THE HIGH COURT

COMMERCIAL

2016 No. 4809P

BETWEEN:

THE DATA PROTECTION COMMISSIONER

Plaintiff

AND

FACEBOOK IRELAND LTD.

-and-

MAXIMILIAN SCHREMS

Defendants

WRITTEN LEGAL SUBMISSION ON BEHALF OF

THE UNITED STATES OF AMERICA AS AMICUS CURIAE

I. Introduction

1. This is the written submission of the United States ("**U.S.**"), delivered pursuant to this Honourable Court's order of 25 July 2016 admitting the U.S. as *amicus curiae* to these proceedings.

A. Background and Key Issues

2. In allowing the U.S. *amicus* status, the Court acknowledged that the United States *"has a significant and bona fide interest in the outcome of these proceedings. At issue in the proceedings is the assessment, as a matter of E.U. law, of the applicant's law governing the treatment of E.U. citizens' data transfer to the U.S."* The U.S. has a vital interest in ensuring that the Court has an accurate, up-to-date, and comprehensive account of the current U.S. legal regime regarding access to data inside the U.S., including access to data of E.U. citizens transferred to the U.S.

3. This matter arises from the judgment of the Court of Justice of the European Union ("**CJEU**") in *Schrems v. Data Protection Commissioner* ("***Schrems I***").[1] The plaintiff (the "**DPC**"), in investigating Mr Schrems' Reformulated Complaint, has been considering the legal basis for the transfer by Facebook Ireland of personal data to Facebook, Inc. in the U.S., and whether such transfers satisfy the requirements of Directive 95/46/EC (the "**Directive**"). In essence, the Directive requires that where personal data is transferred to a third country, that country must ensure an adequate level of protection within the meaning of Article 25 of the Directive; alternatively, the parties to the transfer may adduce adequate safeguards within the meaning of Article 26, including through using standard contractual clauses ("**SCCs**").

4. Arising from the CJEU judgment in *Schrems I*, the DPC in her Draft Decision of 24 May 2016 (the "**Draft Decision**") has formed the provisional view that "*a legal remedy compatible with Article 47 of the Charter* [of Fundamental Rights of the European Union (the "**Charter**")] *is not available in the US to EU citizens whose data is transferred to the*

[1] Judgment of 6 October 2015, *Schrems*, C-362/14, EU:C:2015:650.

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."*

5. On this basis, the DPC considers that the three Commission decisions establishing the adequacy of protection provided by certain SCCs adopted under Article 26(4) of the Directive (the "**SCC Decisions**")[2] 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."* As a result, she considers that there are *"well-founded objections to the SCC Decisions and doubts as to their compatibility with Article 47 of the Charter."*

6. These *"well-founded objections"* appear to be premised on an erroneous conflation of the requirements of Articles 25 and 26 of the Directive. While proof of *"adequacy"* of protections afforded by a third country is a requirement of Article 25, the SCC Decisions rest on Article 26(4), which pertains to situations where SCCs—and not the level of protection provided by the other country as such—are relied upon by the parties to the data transfer as offering adequate safeguards. The SCCs contain numerous safeguards and remedies for data subjects, including remedies that are directly enforceable against the transferring parties. If adequacy of protections in the destination country were a requirement for data exporters to rely on SCCs, then the very notion of SCCs would become meaningless, because data exporters could simply rely on the adequacy of protection under Article 25.[3] No adequacy assessment has been published in respect of many non-E.U. states to which data is transferred under the SCCs.

[2] Commission Decision 2001/497/EC OJ 2001 L 181/19; Commission Decision 2004/915/EC OJ 2004 L 385/74; Commission Decision 2010/87/E.U. OJ 2010 L 39/5.

[3] The concept of ensuring appropriate safeguards through use of contractual clauses is also enshrined in Chapter V of the recently-adopted General Data Protection Regulation, which states that SCCs are required only *"in the absence of a decision"* on adequacy of protection by the third country. Regulation (E.U.) 2016/679 of 27 April 2016.

7. Accordingly, assessments of *"adequacy"* within the meaning of Article 25(2) of protections afforded by the destination country should form no part of the assessment of the validity of the SCC Decisions, which turns on the question whether the SCCs therein contain *"sufficient safeguards"* within the meaning of Article 26(4).

8. Nonetheless, and without prejudice to that observation, the U.S. in this submission addresses the legal regime regarding government access to data in the U.S., with a focus on laws governing access to data for national security purposes (which was given particular attention in the Draft Decision). This submission does not address other arguments made by the parties, which may have considerable merit, concerning the validity of the DPC's decision and the proper standard to be applied. Rather, the U.S. seeks to ensure that the Court, if it considers it necessary to address the adequacy of U.S. laws, has a more complete understanding of these laws and the manner in which they protect individual privacy, including that of E.U. citizens whose data is transferred to U.S. companies.

