THE HIGH COURT
COMMERCIAL

Record No: 2016/4809P

Between:

Data Protection Commissioner

Plaintiff

-and-

Facebook Ireland Limited and Maximillian Schrems

Defendants

AMENDED OUTLINE SUBMISSIONS ON BEHALF OF THE AMICUS CURIAE (EPIC)

I. INTRODUCTION

1. The Electronic Privacy Information Center (EPIC) makes the following submissions as *amicus curiae* in the proceedings. These amended submissions are delivered pursuant to the Direction of the Court made on 20 February 2017.

2. EPIC is an independent, public interest, non-profit research and educational organization based in Washington, D.C. EPIC was established to focus public attention on emerging privacy and civil liberties issues and to protect privacy, freedom of expression, and democratic values in the information age. EPIC has served as amicus curiae in many cases in U.S. courts. EPIC also recently intervened in the case of *10 Human rights organizations and others v. the UK* (App No. 24960/15) before the European Court of Human Rights concerning whether alleged surveillance activities by MI5, MI6, and GCHQ violated Article 8 of the European Convention of Human Rights.

3. EPIC has a direct interest in these proceedings because they concern U.S. privacy protections and remedies as well as transnational personal data transfers to the U.S. by companies such as Facebook Ireland (FB-I). EPIC considers this an issue of broad international significance.

4. At paragraph 9(ii) of the judgment accepting EPIC as amicus in this case, McGovern J. concluded that EPIC could "offer a counterbalancing perspective from the US Government on the position in the U.S."[1] Respecting the Court's ruling, these submissions are limited to addressing issues of U.S. privacy and surveillance law and the availability of legal remedies in the U.S. for E.U. citizens, who may feel that their privacy rights have been breached by the U.S. Intelligence Community. E.U. law is touched upon briefly to provide context for that analysis of US law.

5. While it is not the role of EPIC to compare surveillance and data privacy laws of the E.U. to those of the U.S., it is respectfully submitted that the very recent decision of the CJEU in **Watson**[2] may be of considerable assistance to the Irish High Court. The case concerned the compatibility of mass data retention (and access thereto by the authorities), under the national regimes of the United Kingdom and Sweden, with Articles 7 and 8 of the E.U. Charter of Fundamental Rights ('the Charter'), and is valuable in illustrating the interaction between E.U. data protection law and national security regimes.

II. RIGHTS UNDER ARTICLES 7, 8, AND 47 OF THE E.U. CHARTER (EUCFR)

6. The Plaintiff Commissioner highlights in her Statement of Claim that the standard contractual clauses (SCCs) associated with data transfers from the E.U. (and in particular

[1] Data Protection Commissioner v Facebook Ireland and Schrems, judgment of McGovern J. delivered 19th July 2016 [2016] IEHC 414.
[2] Judgment 21 December 2016 *Watson,* Joined Cases C-203/15 and C-688/15, ECLI:EU:C:2016:970.

Ireland) to the U.S. could conflict with fundamental rights enshrined in Articles 7, 8, and 47 of the Charter.

7. Article 7 of the Charter provides that "*Everyone has the right to respect for his or her private and family life, home and communications.*"

8. Article 8 provides for the right to protection of personal data, and specifically provides that:

> *(1) Everyone has the right to the protection of personal data concerning him or her.*
>
> *(2) Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.*
>
> *(3) Compliance with these rules shall be subject to control by an independent authority.*

9. The CJEU, in its decision in **Schrems**[3], held that

> ". . . *legislation permitting the public authorities to have access on a generalized basis to the content of electronic communications must be regarded as compromising the essence of the fundamental right to respect for private life, as guaranteed by Article 7.*"[4]

10. The CJEU also previously held, in its decision in **Digital Rights Ireland**[5], that the access of national authorities to data relating to a person's private life and his or her communications constitutes "*an interference with the fundamental rights guaranteed by Article 7 of the Charter*"[6] and that the unauthorised processing of personal data constitutes "*an interference with the fundamental right to the protection of personal data guaranteed by Article 8 of the Charter.*"[7]

11. Article 47 of the Charter provides 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*

---

[3] Judgment 6 October 2015, *Schrems*, C-362/14, ECLI:EU:C:2015:650.
[4] *Id*. ¶ 94.
[5] Judgment 8 April 2014, *Digital Rights Ireland Limited v Minister for Communication,* Joined Cases C-293/12 and C-594/12, ECLI:EU:C:2014:238.
[6] *Id*. ¶ 35.
[7] *Id*. ¶ 36.

law. Everyone shall have the possibility of being advised, defended and represented . . . ."

12. The question of how the 'effective remedy' to ensure compliance with the provisions of E.U. law provided for in Article 47 applies where personal data of E.U. nationals is intercepted by a foreign (non E.U.) government for foreign intelligence or other purposes in the other (non E.U.) state was addressed to a limited extent by the CJEU in **Schrems** and arises to be further explored in this case.

III. SURVEILLANCE UNDER U.S. LAW

13. EPIC seeks to make submissions focused on two aspects of U.S. law raised in the reformulated complaint and the Commissioner's Statement of Claim, namely: (1) Privacy protection for foreign communications and other personal data under U.S. surveillance law, and (2) Legal redress available to E.U. citizens who wish to challenge U.S. government surveillance and the interception of personal data.

14. At the outset, EPIC submits that there are serious concerns about the adequacy of privacy protections in the U.S. As Professor Richards explains in his report, "*unlike the EU and virtually all industrialized Western democracies, the US does not have a comprehensive data protection statute*."[8] U.S. privacy law is segmented both because constitutional privacy restrictions do not in general limit the actions of private companies and because statutory privacy protections have been adopted on a somewhat piecemeal, industry-specific basis.

15. Furthermore, unlike under the Charter or the ECHR, there is no explicit right to privacy under the United States Constitution. The U.S. Supreme Court has to date declined to recognize a constitutional right to informational privacy.[9]

16. The Fourth Amendment to the U.S. Constitution provides a protection against "unreasonable searches and seizures" by the Government.[10] But this protection is subject to numerous exceptions. One of the most significant exceptions is the so-called "Third Party Doctrine," which limits the protection of data shared with a third party such as a service provider.[11]

IV. GOVERNMENT ACCESS TO PERSONAL DATA TRANSFERRED TO THE U.S.

17. The laws and regulations governing access to personal data of E.U. citizens by the U.S. Intelligence Community include the Foreign Intelligence Surveillance Act (FISA) (and, in particular, Section 702 of the FISA Amendments Act), the Electronic Communications

[8] Expert Report of Professor Neil Richards at ¶ 33. Trial Book 2, Tab 6.
[9] *See Nat'l Aeronautics and Space Admin. v. Nelson*, 562 U.S. 134 (2011).
[10] U.S. CONST. AMD. IV. Trial Book 14, Tab 1.
[11] Expert Report of Professor Neil Richards ¶ 38.

Privacy Act (ECPA), Executive Order 12333 (EO12333), Presidential Policy Directive 28 (PPD-28), and the United States Signals Intelligence Directive SP0018 (USSID 18).

