126 *HARV. L. REV.* 1934 (2013).
210. Paul M. Schwartz, *Privacy and Participation: Personal Information and Public Sector Regulation in the United States*, 80 *IOWA L. REV.* 553, 585 (1995).
211. Daniel J. Solove & Paul M. Schwartz, *Information Privacy Law* (7th ed. 2015).
212. Stephen I. Vladeck, *The New National Security Canon*, 61 *AM. U. L. REV.* 1295 (2012).
213. Stephen I. Vladeck, *Standing and Secret Surveillance*, 10 *I/S: J. L. & POL. FOR INFO. SOC.* 551, 565-66 (2014).