B. Summary of Submission

9. U.S. law sets rigorous standards for government access to personal data in the U.S. These standards reflect a commitment to privacy that has been ingrained in the U.S. Constitution and laws since the founding of the republic. When examined as a whole, these standards for government access to personal data are *"essentially equivalent"* to the protections afforded under EU law, and meet the requirements of E.U. law which have been referred to as the "Essential Guarantees." Namely, U.S. law: (1) establishes clear and accessible rules for access to personal data; (2) ensures that data is collected for legitimate ends in accordance with principles of necessity and proportionality; (3) provides for meaningful independent oversight; and (4) affords effective remedies to individuals whose rights are violated.[4]

[4] These criteria are summarised by the Article 29 Data Protection Working Party, as based on the jurisprudence of the CJEU and the European Court of Human Rights ("**ECtHR**"). The Working Party is established under the Directive and is composed of the E.U. Member States' national data protection authorities and representatives from the European Data Protection Service and the European Commission. See "*Working Document 01/2016 on the Justification of Interferences with the Fundamental Rights to Privacy and Data Protection Through Surveillance Measures When Transferring Personal Data (European Essential Guarantees),"* at 6, 13 April 2016 (**"Article 29**

10. The European Commission, as part of establishing the Privacy Shield Framework, thoroughly examined U.S. laws governing access to personal data, including recent reforms such as Presidential Policy Directive 28 ("**PPD-28**") and the USA FREEDOM Act, and reached the same conclusions.[5] The Draft Decision, which pre-dated the European Commission's decision on Privacy Shield, expressly states that the DPC has *"not analysed or taken into account"* the arrangements contemplated by the Privacy Shield regime. The Commission's findings should be afforded significant weight by this Honourable Court, which must undertake any assessment of relevant U.S. law by reference to the current position.

11. The Draft Decision erred in focusing on only the issue of remedies available in U.S. law. In assessing relevant privacy protections in the U.S., it is critical to consider not only the existence of remedies but also the legal protections that exist *before*, *during*, as well as *after* government authorities collect information.[6] Moreover, remedies exist not just through individual causes of action, but through internal oversight and through oversight by the judicial and legislative branches of the government.

12. Furthermore, U.S. privacy protections regarding government access to data compare favourably to those of E.U. Member States. This comparison sheds important light on any "essential equivalence" analysis in this case, as many E.U. Member States have limited protections and remedies regarding collection of data for national security purposes. All States collect personal data for national security reasons; doing so is critical to their ability to protect their citizens' fundamental rights to liberty, safety, and security. In light of the elaborate privacy regime governing intelligence collection within the U.S., which is at least as strong and transparent as that in any E.U. Member State, transfer of personal data of

---

Working Party Document"), *available at* http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2016/wp237_en.pdf; see also, *e.g.*, *Schrems I*, para. 91.

[5] Commission Implementing Decision 2016/1250 of 12 July 2016 on the Adequacy of the Protection Provided by the E.U.-U.S. Privacy Shield ("**EC Adequacy Decision**"), OJ L207/1 of 1 August 2006, *available at* http://ec.europa.eu/justice/data-protection/files/privacy-shield-adequacy-decision_en.pdf. See especially recitals 64-141.

[6] See, *e.g.*, *Kennedy v UK*, para. 153, No. 26839/05 (ECtHR 2010) (entire regulatory framework must be assessed in considering whether privacy rights have been breached).

E.U. citizens to the U.S. poses no greater privacy concerns than transfer of such data among E.U. Member States.

13. As expressly confirmed by the CJEU in *Schrems I*, E.U. law does not require that U.S. or other foreign laws precisely replicate E.U. privacy protections as a condition to data transfer. If it did, it is highly unlikely that personal data could be transferred from E.U. Member States to anywhere outside the European Economic Area. In other areas of law respecting cooperation between nations, American and European courts have highlighted the need to allow for differences between legal systems.[7] Similar "margin of appreciation" principles should apply here. It is vital to global commerce and continued cooperation between the U.S. and Europe in a host of areas that each affords appropriate respect to the strong privacy regimes that exist on both sides of the Atlantic.

II. U.S. Privacy Protections Meet European Essential Guarantees.

14. The U.S. legal regime must be examined as a whole because numerous laws and policies comprehensively address government access to personal data in the U.S. Although there is no single data privacy statute, U.S. law thoroughly sets out rules and constraints regarding government access to personal data. Taken together, these laws afford privacy protections and remedies that are essentially equivalent to those provided under E.U. law.