18. EPIC submits that when E.U. citizens' personal data or private communications are transferred from the E.U. to a data processor (such as Facebook) in the United States, the data can be accessed by the U.S. government. E.U. citizens' personal data and private communications are also subject to lesser protections than apply to the personal data and communications of U.S. persons.

19. It is submitted that the U.S. government can gain access to personal data and communications from a data processor through several different mechanisms. These mechanisms include formal requests as well as administrative subpoenas, court orders, and mandatory directives issued under 50 U.S.C. § 1881a.[12] Alternately, the U.S. government can gain access to data transferred to and from the U.S. directly and without the data processor's cooperation or knowledge by intercepting the data *en-route*; this can include compelling the assistance of internet backbone providers to assist in intercepting data streams.[13] The interception of data en-route can occur in the U.S. under the Section 702 "Upstream" program, or at or outside of the U.S. border, pursuant to Executive Order 12333.[14]

a) The Foreign Intelligence Surveillance Act of 1978 ("FISA")[15]

20. The Foreign Intelligence Surveillance Act of 1978 ("FISA") was enacted "*to authorize and regulate certain governmental electronic surveillance of communications for foreign intelligence purposes.*"[16]

21. The FISA was "*the exclusive means by which electronic surveillance and the interception of domestic wire, oral, or electronic communications may be conducted.*"[17]. FISA operates in conjunction with the Electronic Communications Privacy Act (ECPA),[18] which consists of the Wiretap Act, the Stored Communications Act (SCA), and the Pen Register Act.

22. The FISA's four basic surveillance provisions concern electronic surveillance (50 U.S.C. §§ 1801-1813), physical searches (50 U.S.C. §§ 1821-1829), pen/trap surveillance (50 U.S.C. §§ 1841-1846), and orders compelling production of tangible things including business records (50 U.S.C. §§ 1861-1864).

---

[12] *See generally* Expert Report of Professor Steven I. Vladeck ¶¶ 14–53. Trial Book 3, Tab 2.
[13] *See* Privacy and Civil Liberties Oversight Board (PCLOB), *Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act* 7 (2014) [hereinafter PCLOB 702 Report]. Trial Book 14, Tab 56.
[14] *See* Expert Report of Ashley Gorski ¶ 32. Trial Book 6, Tab 1.
[15] FISA, in its totality, is in Trial Book 14, Tab 3.
[16] *Clapper v. Amnesty Int'l USA*, 133 S. Ct. 1138, 1143 (2013). Trial book 14, Tab 16.
[17] 50 U.S.C. § 1812.
[18] ECPA is Tab 6 in Trial Book 14. The SCA provisions are in Tab 6A, the Wiretap Act provisions are in Tab 6B, and the Pen Register provisions are in Tab 6C.

23. Under FISA, 50 U.S.C. § 1801(f), the term "electronic surveillance" only includes "*the acquisition by an electronic, mechanical, or other surveillance device of the contents*" of a communication in three circumstances: (1) where the communication is to or from a "*known United States person*" and "*the contents are acquired by intentionally targeting that person*," (2) where a communication is "*to or from a person in the United States*," is acquired "*without the consent of any party*," and "*such acquisition occurs in the United States*," and (3) where the acquisition is intentional, "*both the sender and all intended recipients are located within the United States*," and a warrant would be required. The traditional (or "Title I") FISA provisions require the Government to follow certain procedures when conducting electronic surveillance, including obtaining a FISA warrant in most cases from the Foreign Intelligence Surveillance Court (FISC).[19]

24. In 2008, Congress added new provisions authorizing access to international electronic communications to enable the targeting of **non-U.S. persons** located outside of the U.S. in 50 U.S.C. §§ 1881a et seq.

25. In essence, Section 702 (50 U.S.C. § 1881a (a)) empowers the Attorney General and the Director of National Intelligence to jointly authorize the (1) targeting of any persons who are not United States persons, (2) who are reasonably believed to be located outside the United States, (3) with the compelled assistance of an electronic communication service provider, (4) in order to acquire foreign intelligence information.

26. The U.S. Government is thereby authorized under Section 702 to obtain and/or scan international communications, even those involving U.S. persons, without a warrant, in order to "target" the communications of non-U.S. persons abroad and to acquire foreign intelligence information. Most significantly, Section 702 directives are not subject to any prior approval by the FISC. There is no warrant requirement or prior judicial review of the targeting or scanning. The Attorney General and the Director of National Intelligence need only certify that they have submitted to the FISC for approval 'targeting procedures' and 'minimization procedures' that satisfy the FISA requirements. Section 702, 50 U.S.C. § 1881a (g), provides that the FISC "*shall have jurisdiction to review the certification submitted.*"

27. A FISC order approving the annual certification does not involve the establishment of 'probable cause' or a review of whether any target is an agent of a foreign power or engaged in criminal activity, nor does the government have to identify to the FISC the specific facilities or places at which electronic surveillance is to be directed.

28. The government can collect or scan communications under Section 702 after issuing 'directives' to communications providers. The providers are legally obligated under 50 U.S.C. § 1881a (h)(1) to "*immediately provide the Government with all information,*

[19] *See* Expert Report of Steven I. Vladeck ¶¶ 17–25.

facilities, or assistance necessary to accomplish the acquisition" of private communications. The providers are required to comply with these directives in secret, are not allowed to notify their users, and face civil contempt charges if they refuse.[20]

29. The PRISM program, which was the subject of review following the Snowden revelations, is operated under Section 702 directives. The government "*sends a selector, such as an email address, to a United States-based electronic communications service provider*" and that provider must return "communications sent **to or from** that selector" back to the government.[21] But even individuals who are not associated with a selector can have their communications collected by the U.S. Government if they are sending messages to the target.[22]

30. The experts agree that the "precise technological means by which the government transmits selectors to providers and providers send data to the government" has not been made public.[23] But none of the experts dispute the description in the PCLOB 702 Report, which describes how the tasking process works using a hypothetical "USA-ISP Company" example:

> "*The NSA applies its targeting procedures (described below) and 'tasks' johntarget@usa-ISP.com to Section 702 acquisition for the purpose of acquiring information about John Target's involvement in international terrorism. The FBI would then contact USA-ISP Company (**a company that has previously been sent a Section 702 directive**) and instruct USA-ISP Company to provide to the government all communications to or from email address johntarget@usa-ISP.com. The **acquisition continues** until the government "detasks" johntarget@usa-ISP.com*"[24]

31. Two things are clear from the PCLOB description of the PRISM process. First, tasking of a selector occurs **after** a company has been served a formal Section 702 directive. Second, tasking is an **ongoing** process, which implies that it involves some technological connection or data transfer mechanism. Whether this process can fairly be characterized as "direct access" to the companies servers is clearly a matter of some dispute between the experts and others working in this area.

---

[20] *See In re Directives*, 551 F.3d 1004, 1007–8 (FISA Ct. Rev. 2008). Trial Book 14, Tab 23.
[21] PCLOB 702 Report at 7. Trial book 14, Tab 56.
[22] *See, e.g.*, *United States v. Mohamud*, 843 F.3d 420 (9th Cir. 2016) (holding that the Fourth Amendment was not violated when a U.S. person's communications with a non-U.S. person abroad were collected pursuant to Section 702 because the non-U.S. person was a target).
[23] Agreed Note of Meeting of US Law Experts at 7.
[24] PCLOB 702 Report at 34.