A. Principles of E.U. Law for Assessing U.S. Privacy Protections

15. As the CJEU emphasized in *Schrems I*, "*a third country cannot be required to ensure a level of protection identical to that guaranteed in the E.U. legal order,*" and the means through which a third country protects the right to privacy "*may differ from those employed within the European Union.*"[8] Furthermore, as Article 52(1) of the Charter makes clear, interferences with basic rights, including the right to privacy, may be justified

[7] See, *e.g., Bosphorus Airways v Ireland* (judgment of the Grand Chamber of 30 June 2005, Application no. 45036/98) (declining to review the compatibility of individual provisions of E.U. law with the European Convention on Human Rights ("**ECHR**") as long as the rights protection provided by E.U. law, viewed as a whole, was "*equivalent*" to that provided by the ECHR).
[8] *Schrems I*, paras. 73, 74.

if they are provided for by law, respect the essence of the right, and are proportionate to "*objectives of general interest recognized by* the *Union or the need to protect the rights and freedoms of others.*" The CJEU has noted that the need to maintain security constitutes an objective of general interest[9] and that surveillance measures, including secret measures, may be justifiable means to protect public safety.[10] Efforts to combat terrorism and serious crime are of *"the utmost importance."*[11] *"Moreover, the protection of national security and public order also contributes to the protection of the rights and freedoms of others,"* as the Charter guarantees *"the right of any person not only to liberty, but also to security."*[12]

16. The European Court of Human Rights ("**ECtHR**")[13] has also "*consistently recognise*[d] *that* [Member] *States have a fairly wide margin of appreciation in choosing the means for achieving the legitimate aim of protecting national security,"*[14] and that courts should not substitute their own assessments for those of national authorities regarding the appropriate means for protecting national security.[15]

17. Because surveillance measures must often be carried out secretly,[16] the CJEU and ECtHR have emphasised the need to build effective safeguards into legal regimes. These safeguards include rules concerning the scope of permissible surveillance; authorisation procedures; limitations on duration; and limitations on access to data obtained by authorities.[17] While courts have recognised the importance of effective remedies, they have also acknowledged that the right to a remedy does not require authorities to provide

[9] See, *e.g.*, Judgment of 8 April 2014, *Digital Rights Ireland and Seitlinger and Others*, Joined cases C-293/12 and C-594/12, EU:C:2014:238, para. 42; Judgment of 3 September 2008, *Kadi and Al Barakaat International Foundation* v *Council and Commission*, C-402/05 P and C-415/05 P, E.U.:C:2008:461, para. 363.
[10] See, *e.g.*, discussion in Opinion of Advocate General Saugmandsgaard Øe in *Tele2 Sverige*, Joined Cases C-203/15 and C-698/15, EU:C:2016:572, at paras. 177-184, and case-law cited.
[11] *Digital Rights Ireland*, para. 51.
[12] *Id.* para. 42.
[13] While the ECHR and ECtHR jurisprudence are not part of E.U. law as such, other foundational laws of the E.U. recognise that the ECHR informs the scope of basic human rights protections. See Treaty on European Union Art. 6(3); Charter of Fundamental Rights of the European Union, Art. 53; Judgment of 5 October 2010, *McB v. L.E.*, C-400/10, EU:C:2010:582, para 53.
[14] Article 29 Working Party Document at 5; see also, *e.g.*, *Zakharov v Russia*, para. 232, No. 47143/06 (ECtHR 2015).
[15] *Klass and others v. Germany*, para. 49, No. 5029/71 (ECtHR 1978).
[16] *Id.* para. 48.
[17] *Schrems I*, para. 91; see also *Szabo and Vissy v. Hungary*, para.56, No. 37138/14 (ECtHR 2016).

notice to affected individuals if providing such notice would undermine an investigation or compromise intelligence methods.[18] Rather, if providing notice is impracticable, effective remedies can take other forms, including through independent oversight.[19]

B. U.S. Legal Authorities Governing National Security Investigations Meet European Essential Guarantees.

18. U.S. law governing access to personal data for national security investigations meets the "essential equivalence" standard articulated in *Schrems I*. More precisely, U.S. law *"lay[s] down clear and precise rules governing the scope and application of [surveillance] measure[s] and impos[es] minimum safeguards, so that persons whose personal data is concerned have sufficient guarantees enabling their data to be effectively protected against the risk of abuse."*[20] These provisions have been developed over decades to protect both public safety and the privacy interests of all individuals affected. Investigative activities in the U.S. are subject to rigorous oversight from many independent authorities. And the U.S. legal system provides a number of means for redress for unwarranted invasions of privacy.