32. In addition to the PRISM program, the 'Upstream' program, which is also conducted under Section 702, involves the interception of communications without the knowledge or assistance of downstream data processors.[25] Upstream surveillance is conducted by the National Security Agency (NSA) "*with the compelled assistance of providers that control the telecommunications 'backbone' over which telephone and Internet communications transit*."[26] Similar surveillance could also be conducted off-shore or otherwise outside the U.S. pursuant to Executive Order 12333, which is discussed below.

33. Government access to private communications under the Upstream program is significantly broader than under the PRISM program because Upstream involves scanning all messages over a particular network (including so-called multiple communications transactions) in order to conduct searches for "**about communications**." As explained by the U.S. Privacy and Civil Liberties Oversight Board (PCLOB):

> "*An 'about' communication is one in which the selector of a targeted person (such as that person's email address) is contained within the communication but the targeted person is not necessarily a participant in the communication . . . . An MCT is an Internet 'transaction' that contains more than one discrete communication within it. If one of the communications within an MCT is to, from, or 'about' a tasked selector, and if one end of the transaction is foreign, the NSA will acquire the entire MCT through upstream collection, including other discrete communications within the MCT that do not contain the selector.*".[27]

34. The FISC has recognized that the U.S. government's collection of about communications is fundamentally different than other types of Section 702 surveillance. In 2011, attorneys representing the U.S. Intelligence Community revealed to the FISA Court that:

> *"acquisition of Internet communications through [the] upstream collection under Section 702 is accomplished by acquiring Internet 'transactions,' which may contain a single, discrete communication, or multiple discrete communications, including communications that are neither to, from, nor about targeted facilities."*
>
> .[28]

35. The FISC found that the:

> "*NSA's upstream Internet collection devices are generally incapable of distinguishing between transactions containing only a single discrete*

[25] PCLOB 702 Report at p.7. Trial book 14, Tab 56.
[26] *Ibid.*
[27] PCLOB 702 Report at p.7. Trial Book 14, Tab 56.
[28] [*Redacted*], [docket no. redacted], slip op. at 15 (FISC Oct. 3, 2011). Trial Book 14, Tab 25.

> *communication to, from, or about a tasked selector and transactions containing multiple discrete communications, not all of which may be to, from, or about a tasked selector.*"[29]

36. The FISC emphasized that:

> *As a practical matter, this means that* ***NSA's upstream collection devices acquire any Internet transaction transiting the device*** *if the transaction contains a targeted selector anywhere within it.*[30]

37. The PCLOB report on Section 702 concluded that the surveillance technique used by the NSA to conduct "about communication" searches operates in such a way that:

> "[A] *person's communication will have been acquired because the government's collection devices examined the contents of the communication, without the government having held any prior suspicion regarding that communication.*"[31]

38. In order to identify communications "about" a selector, the NSA device must necessarily scan all communications transmitted over that facility, though the PCLOB notes in the 702 Report that the NSA first filters the communications "*to eliminate purely domestic communications*."[32] Thus, the U.S. Government has access to and is scanning e-mails and other electronic communications, *en masse*, at the internet backbone level in order to identify and intercept certain target communications based on their contents. The PCLOB notes in the 702 Report that:

> "*[n]othing comparable is permitted as a legal matter or possible as a practical matter with respect to analogous but more traditional forms of communication. . . the government cannot listen to telephone conversations, without probable cause about one of the callers or about the telephone, in order to keep recordings of those conversations that contain particular content."*[33]

---

[29] [*Redacted*], [docket no. redacted], slip op. at 43 (FISC Oct. 3, 2011).
[30] [*Redacted*], [docket no. redacted], slip op. at 31 (FISC Oct. 3, 2011).
[31] PCLOB 702 Report at 123.
[32] PCLOB 702 Report at 120. Trial Book 14, Tab 56.
[33] PCLOB 702 Report at 122.

39. The FISC found in 2011 that the "*NSA acquires more than two hundred fifty million internet communications each year pursuant to Section 702*."[34]

40. The only statutory limitations on surveillance under Section 702 are the acquisition limits, the targeting procedures, and the minimization procedures referred to under 50 U.S.C. §§ 1881a(b)–(e).

41. Under Section 702, there are five acquisition limits.[35] The first four limitations are aimed at limiting the intentional targeting of U.S. person communications. The fifth limitation requires that acquisition be conducted "*consistent with the fourth amendment*," which does not protect non-U.S. persons with no substantial voluntary connections to the United States.[36] These limitations do not protect E.U. citizens outside of the U.S. from surveillance conducted under Section 702.

42. The Attorney General, in consultation with the Director of National Intelligence must adopt both targeting and minimization procedures under 50 U.S.C. §§ 1881a(d)(1), (e)(1). These procedures are subject to judicial review for their compliance with the statutory requirements under 50 U.S.C. §§ 1881a (d)(2), (e)(2).

43. The Section 702 targeting procedures are only required to be "reasonably designed" to limit acquisition to targets reasonably believed to be located outside the United States and to prevent the acquisition of purely domestic communications.[37] The targeting limitations do not protect E.U. citizens from surveillance

44. The Section 702 minimization procedures must satisfy the four-part definition in § 1801(h). 50 U.S.C. § 1881a (e)(1). These minimization procedure rules only require limits on the acquisition, retention, and dissemination of U.S. person communications and information.

45. It is notable that neither the targeting nor the minimization procedures in Section 702 provide any specific protections for non-U.S. persons. Indeed, Section 702 clearly discriminates between U.S. and non-U.S. persons and imposes restrictions primarily on the collection, use, and dissemination of U.S. person communications and information.[38]

---

[34] [*Redacted*], [docket no. redacted], slip op. at 9 (FISA Ct. Oct. 3, 2011).
[35] 50 U.S.C. §§ 1881a(b)(1)–(5).
[36] *See, e.g.*, *United States v. Mohamud*, 843 F.3d 420, 439 (9th Cir. 2016) (holding that no warrant is required to intercept an overseas foreign national's communications because the interception was "targeted at a non-U.S. person with no Fourth Amendment right).
[37] 50 U.S.C. § 1881a(d)(1).
[38] *See* Expert Report of Professor Steven I. Vladeck ¶ 41. Trial Book 3, Tab 2.

b) Executive Order 12333[39]

46. Executive Order 12333 (EO 12333) sets out the President's rules and orders governing activities of the U.S. Intelligence Community. The Order outlines the roles of the different departments and agencies (Part 1), regulates their conduct (Part 2), and outlines oversight, procedures, and definitions (Part 3). In general terms, the Order is the authority under which the National Security Agency (NSA) collects foreign intelligence. The Director of the NSA is authorized under the Order to:

> "*collect (including through clandestine means), process, analyze, produce, and disseminate signals intelligence information and data for foreign intelligence and counterintelligence purposes to support national and departmental missions*" [40]

47. The Order also indicates that the Director of National Intelligence (DNI) serves "as the head of the Intelligence Community" and is charged with developing "*guidelines for how information or intelligence is provided to or accessed by the Intelligence Community . . . and for how the information or intelligence may be used and shared by the Intelligence Community*"[41]. The Order, however, requires that the Director of National Intelligence carry out the responsibilities above "consistent with applicable law and with full consideration of **the rights of United States persons**, whether information is to be collected inside or outside the United States*"*[42] (emphasis added)). Collection under the Order includes surveillance conducted **outside** the U.S. without judicial oversight.