19. The only data access at issue in this case is access to E.U. citizens' personal data that are transferred to businesses in the U.S. under the SCCs. The crux of Mr Schrems' Reformulated Complaint is that if his personal data is transferred from Facebook's server in Ireland to a server in the U.S., it could become subject to collection by U.S. government authorities. Accordingly, this Court should address only the laws concerning U.S. government access to data stored or accessible within the U.S. Although the United States collects intelligence abroad—as do E.U. Member States—those activities and legal provisions are not relevant to assessing the protections afforded to data transferred to and stored by businesses in the U.S.[21]

---

[18] See *Zakharov*, para. 287; *Weber and Saravia*, para 135.
[19] *Klass*, paras 59, 67-68; see also *Weber and Saravia*, para 136.
[20] *Schrems I*, para. 91.
[21] That said, the U.S. has legal and policy constraints and a level of transparency regarding its intelligence activities abroad, including with respect to non-U.S. persons, that few (if any) other countries have imposed on their intelligence services. See Affidavit of Mr Swire ("**Swire**"), Ch. 3, paras. 16-25, for further description of PPD-28, which applies to all signals intelligence collection activities, including those that occur abroad.

1. Access to personal data is governed by clear, accessible rules.

20. Legal provisions governing access to personal data in the U.S. for national security purposes are clear and comprehensive. They build on the fundamental guarantee in the Fourth Amendment to the United States Constitution, which provides that "[t]*he 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*." Although the Fourth Amendment generally does not apply to searches of non-U.S. persons located abroad,[22] it does typically govern searches of non-U.S. persons and their property if they are located in the U.S.,[23] including through electronic surveillance.[24] Additionally, most statutory limitations on government searches or demands for personal data in the U.S. generally apply without regard to nationality, with the qualifications discussed below.

21. The Foreign Intelligence Surveillance Act ("**FISA**") is the principal legal provision governing access to personal data for foreign intelligence and national security purposes inside the U.S. FISA was first enacted in 1978, and it "*embodie*[d] *a legislative judgment that court orders and other procedural safeguards are necessary to* [e]*nsure that electronic surveillance by the U.S. Government within this country conforms to the fundamental principles of the Fourth Amendment.*"[25] All parts of the statute (including all subsequent amendments) are public and are contained within Title 50 of the U.S. Code.

22. FISA constrains the U.S. government's authority to conduct intelligence-gathering in the U.S., including by creating a specialised, fully independent court of judges with life tenure (the "**FISC**") that authorises electronic surveillance, physical searches, and other related activities for national security purposes.[26] Pursuant to provisions of "traditional" FISA (that is, provisions other than Section 702, discussed below), government authorities must

[22] See *United States v. Verdugo-Urquidez*, 494 U.S. 259 (1990).
[23] See *id.* at 278 (Kennedy, J., concurring); see also Swire, Ch. 3, para. 4.
[24] See generally *Katz v. United States*, 389 U.S. 347 (1967).
[25] *United States v. Duggan*, 743 F.2d 59, 73 (2d Cir. 1984) (quoting Senate Report No. 95-701, at 13 (1978)).
[26] 50 U.S.C. § 1803.

obtain orders from the FISC on an individualised basis to conduct electronic surveillance or physical searches as defined in the law. While traditional FISA was generally intended to govern such activities when directed at individuals (regardless of nationality) inside the U.S., it also applies to certain types of activities aimed at non-U.S. persons outside the U.S. (*e.g.*, certain requests for business records, as discussed below).

23. To obtain an order authorising electronic surveillance or a physical search, the government must demonstrate to the FISC *"probable cause"* that, among other things, the target is *"a foreign power or an agent of a foreign power."*[27] FISA describes the exclusive categories of persons and entities that may qualify as *"foreign powers"* or *"agents of a foreign power"*—principally, foreign governments, international terrorist groups or proliferation networks, and their agents.[28] It requires that a *"significant purpose"* of the collection must be to gather *"foreign intelligence information,"* which it defines as five specific categories of information that relate to the government's ability to protect against foreign attack, terrorism, proliferation of weapons of mass destruction, and other threats, or to conduct foreign affairs.[29] Accordingly, intelligence activities governed by traditional FISA meet the standard that the legal basis for access to data be clear and accessible.