48. The Director of the NSA is authorized under the Order to "*[c]ollect (including through clandestine means), process, analyze, produce, and disseminate signals intelligence information and data for foreign intelligence and counterintelligence purposes to support national and departmental missions*".[43]

49. The Order grants broad authority to members of the U.S. Intelligence Community to collect all forms of intelligence. The only collection limits imposed under the Order are outlined in Sections 2.3 and 2.4 (see below). Under the Order, "*Intelligence includes foreign intelligence and counterintelligence*".[44] Foreign intelligence is defined broadly as "*information relating to the capabilities, intentions, or activities of foreign governments or elements thereof, foreign organizations, **foreign persons**, or international terrorists*".[45]

---

[39] Exec. Order No. 12,333: 40 Fed. Reg. 59,941 (Dec. 4, 1981), *reprinted as amended in* 73 Fed. Reg. 45,328 (2008) (July 30, 2008). Trial Book 6, Tab 2.
[40] EO 12333 § 1.7(c)(1).
[41] EO 12333 § 1.3.
[42] EO 12333 § 1.3(b)(19).
[43] EO 12333 § 1.7(c)(1).
[44] EO 12333 § 3.5(f).
[45] EO12333 § 3.5(e).

50. Section 2.3 limits the collection, retention, and dissemination of "*information concerning United States persons*" by requiring that Intelligence Community agencies adopt procedures to limit the types of information collected to those specified in Section 2.3(a)–(j) of the Order.

51. Section 2.4 also imposes a general restriction on collection by requiring that members of the U.S. Intelligence Community:

> *"Shall use the least intrusive collection techniques feasible within the United States or directed against United States persons abroad. Elements of the Intelligence Community are not authorized to use such techniques as electronic surveillance, unconsented physical searches, mail surveillance, physical surveillance, or monitoring devices unless they are in accordance with procedures established by the head of the Intelligence Community element concerned or the head of a department containing such element and approved by the Attorney General, after consultation with the Director. Such procedures shall protect constitutional and other legal rights and limit use of such information to lawful governmental purposes."*[46]

52. As Professor Vladeck explains in his expert report, EO12333 "*imposes fairly strict limits on surveillance within the United States or directed against U.S. persons abroad—leaving surveillance directed against non-U.S. persons abroad subject only to the more general collection restrictions*."[47]

c) PPD-28[48]

53. Presidential Policy Directive 28 (PPD-28) is a presidential order, adopted after the Snowden revelations, that imposes certain restrictions on U.S. signals intelligence activities implicating personal information **regardless of the person's nationality or location**.[49]

54. The first section of PPD-28 outlines four "principles" that are framed as general limits on all signals intelligence collection by the U.S. Government (PPD-28 § 1(a)–(d)). The first principle requires that collection "be authorized" by law or executive order and undertaken in a lawful manner. The second principle states that "[p]rivacy and civil liberties shall be integral considerations" in the planning of signals intelligence activities and prohibits

---

[46] EO 12333 § 2.4.
[47] Expert Report of Professor Steven I. Vladeck ¶ 15. Trial Book 3, Tab 2.
[48] Trial Book 14, Tab 43.
[49] THE WHITE HOUSE, PRESIDENTIAL POLICY DIRECTIVE 28: SIGNALS INTELLIGENCE ACTIVITIES (2014) [hereinafter PPD-28].

collection for specified improper purposes. The third principle prohibits the "collection of foreign private commercial information or trade secrets" in order to "afford a competitive advantage to U.S. companies." And the fourth and final principle requires that collection "be as tailored as feasible."

55. The Director of National Intelligence has explained that pursuant to the fourth principle, "*the Intelligence Community takes steps to ensure that even when we cannot use specific identifiers to target collection, the data to be collected is likely to contain foreign intelligence that will be responsive to requirements articulated by U.S. policy-makers pursuant to the process explained in my earlier letter, and minimizes the amount of non-pertinent information that is collected.*"[50] As an example, where specific selectors are not available but a group is being targeted, the U.S. "*might choose to target that group by collecting communications to and from that region for further review and analysis to identify those communications that relate to the group.*"[51]

56. Section 2 governs signals intelligence collected in bulk. PPD-28 defines "bulk collection" as:

> "*the authorized collection of large quantities of signals intelligence data which, due to technical or operational considerations, is acquired* ***without the use of discriminants*** *(e.g., specific identifiers, selection terms, etc.)*"[52]

57. Section 2 allows for the collection of signals intelligence in bulk in certain circumstances which "*may . . . result in the collection of information about persons whose activities are not of foreign intelligence or counterintelligence value*".[53]

58. Section 2 does not impose any limits on access to or acquisition of communications; it only limits the *use* of acquired communications. Section 2 requires that that the U.S. shall use non-publicly available signals intelligence collected in bulk only for six listed purposes.[54]

59. These limitations on bulk collection are also themselves subject to an exception; they "*do not apply to signals intelligence data that is temporarily acquired to facilitate targeted collection*".[55] This exception refers to data that is acquired in bulk for searching/filtering

---

[50] Annexes to the Commission Implementing Decision pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield at L 207/105 (Dec. 7, 2016) [hereinafter Privacy Shield Annexes].
[51] *Ibid*.
[52] PPD-28 § 2 n.5.
[53] PPD-28 § 2.
[54] PPD-28 § 2.
[55] PPD-28 § 2 n.5.

over a relatively short period of time (for example data to be searched for information 'about' a particular selector).

60. PPD-28 extended EO 12333's limits on dissemination and retention of personal information, but did not extend the collection limits. Specifically, in reference to EO 12333, PPD-28 mandates that for all individuals:

> "*Dissemination: Personal information shall be disseminated only if the dissemination of comparable information concerning U.S. persons would be permitted under section 2.3 of Executive Order 12333.*
>
> *Retention: Personal information shall be retained only if the retention of comparable information concerning U.S. persons would be permitted under section 2.3 of Executive Order 12333 and shall be subject to the same retention periods as applied to comparable information concerning U.S. persons. Information for which no such determination has been made shall not be retained for more than 5 years, unless the DNI expressly determines that continued retention is in the national security interests of the United States.*"[56]

d) USSID 18[57]

61. The NSA has adopted a set of procedures in United States Signals Intelligence Directive SP0018, pursuant to EO12333, that govern signals intelligence activities. The purpose of USSID 18 is to establish rules such that signals intelligence operations "*are conducted pursuant to procedures which meet the reasonableness requirements of the Fourth Amendment*".[58] The rules in USSID 18 are based on the premise that "The Fourth Amendment to the United States Constitution protects all U.S. persons anywhere in the world and all persons within the United States from unreasonable searches and seizures by any person or agency acting on behalf of the U.S. Government". [59]

62. The USSID 18 rules limit the collection of "communications to, from or about U.S. persons or persons or entities in the U.S."[60] ().