24. Section 702 of FISA (contained in Title VII) was enacted in 2008 as a limited exception to the requirement for individualised court authorization to conduct electronic surveillance or physical searches. It authorises the government to issue "directives" to electronic communications service providers in the U.S. to acquire foreign intelligence information where the target of surveillance is a non-U.S. person reasonably believed to be located outside the U.S.[30] While Section 702 does not require individualised orders from the FISC, the FISC maintains judicial oversight and regulation of such collection activities. Before the government may issue directives to service providers, the FISC must approve a written certification by the Attorney General and the Director of National Intelligence ("**DNI**") jointly authorising the collection activities for up to one year.[31] The certification must

[27] *Id.* §§ 1805(a)(2), 1824(a)(2).
[28] *Id.* §§ 1801(a), (b).
[29] *Id.* § 1801(e).
[30] As relevant, the term "U.S. person" includes U.S. citizens and lawful permanent residents. *Id.* § 1801(i).
[31] *Id.* §§ 1881a (a), (g).

attest that a significant purpose of the acquisition is to obtain foreign intelligence information, *e.g.*, intelligence related to international terrorism. The certification must also include targeting and minimisation procedures (*i.e.*, regulations regarding acquisition, access to, and retention of data), which the FISC must determine are consistent with the statute and the Fourth Amendment.[32] It is therefore likewise submitted that, in the case of intelligence activities governed by Section 702 of FISA, the legal basis for access to data is clear and publicly available.

25. Procedures for obtaining information other than the contents of communications on national security grounds are also set out in detail in FISA. Title IV authorises the use of pen registers and trap-and-trace devices to obtain data pertaining to the phone numbers or e-mail addresses of communicants (but not the contents of communications) pursuant to a court order in connection with authorised foreign intelligence, counterintelligence, or counterterrorism investigations.[33] (A pen register is a device that records all numbers dialed from a particular telephone line; a trap-and-trace device shows incoming numbers dialed to connect to a particular telephone line. These devices also operate in analogous manners for e-mail communications, *e.g.*, by recording e-mail addresses of communicants, but not the contents of communications.[34]) Title V permits the Federal Bureau of Investigation ("**FBI**") to apply to the FISC for an order directing production of business records or other tangible things that are relevant to a national security investigation and that could, in analogous law enforcement circumstances, be obtained pursuant to a grand jury subpoena or other order issued by a U.S. court (*e.g.*, records held by a third party).[35] Where applicable, these authorities operate regardless of the nationality or location of the individual who is targeted for collection.

26. The DNI has declassified and released certain significant opinions of the FISC governing traditional FISA and Section 702.[36] The USA FREEDOM Act, enacted in 2015, provides additional transparency measures respecting FISA. It requires prospective declassification

[32] *Id.* § 1881a(d).
[33] *Id.* § 1842.
[34] See 18 U.S.C. § 3127(3), (4).
[35] 50 U.S.C. § 1861.
[36] All public filings of the FISC, including declassified opinions, are available at www.fisc.uscourts.gov.

or publication of an unclassified summary of each decision issued by the FISC or the Foreign Intelligence Surveillance Court of Review ("**FISC-R**") that includes a significant construction or interpretation of any legal provision.[37] It also requires the government to disclose annually the number of FISA orders and certifications sought and approved and to provide estimates of the number of U.S. persons and non-U.S. persons targeted and affected by surveillance.[38] Furthermore, it authorises companies that have received FISA orders or other national security demands for data to publish certain aggregate data concerning the process they receive.[39]

27. The other legal bases for access to personal data for national security purposes are also public and provide clear standards enforceable by U.S. courts. Five statutes authorise investigators to issue National Security Letters ("**NSLs**") in connection with authorised national security investigations.[40] NSLs, like subpoenas, allow investigators to request certain basic information from specified third parties, such as telephone or banking records from phone companies and financial institutions. Courts have not hesitated to enforce these statutes to limit government authority.[41] Again, legal provisions respecting NSLs apply regardless of the nationality or the location of the individual whose records are sought.

28. Finally, PPD-28, signed by President Obama in 2014, and which is legally binding within the Executive Branch of the U.S. Government,[42] sets out a series of principles and requirements that apply to all U.S. signals intelligence activities, including collection under Section 702 of FISA, in order to afford basic privacy safeguards for all people, regardless of nationality or location. It provides that signals intelligence collection must be *"as*

[37] 50 U.S.C. § 1872.
[38] 50 U.S.C. § 1873.
[39] *Id.* § 1874.
[40] See 12 U.S.C. § 3414; 15 U.S.C. §§ 1681u and v; 18 U.S.C. § 2709; and 50 U.S.C. § 3162.
[41] See *Doe v. Mukasey*, 549 F.3d 861 (2d Cir. 2008).
[42] While PPD-28, like other Presidential directives, may be amended or repealed, it remains legally binding unless or until that occurs. PPD-28 is exhibited at Ms. Gorski's Exhibit AG2, item 3 and is also available at https://www.whitehouse.gov/the-press-office/2014/01/17/presidential-policy-directive-signals-intelligence-activities.