63. The NSA updated USSID 18 in 2015 in accordance with PPD-28 by issuing supplemental procedures focused on signal intelligence activities directed at **non-US persons.**[61]

---

[56] PPD-28 § 4(a)(i).
[57] Nat'l Sec. Agency, USSID SP0018: Legal Compliance and U.S. Persons Minimization Procedures (2011) [hereinafter USSID 18]. Trial Book 14, Tab 49.
[58] USSID 18 § 1.1.
[59] USSID 18 § 1.1.
[60] USSID 18 § 3.1.

64. The supplemental procedures are focused primarily on the use of "personal information" of non-U.S. persons that has already been collected. The rules state that "*If the [U.S. Signals Intelligence System] collects personal information of non-U.S. persons, it will process, analyze, disseminate, and retain such personal information only in accordance with these Supplemental Procedures*." The term "personal information" includes "*the same types of information covered by 'information concerning U.S. persons' under Section 2.3 of Executive Order 12333*."[62] Information concerning U.S. persons is not defined in EO 12333, but is defined in the Department of Defense manual that governs NSA and other Department of Defense intelligence activities:

> *Information that is reasonably likely to identify one or more specific U.S. persons. USPI may be either a single item of information or information that, when combined with other information, is reasonably likely to identify one or more specific U.S. persons.*[63]

V. INADEQUACY OF PRIVACY SAFEGUARDS FOR EU CITIZENS

65. It is submitted that U.S. law fails to ensure an adequate level of protection for the personal data and private communications of E.U. citizens outside the U.S. This is because (1) both the scope of application of privacy protections and the definitional scope of personal information in U.S. law are restrictive, (2) important statutory and constitutional protections do not apply to non-U.S. data, and (3) many of the privacy restrictions are subject to executive branch modification or rescission.

a) U.S. Privacy Protections are Limited in Scope

66. U.S. privacy law is characterized by particularly narrow conceptions of privacy and personal data, which in turn limit the scope of relevant constitutional, statutory, and regulatory privacy protections.

67. For example, in *Smith v. Maryland*, the Court considered the use of a 'pen register' device to record telephone numbers dialed by a criminal suspect (but not the content of the calls) without a warrant.[64]. The Court held that "*a person has **no legitimate expectation of privacy** in information he voluntarily turns over to third parties*" such as telephone

---

[61] Nat'l Sec. Agency, USSID SP0018: Supplemental Procedures for the Collection, Processing, Retention, and Dissemination of Signals Intelligence Information and Data Containing Personal Information of United States Persons (2015) [hereinafter USSID 18 Supplemental Procedures]. Trial Book 14, Tab 44.
[62] USSID 18 Supplemental Procedures § 3.3.
[63] DoD MANUAL 5240.01: PROCEDURES GOVERNING THE CONDUCT OF DoD INTELLIGENCE AGENCIES § G.2 (2016). Trial Book 14, Tab 51.
[64] 442 U.S. 735 (1979).

companies. *Id.* at 743–44.[65] Despite this ruling, the practice at the U.S. Department of Justice has been "to get a warrant when seeking to obtain the **content** of US persons' email communications that are stored on third party servers," in accordance with the decision in *United States v. Warshak*,.[66] But even under the *Warshak* rule, the U.S. Government has taken the position that mass collection of non-content personal data is not prohibited by the Fourth Amendment. *See ACLU v. Clapper*[67]

68. It is submitted that much of the personal data of E.U. citizens transferred to the U.S. by **FB-I** and other similarly-situated processors is not protected under the Fourth Amendment.

69. Even in cases where personal information and communications transferred from the E.U. are subject to protections in the U.S., those protections may not attach until the data is viewed, reviewed, or disseminated by a government agent. It is important to note that the United States does not view technological access, like electronic scanning, as implicating privacy or data protection concerns.[68] It is only when the information is accessed or viewed by a human, under the U.S. theory, that data protection issues arise (temporarily storing and scanning data electronically in order to locate selectors or relevant terms is not therefore a breach of privacy or data protection as such).

70. The statutory privacy protections for electronic communications and data in the U.S. are also subject to numerous exceptions. For example, a number of provisions of the Stored Communications Act only apply to communications held in "electronic storage" by the provider, which is a narrowly defined term.[69] The U.S. can also compel communications providers to disclose the contents of communications that have been in electronic storage "for more than one hundred and eighty days."[70]

71. In addition, U.S. regulations on use, retention, and dissemination of data collected by the government are limited by the narrow definition of personal information. The minimization procedures applied by the NSA to seized communications only impose limitations on the use, retention, and dissemination of "*information that is reasonably likely to identify*" a specific person or "*information that, when combined with other information, is reasonably likely to identify*" a specific person.[71]

---

[65] *See also* Expert Report of Professor Neil Richards, ¶38–39. Trial Book 2, Tab 6.
[66] 631 F.3d 266 (6th Cir. 2010). Agreed Note of Meeting of US Law Experts at 24, #9.
[67] 785 F.3d 787 (2nd Cir. 2015). Trial Book 14, Tab 15.
[68] *See* Robert S. Litt, *The Fourth Amendment in the Information Age*, 126 Yale L. J. F. 8, 15 (2016) ("If the government electronically scans electronic communications, even the content of those communications, to identify those it is lawfully entitled to collect, and no one ever sees a non-responsive communication, or knows that it exists, where is the actual harm?").
[69] 18 U.S.C. § 2510(17).
[70] 18 U.S.C. §§ 2703(a)–(b). *See* Expert Report of Professor Steven I. Vladeck ¶ 26. Trial Book 3, Tab 2.
[71] DOD MANUAL 5240.01: PROCEDURES GOVERNING THE CONDUCT OF DOD INTELLIGENCE AGENCIES § G.2 (2016).

72. It is submitted that under the operative regulations of the NSA and other members of the U.S. Intelligence Community, a wide range of personal data and private communications would not be subject to privacy protections. In particular, the "minimization procedures" adopted under **FISA** and **PPD-28** would not prevent use and dissemination of the contents of private communications. The minimization procedures would only require removal or redaction of a narrowly defined category of "personal information" in those communications.

73. In light of the foregoing, it is clear that the general scope of protection of personal data and private communications under U.S. law is limited.

b) Personal Data and Communications of non-U.S. Persons Are Excluded from Important U.S Privacy Safeguards

74. Importantly, many of the privacy safeguards under U.S. law in fact operate to the exclusion of E.U. citizens situated outside the United States.