tailored as feasible" and extends to non-U.S. person information certain protections already afforded to the personal information of U.S. persons.[43]

2. U.S. legal provisions are reasonably tailored to serve legitimate public safety needs.

29. E.U. law recognises that interferences with the right to privacy are permissible if they are provided for by law, respect the essence of the right, and are justified by and proportionate to a legitimate objective.[44] U.S. national security authorities are constrained by the Fourth Amendment, which provides a fundamental protection against "*unreasonable searches and seizures."* The founders of the United States wrote this requirement into the Constitution to prevent government officials from having "*blanket authority to search where they pleased."*[45]

30. The U.S. Supreme Court has described "reasonableness" as "*the ultimate touchstone of the Fourth Amendment."*[46] While this "reasonableness" standard does not use the same terms as the E.U. system's concepts of necessity and proportionality, the frameworks contain fundamental similarities. As the U.S. Supreme Court has held, "[w]*hether a search is reasonable is determined by assessing, on the one hand, the degree to which it intrudes upon an individual's privacy, and, on the other, the degree to which it is needed for the promotion of legitimate governmental interests."*[47] And "[w]*hat is reasonable"* will "*depend… on all of the circumstances surrounding the search or seizure and the nature of the search or seizure itself."*[48]

[43] Although not relevant here, U.S. collection of intelligence overseas is generally defined and limited by Executive Order 12,333. E.O. 12,333 describes the scope and purposes of U.S. intelligence collection authorities in detail and is available at https://www.cia.gov/about-cia/eo12333.html. Collection activities under E.O. 12,333, like all foreign intelligence collection activities, are limited to specific intelligence priorities, such as nuclear proliferation, terrorism, and espionage. See Letter from Robert Litt, General Counsel of the Office of the DNI, dated 22 February 2016, at 4-6 (Annex VI to the Privacy Shield documents) ("**Litt Letter**"), *available at* http://ec.europa.eu/justice/data-protection/files/privacy-shield-adequacy-decision-annex-6_en.pdf.
[44] See discussion in Section II.A, *supra*, and Article 52(1) of the Charter.
[45] *Stanford v. State of Texas*, 379 U.S. 476, 481 (1965).
[46] *Kentucky v. King*, 563 U.S. 452, 459 (2011).
[47] *Samson v. California*, 547 U.S. 843, 848 (2006).
[48] *Skinner v. Railway Labor Execs. Ass'n*, 489 U.S. 602, 619 (1989).

31. Congress enacted FISA with the express purpose of building a "*secure framework by which the Executive Branch may conduct legitimate electronic surveillance for foreign intelligence purposes within the context of this Nation's commitment to privacy and individual rights.*"[49] Consistent with that aim, surveillance conducted under FISA is tailored to serve legitimate public safety needs.

32. Pursuant to "traditional" FISA provisions, the government must make individual applications to the FISC to conduct electronic surveillance or physical searches, or otherwise to obtain certain records for national security purposes. These requirements to make individualised applications apply regardless of the nationality of the individual targeted. Applications for electronic surveillance or for physical searches must specify both the target of the surveillance or search and each facility (*e.g.*, e-mail account or telephone number) or place at which the surveillance or search will be directed.[50] As noted above, the government must show probable cause that the target of the surveillance or search is a "*foreign power*" or an "*agent of a foreign power*"; it must also show probable cause that any electronic surveillance or physical search is directed at facilities or premises being used by or owned by a foreign power or agent of a foreign power.[51] Additionally, applications for electronic surveillance or physical searches must certify that the information sought is foreign intelligence information and may not reasonably be obtained by normal investigative techniques.[52] Orders targeting suspected agents of foreign powers who are not U.S. persons may be authorised for a maximum of 120 days (subject to applications for extension).[53] U.S. courts, taking into account these and other important safeguards, have repeatedly upheld traditional FISA provisions as consistent with the Fourth Amendment.[54]

33. Surveillance under Section 702 is likewise tailored to serve legitimate public safety needs. Section 702 authorises collection against non-U.S. persons located outside the U.S.,

[49] *Duggan*, 743 F.2d at 73 (quoting Senate Report No. 95-604, pt. 1 (1977)).
[50] 50 U.S.C. §§ 1804(a), 1823(a).
[51] *Id.* §§ 1805(a)(2)(B), 1824(a)(2)(B).
[52] *Id.* §§ 1804(a)(6)(C), 1823(a)(6)(C).
[53] *Id.* § 1805(d)(1).
[54] See, *e.g.*, *Duggan*, 743 F.3d 59; *United States v. Abu-Jihaad*, 630 F.3d 102, 119-29 (2d Cir. 2010); *United States v. Duka*, 671 F.3d 329, 336-45 (3d Cir. 2011).

conducted with the compelled assistance of electronic communications service providers in the U.S. Although each individual directive does not need to be approved by the FISC, the FISC must approve procedures for targeting collection activities that are set out in the annual certifications, which must also attest that obtaining foreign intelligence (as further defined through specific categories of information) is a significant purpose of the collection.[55]

34. The Privacy and Civil Liberties Oversight Board ("**PCLOB**"), an independent oversight body, conducted a comprehensive assessment of collection activities under Section 702 and concluded that this provision *"has proven valuable in the government's efforts to combat terrorism as well as in other areas of foreign intelligence."*[56] It also concluded that collection activities conducted under Section 702 are not mass or indiscriminate. Rather, they *"consist… entirely of targeting specific persons about whom an individualized determination has been made."*[57] To target any individual, the government must have reason to believe the individual will communicate foreign intelligence information covered by a particular certification.[58] Collection is carried out through use of individual "selectors," which identify a particular facility such as an e-mail address or telephone number, that is assessed to be used by the target of the acquisition.[59] As the PCLOB has noted, selectors *cannot* consist of general "key words" such as "bomb" or "attack," or even names of individuals, because such terms would not identify specific communications facilities.[60] Consistent with these conclusions, there were approximately 94,368 targets worldwide affected by surveillance under Section 702 in 2015, a miniscule fraction of the over 3 billion internet users worldwide.[61]

---

[55] 50 U.S.C. § 1881a(g).
[56] Privacy and Civil Liberties Oversight Board, "Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act," at 10 (22 July 2014) ("**PCLOB 702 Report**"), *available at* https://www.pclob.gov/library/702-Report.pdf; .
[57] *Id.* at 103; see also EC Adequacy Decision, para. 81.
[58] PCLOB 702 Report at 22.
[59] *Id.* at 32.
[60] *Id.* at 33; see also Swire, Ch. 3, paras. 59-69. As the PCLOB 702 Report and Mr Swire make clear, Section 702 collection does not operate through generalized or "bulk" access to the servers of U.S. internet companies.
[61] Director of National Intelligence 2015 Transparency Report, *available at* https://icontherecord.tumblr.com/transparency/odni_transparencyreport_cy2015.

35. Moreover, collection under Section 702 (like information collected under traditional FISA) is subject to court-approved minimisation procedures. These procedures, which have been publicly released, focus on U.S. persons but also provide important protections to non-U.S. persons.[62] For example, communications acquired under Section 702 must be stored in databases with strict access controls, and the data can only be queried to identify foreign intelligence information or, in the case of the FBI only, to obtain evidence of a crime.[63] Further privacy measures adopted in accordance with PPD-28 also apply to collection under Section 702.[64] These procedures contain limitations, for example, with respect to how long non-U.S. persons' data may be retained, and the circumstances under which data can be queried or disseminated, that are comparable to the privacy protections applicable to U.S. persons.[65]

36. The FISC-R concluded in 2008 that a predecessor law to Section 702, which contained similar provisions, had a *"matrix of safeguards"*—including *"targeting procedures, minimization procedures,* [and] *a procedure to ensure that a significant purpose of the surveillance is to obtain foreign intelligence information"*— and, as such, was constitutionally reasonable with respect to U.S. persons.[66] More generally, the court made clear that it was not *"endors*[ing] . . . *broad-based, indiscriminate executive power,"* because the government had *"instituted several layers of serviceable safeguards to protect individuals against unwarranted harms and to minimize incidental intrusions."*[67] Several other courts have since affirmed the lawfulness of Section 702 as applied in particular instances.[68]

---

[62] The minimisation procedures pertaining to Section 702 collection are available at http://www.dni.gov/files/documents/ppd-28/2014%20NSA%20702%20Minimization%20Procedures.pdf (NSA); http://www.dni.gov/files/documents/ppd-28/2014%20FBI%20702%20Minimization%20Procedures.pdf (FBI); and http://www.dni.gov/files/documents/ppd-28/2014%20CIA%20702%20Minimization%20Procedures.pdf (CIA).

[63] See, *e.g.*, NSA Minimization Procedures at 6.

[64] See, *e.g.*, NSA PPD-28 Section 4 Procedures, *available at* https://www.dni.gov/files/documents/ppd-28/NSA.pdf.