75. Firstly, it is submitted that the Fourth Amendment does not protect the privacy of E.U. citizens outside the United States. The experts in this case agree that the protections of the Fourth Amendment do not extend to individuals who have no "'substantial voluntary connections' to the U.S., such as physical presence in the country."[72] U.S. courts have found that "the Fourth Amendment does not apply to searches and seizures by the United States against a non-resident alien in a foreign country."[73]

76. Secondly, U.S. surveillance laws authorize the collection of **foreign** communications without the requirement of individualized suspicion and in the absence of judicial oversight (see section on FISA above). Section 702 specifically authorizes broad scale surveillance of non-U.S. communications without a warrant.[74] The key limitations on Section 702 surveillance— namely, acquisition limits, targeting procedures, and minimization procedures—effectively exclude non-US persons' communications from protection.[75]

77. It is true that some limitations on Section 702 surveillance apply regardless of whether the target is a U.S. person.[76] For instance, collection is required to be conducted, to the greatest extent reasonably feasible, to minimize the acquisition of information not relevant

---

[72] Agreed Note of Meeting of US Law Experts at 19 #25.
[73] *United States v. Mohamud*, --- F.3d. ---, No. 14-30217, 2016 WL 7046751, at *16 (9th Cir. Dec. 5, 2016).
[74] 50 U.S.C. § 1881a(a).
[75] *See* 50 U.S.C. §§ 1881a(e)(1), 1801(h)(1)–(4). *See also* Expert Report of Professor Steven I. Vladeck ¶ 41.
[76] The PCLOB notes in its report that non-U.S. persons do enjoy several of the general protections that apply to all 702 collection, including (1) the "foreign intelligence" purpose limitation, (2) civil remedies for unauthorized surveillance, and (3) prohibitions on secondary unauthorized use. PCLOB 702 Report at 98. Trial Book 14, Tab 56.

to an authorized foreign intelligence purpose.[77] However, the caveat of reasonable feasibility is important. Even information that is "not relevant" to foreign intelligence could be lawfully captured in circumstances where it was not "reasonably feasible" to focus collection on relevant information because of technological or intelligence restraints. In any event, the "relevance" threshold is particularly low; it is noteworthy that there is no requirement for information to be "necessary" to the authorized purpose.

78. In addition, the U.S. has, under Section 702, gained access to international communications in bulk and scanned or processed those communications without individualized suspicion or judicial oversight in order to target certain selectors. While the exact procedure for issuing directives and collecting communications under PRISM has not been made public, the bulk searching of the contents of communications under Upstream and acquisition of non-target communications in MCTs has been discussed at length in the PCLOB 702 Report and published FISC decisions.

79. It is respectfully submitted, on the basis of the above, that with regard to privacy safeguards, non-U.S. citizens are in a significantly disadvantageous position.

c) Many Privacy Rules Are Subject to Executive Branch Modification or Rescission

80. EPIC submits that many of the rules and restrictions discussed in the expert reports submitted by **FB-I** are not enshrined in law and can be modified or rescinded by the U.S. Executive at any time, at their discretion. This is a significant limitation on the long-term viability of these rules, especially during a change in administration.

81. Executive Order 12333, for example, is a presidential order structuring all U.S. intelligence activities.[78]

82. EO 12333 already provides broad authority to conduct signals intelligence surveillance for "foreign intelligence and counterintelligence purposes" and offers few corresponding limits on collection. None of the limits provided in the Order meaningfully restrict collection of information about foreign citizens abroad. Importantly, while recent reforms extended retention and dissemination limits in Section 2.3 to persons regardless of nationality or location, the limits on collection *were not extended*.

83. Presidential Policy Directive 28 (PPD-28) was a 2014 presidential order that placed certain limits on signals intelligence activities regardless of the person's nationality or location.[79] However, PPD-28 offered no hard limits on collection pertaining to E.U. citizen data, and expressly authorized bulk surveillance.

---

[77] MINIMIZATION PROCEDURES USED BY THE NATIONAL SECURITY AGENCY IN CONNECTION WITH ACQUISITIONS OF FOREIGN INTELLIGENCE INFORMATION PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978, AS AMENDED § 3(a) (2015).
[78] Expert Report of Professor Steven I. Vladeck, ¶15. Trial Book 3, Tab 2.
[79] Privacy Shield Annexes at 207/91.

84. As with EO 12333, any surveillance limitations in PPD-28 can be rescinded or modified by the President at any time.

VI. LACK OF EFFECTIVE REDRESS FOR E.U. CITIZENS

85. It is submitted that U.S. law does not provide an effective means for E.U. citizens to seek redress for claims related to surveillance carried out in violation of their rights under Article 7 and 8 of the Charter.

86. Firstly, E.U. citizens with no substantial voluntary connections to the United States have no mechanism to challenge *authorized* surveillance programs that could violate their fundamental rights. Secondly, even challenges to *unauthorised* surveillance have severely restricted remedies. Thirdly, data protection remedies of access and correction are also restricted. Finally, the standing and state secrets doctrines are structural barriers that significantly restrict all forms of judicial redress in privacy cases.

87. Furthermore, in EPIC's view, the expert reports of Mr. Serwin and Professor Richards provide a detailed and accurate account of the limitations of the civil remedies available under U.S. law.[80]

a) U.S. Law Does Not Provide E.U. Citizens with Effective Redress for Violations of Their Charter Rights Arising from Authorized Surveillance

88. Of the statutory provisions detailed in the expert reports, the most relevant to an E.U. citizen seeking redress for unlawful surveillance activities are 18 U.S.C. § 2712 and 50 U.S.C. § 1810.[81] In addition to those provisions, the experts also discussed remedies available under the Computer Fraud and Abuse Act (18 U.S.C. § 1030), the Administrative Procedure Act (5 U.S.C. § 702), the Privacy Shield ombudsman mechanism, and other provisions.[82] None of these statutes, however, provide a means to seek redress for violations of Charter rights caused by surveillance **authorized** under U.S. law. In particular, surveillance conducted pursuant to Section 702 itself cannot be challenged under any of these statutes.

89. The provision of the Stored Communications Act permitting civil actions against the United States for certain violations of the ECPA and the FISA, 18 U.S.C. § 2712, limits claims to those individuals who can establish a **willful violation** of specific provisions in (1) the Stored Communications Act, (2) the Wiretap Act, (3) traditional FISA, (4) the

---

[80] *See* Expert Report of Professor Neil Richards (Trial Book 2, Tab 6); First Memorandum of Andrew B. Serwin (Trial Book 2, Tab 2).

[81] First Memorandum of Andrew B. Serwin at pp 2–3.

[82] *See* First Memorandum of Andrew B. Serwin at 11–12 (discussing 18 U.S.C. § 1030); Expert Report of Professor Steven I. Vladeck ¶¶ 81–83 (discussing 5 U.S.C. § 702); Second Memorandum of Andrew B. Serwin at pp 3–6 (responding to Professor Vladeck's points about 5 U.S.C. § 702); Testimony of Professor Peter Swire, Chapter 7, ¶¶ 17–18 (discussing the Privacy Shield); Expert Report of Professor Neil Richards ¶¶ 105–124 (discussing the Privacy Shield framework).

FISA physical search provision, or (5) the FISA pen register and trap and trace provisions.[83] This imposes a prohibitively high threshold on potential claimants and provides no mechanism to challenge **authorized** surveillance that violates E.U. citizens' Charter rights. And although § 2712 does provide a remedy for the violation of certain FISA minimization procedures, it does not provide a remedy for violations of Section 702's targeting or minimization proedures.[84]

90. FISA § 1810, which provides for a civil cause of action for damages, in fact has a very narrow scope of application. The provision only applies to cases where information is used or disclosed in violation of § 1809, which makes it a criminal offense to (1) intentionally conduct **unauthorized** electronic surveillance, and (2) intentionally use or disclose information the individual knew or had reason to know was obtained through **unauthorized** electronic surveillance.[85] Surveillance conducted pursuant to directives issued under Section 702 is not actionable under FISA § 1810 because Section 702 would qualify as an "express statutory authorization" under 1809(a)(2).

91. The Privacy Shield ombudsman mechanism, which does provide a mechanism to seek judicial redress,[86] requires that E.U. citizens submitting inquiries regarding access to their personal data for national security purposes must allege a "violation of law or other misconduct" to merit referral of their complaint to an "appropriate United States Government body."[87] Even then, the only reassurance that the Ombudsman can provide to an E.U. citizen is that (1) their "complaint has been properly investigated" and (2) any "non-compliance" with "U.S. law, statutes, executive orders, presidential directives, and agency policies" has "been remedied."[88] The Privacy Shield framework thus does not provide any means to challenge **authorized** surveillance that contravenes Charter rights.

92. Finally, the Computer Fraud and Abuse Act (CFAA), which generally prohibits intentional access to protected systems without authorization, exempts any "lawfully authorized investigative, protective, or intelligence activity of a law enforcement agency of the United States, a State, or a political subdivision of a State, or of an intelligence agency of the United States."[89]

93. It is clear that the above statutes do not provide adequate remedies for breach of Charter Rights arising from **authorized** surveillance.

---

[83] First Memorandum of Andrew B. Serwin at 2–3, 9–10.
[84] *See* 18 U.S.C. § 2712(a) (listing three FISA minimization provisions: sections 106(a) [50 U.S.C. § 1806(a)], 305(a) [50 U.S.C. § 1825(a)], and 405(a) [50 U.S.C. § 1845(a)]).
[85] *See* 18 U.S.C. §§ 1809(a), 1810; First Memorandum of Andrew B. Serwin at 3.
[86] Expert Report of Professor Neil Richards ¶¶ 120–124.
[87] Privacy Shield Annexes at L 207/75.
[88] Privacy Shield Annexes at L 207/74.
[89] 18 U.S.C. § 1030(f).

b) Remedies that Permit Challenges to Unauthorized Surveillance are Effectively Untenable

94. It is submitted that even the U.S. remedies available for **unauthorized** surveillance are so restricted as to be effectively untenable for E.U. citizens.

95. The doctrine of "sovereign immunity" may entirely bar any § 1810 claim against U.S. government agencies or government employees acting in their official capacity.[90] As a result, 1810 only provides a means to seek redress against individual government agents, acting *ultra vires*, for electronic surveillance (as narrowly defined in FISA § 1801).

96. Although Section 2712 of the Stored Communications Act provides a means for individuals to seek redress against the United States for unauthorized surveillance, such challenges are strictly limited. To bring a claim against the United States under § 2712, an individual must present the claim "to the appropriate department or agency under the procedures of the Federal Tort Claims Act" (FTCA), a complex statute that imposes a number of procedural restrictions.[91] Section 2712 also only provides remedies for a **wilful violation** of the SCA, the Wiretap Act, or certain FISA provisions.

97. Although Section 2712 provides redress for breach of certain FISA provisions, the scope of provisions covered is narrow and unrelated to surveillance on foreign citizens.[92] The provisions covered by § 2712 are those focused on protecting U.S. persons and those which prohibit use or disclosure of information for unlawful purposes.[93] Importantly, Section 2712 does not provide a remedy for a violation of the corresponding FISA provisions concerning compelled production of tangible things under FISA or of the Section 702 targeting and minimization procedures.

98. It is submitted therefore, that even where remedies are available relating to unauthorized surveillance, such remedies are to a large extent illusory and ineffective.

c) E.U. Citizens' Data Protection Rights of Access and Correction are Strictly Limited under The Judicial Redress Act, and are Subject to Discretionary Policies that are Revocable by The Executive

99. Although the Judicial Redress Act offers a restricted set of data protection remedies against U.S. agencies for their handling of individual records, the availability of such remedies is predicated upon a series of unreviewable and revocable discretionary decisions by U.S. officials.[94] The robustness of such remedies is accordingly seriously undermined.

---

[90] First Memorandum of Andrew B. Serwin at p.3.
[91] 18 U.S.C. §b 2712(b)(1).
[92] First Memorandum of Andrew B. Serwin at p.3.
[93] *See* 50 U.S.C. § 1806(a); 50 U.S.C. § 1825(a); 50 U.S.C. § 1845(a)).
[94] *See* Expert Report of Professor Neil Richards ¶¶ 44–52.

100. As Professor Richards explains in his expert report, for an individual to have remedies against a U.S. agency under the Judicial Redress Act, that individual must be a citizen of a "covered country."[95] Such a designation, which is contingent on certain data transfers being conducted with the U.S., is made by U.S. officials through a discretionary process which is not subject to judicial review. However, the United States recently confirmed that the E.U. and all member states except Denmark and the United Kingdom have been designated by the U.S. Attorney General as "covered countries."[96]

101. Furthermore, remedies available to non-U.S. persons under the Judicial Redress Act are not co-extensive with those available to U.S. persons under the Privacy Act. Remedies available under the Judicial Redress Act are comparably limited in number and form.[97] Firstly, the Judicial Redress Act does not provide for one of the four causes of action available in the Privacy Act, namely failure to "*maintain any record concerning any individual with such accuracy, relevance, timeliness, and completeness as is necessary to assure fairness in any determination relating to the qualifications, character, rights, or opportunities of, or benefits to the individual that may be made on the basis of such record, and consequently a determination is made which is adverse to the individual*."[98] Secondly, the two analogous causes of action relating to requests for amendment of an individual's record, are permitted **only** against "designated agencies."[99] Designation of such agencies is again carried out through an unreviewable, discretionary decision by U.S. officials and depends on the existence of specific types of data transfers with another country or a determination that designation would be in the interest of law enforcement for the U.S.[100] Finally, the application of the fourth cause of action arising under the Privacy Act (namely failure to comply with any other provision of the Privacy Act or any rule promulgated thereunder, in such a way as to have an adverse effect on an individual) is limited by the Judicial Redress Act to instances of intentional or wilful conduct.[101] This imposes a significant and prohibitive threshold for availability of the remedy to E.U. citizens.

102. In light of the foregoing, it is submitted that causes of action for breach of privacy extended to non-U.S. citizens by the Judicial Redress Act are so curtailed as to fall far short of constituting effective remedies for breach of privacy. In any event, the availability of such remedies is predicated on discretionary decisions of the President.

d) Overarching Barriers to Redress Are Likely to Preclude E.U. Citizen Claims Involving U.S. Surveillance

---

[95] Expert Report of Professor Neil Richards ¶ 51.
[96] Agreed Note of Meeting of U.S. Law Experts at p.2.
[97] First Memorandum of Andrew B. Serwin at pp. 6–7. Trial Book 2, Tab 2.
[98] 5 U.S.C. § 552(g)(1)(C).
[99] First Memorandum of Andrew B. Serwin at 7–8.
[100] *Id.*
[101] *Id*. at 6.

103. It is submitted that even where it appears that one of the narrow remedies set out above, is available to an E.U. citizen, there are under U.S. law overarching barriers which would prevent effective access to such remedies. In particular, the standing doctrine and the state secrets privilege strictly limit most claims involving U.S. surveillance at the outset.

104. As described in the Expert Reports of Mr. Serwin, Professor Vladeck, Professor Swire, and Professor Richards, the U.S. Supreme Court has limited the availability of judicial redress in privacy and surveillance cases under the "standing doctrine."[102] It is submitted that under the U.S. standing doctrine, very few E.U. claimants will be able to challenge surveillance in a U.S. court.

105. The experts agree standing doctrine requires that, in order to bring an action in federal court, a plaintiff must demonstrate an "injury in fact," that is "fairly traceable" and "likely" to be "redressed by a favorable decision."[103] In *Clapper v. Amnesty Int'l USA*, the U.S. Supreme Court held that a group of plaintiffs did not have standing to challenge the Section 702 surveillance program even though the plaintiffs were a group of attorneys, advocates, and others who routinely communicated with foreigners abroad.[104] The Court concluded the plaintiffs' claim that their communications would being collected under Section 702 was "too speculative to satisfy the well-established requirement that threatened injury must be 'certainly impending'" and that the plaintiffs' injury was not "fairly traceable" to Section 702.[105]

106. *Clapper v. Amnesty* presents significant hurdles for plaintiffs seeking to challenge surveillance programs in the United States.[106] In order to challenge Section 702 surveillance under the *Clapper* standard, an individual would have to establish that either (a) their communications had already been intercepted by the United States, or (b) the interception of their communications is "certainly impending." In either case, they would need to establish the particular statutory authority used by the United States to authorize the collection. Surveillance is, of course, conducted in secret. It is likely to be impossible for the potential claimant to establish with certainty the specific statutory authority used to conduct the surveillance and indeed whether a particular individual was the subject of surveillance. The specific statutory authority used to conduct the surveillance may be impossible for a plaintiff to establish with certainty, as is whether a particular individual was surveilled. Yet, without this information, a plaintiff attempting to challenge surveillance will not be able to establish standing. By its nature, a claim arising from surveillance is likely to be speculative and to fail the *Clapper* test.

---

[102] First Memorandum of Andrew B. Serwin at 13–16; Expert Report of Professor Steven I. Vladeck ¶¶ 89–95; Testimony of Professor Peter Swire, Chapter 7, ¶¶ 87–92; Second Memorandum of Andrew B. Serwin at 1–3; Expert Report of Professor Neil Richards ¶¶ 69–96.
[103] Agreed Note of Meeting of U.S. Law Experts at 33.
[104] 133 S. Ct. 1138, 1145 (2013).
[105] *Id.*
[106] *See* Expert Report of Professor Neil Richards ¶ 93.

107. The cases discussed in Professor Vladeck's report, Mr. Serwin's second report, and in the joint expert statement are the exceptions that prove the rule. First, the lower court decisions that have found standing to challenge NSA surveillance were brought by U.S. plaintiffs who could assert a Fourth Amendment injury.[107] Nothing in Professor Vladeck's report supports the conclusion that E.U. citizens could establish an injury under Article III even if they *could prove* that they had been subject to surveillance. In particular, an E.U. citizen could not assert a constitutional *or* statutory injury if they sought to challenge surveillance authorized under Section 702. Second, the "concrete" injury requirement outlined in *Spokeo* is an additional obstacle to plaintiffs seeking to assert privacy claims in the United States, though the experts disagree on the significance of the obstacle that the concreteness test poses.[108] The record shows that a significant number of post-*Spokeo* privacy claims have been rejected under the concreteness test,[109] and the reports of Professor Vladeck and Professor Swire do not provide evidence to show that E.U. plaintiffs could overcome this hurdle in challenging government surveillance programs absent some alleged Fourth Amendment injury.

108. A second major barrier to the adjudication of surveillance-related claims against the United States is the state secrets doctrine, which can result in exclusion of evidence or even the dismissal of cases against the government.

109. The U.S. Supreme Court has held that where there is a "reasonable danger that compulsion of the evidence will expose military matters which, in the interest of national security, should not be divulged," that evidence is privileged.[110] As Professor Vladeck explains in his report, the state secrets doctrine includes both the "*Totten* bar" and the "*Reynolds* privilege."[111] Under the *Totten* bar, a court can "completely bar adjudication of claims premised on state secrets"—as, for example, where classified information would be necessary to establish standing, or where the very subject matter of the suit is secret.[112] Under the *Reynolds* privilege, the court can exclude certain secret evidence from the case. Indeed, in a recent challenge to Section 702 "upstream" surveillance program on Fourth Amendment grounds, the case was dismissed on state secrets grounds.[113] The experts agree

---

[107] *See Schuchardt v. Obama*, 839 F.3d 336 (3d Cir. 2016) (concerning a challenge to Section 702 brought by a Virginia resident); *ACLU v. Clapper*, 785 F.3d 787 (2nd Cir. 2015) (concerning a challenge to Section 215 brought by a civil rights organization based in New York); *Valdez v. NSA*, No. 15-584 (D. Utah Jan. 10, 2017) (concerning a challenge to alleged bulk surveillance during the 2002 Olympics brought by six individuals who lived in Utah at that time); *Klayman v. Obama*, 142 F. Supp. 3d 172 (D.D.C. 2015) (concerning a challenge to Section 215 brought by individuals and an organization in the District of Columbia).

[108] *See* Expert Report of Professor Neil Richards ¶¶ 85–96; Agreed Note of Meeting of U.S. Law Experts at 34–36.

[109] *See* Calli Schroeder, *Intangible Privacy Harms Post-Spokeo*, Privacy Tracker, Westin Research Center (Dec. 15, 2016).

[110] *United States v. Reynolds*, 345 U.S. 1, 10 (1953). Trial Book 8, Tab 36.

[111] Expert Report of Professor Steven I. Vladeck ¶ 100. Trial Book 3, Tab 2.

[112] *Ibid*.

[113] *See Jewel v. NSA*, No. 08-4373, 2015 WL 545925 (N.D. Cal. Feb. 10, 2015).

that the government could seek dismissal of a surveillance challenge on state secrets grounds based on either the *Totten* bar or the *Reynolds* privilege.[114]

CONCLUSION

In conclusion, it is submitted that interception and surveillance of the personal data of E.U. citizens sent to the U.S. by data processors—such as Facebook—is permitted by U.S. Surveillance/Foreign Intelligence law and is subject to limited, if any, judicial oversight. Furthermore, U.S. Privacy Law does not provide adequate safeguards for personal data and private communications of E.U. citizens and does not provide an effective means of redress for a breach of Charter Rights.

Grainne Gilmore BL

Colm O'Dwyer SC

Word Count (excluding footnotes): 8,252

[114] Agreed Note of Meeting of U.S.Law Experts at 23.