[65] Pursuant to PPD-28 Section 4(a)(i), to the maximum extent feasible, personal information may only be disseminated or retained if comparable information concerning U.S. persons could be disseminated or retained under Section 2.3 of E.O. 12,333.

[66] *In re Directives Pursuant to Section 105B of the Foreign Intelligence Surveillance Act*, 551 F.3d 1004, 1013 (FISC-R 2008).

[67] *Id.* at 1016.

[68] *United States v. Mohamud*, No. 14-30217, 2016 WL 7046751, at *15-20 (9th Cir. Dec. 5, 2016); *United States v. Hasbajrami*, No. 11-cr-623, 2016 WL 1029500, at *13(E.D.N.Y. Mar. 8, 2016) (noting that the targeting that occurred *"was as particular as it gets"* because *"the FISC approved the targeting of specific non-U.S. persons outside the United States for specific counter-terrorism purposes"*).

37. With respect to information other than the contents of communications, such as the telephone numbers of communicants or business records held by third parties, U.S. national security authorities are also carefully tailored. An order from the FISC is required for the government to use pen registers or trap-and-trace devices under Title IV of FISA. The government official seeking the order must certify that the information likely to be obtained is foreign intelligence information not concerning a U.S. person, or that the information is relevant to an ongoing investigation to protect against international terrorism or clandestine intelligence activities.[69] The FISC must generally specify the identity of the person who is the subject of the investigation and the person in whose name is listed the telephone line or other facility to which the device is to be applied.[70]

38. To collect business records under Title V of FISA, the government must apply for an order from the FISC and must show that the records sought are relevant to an authorised national security investigation.[71] Recipients of these orders may challenge them in the FISC, and FISC judges may set aside orders that do not meet the statutory requirements or are otherwise unlawful.[72] The USA FREEDOM Act enacted further limitations: it expressly prohibits bulk collection of any records—including of non-U.S. persons—pursuant to FISA authorities or through use of NSLs.[73] To seek business records under FISA, the government must base requests on a *"specific selection term"*—that is, a term that specifically identifies a person, account, address, or personal device—in a way that limits the scope of information sought to the greatest extent reasonably practicable.[74]

39. Finally, with respect to signals intelligence collection (including pursuant to Section 702 as well as collection abroad), PPD-28 requires that signals intelligence activities be *"as tailored as feasible"* and that privacy and civil liberties, including those of non-U.S. persons, must be *"integral considerations in the planning of U.S. signals intelligence activities."* Furthermore, it directs all intelligence agencies to adopt procedures,

[69] 50 U.S.C. § 1842(c).
[70] *Id.* § 1842(d)(2).
[71] *Id.* § 1861(b)(2).
[72] *Id.* § 1861(f)(2).
[73] 18 U.S.C. §§ 103, 201, 501.
[74] 50 U.S.C. § 1861(k)(4).

irrespective of nationality, *"reasonably designed to minimize the dissemination and retention of personal information collected from signals intelligence activities."*[75]

3. U.S. national security authorities are subject to independent oversight.

40. As the European Commission has noted, the U.S. conducts extensive oversight of national security authorities through all three government branches.[76]

41. *First*, the U.S. legal system empowers independent federal judges with robust oversight authorities. Any authorisation under FISA to compel disclosure of personal data held in the U.S., regardless of the nationality or location of the target, must be given in advance by a judge or must be subject to judicial oversight. The FISC judges are independent life-tenured federal judges nominated by the President and confirmed by the Senate.[77]

42. Activity under traditional FISA authorities must be authorised in advance by a FISC judge, except in emergency circumstances, in which case a judge must be notified immediately and an application made within seven days of the non-judicial authorisation.[78] FISC judges oversee surveillance conducted under Section 702 through prior approval of the government's targeting and minimisation procedures and through annual certifications submitted to and approved by the FISC.[79] As described in detail in Chapter 5 of Mr Swire's report, the FISC also plays a robust oversight role in enforcing compliance with its orders, including by demanding that the government take remedial action where necessary.[80]

---

[75] Although other signals intelligence activities conducted abroad (*i.e.*, those not governed by FISA) are not relevant here for the reasons explained, the DNI has represented that *"whenever practicable,"* these activities *"are conducted in a targeted manner rather than in bulk."* Litt Letter at 3. Even when the intelligence community is unable to collect signals intelligence in a more targeted manner, PPD-28 limits the use of signals intelligence collected in "bulk" to purposes of detecting and countering six specific types of serious threats to U.S. national security. See *id.* at 3; PPD-28 Section 2. As such, the European Commission has concluded that *"these principles capture the essence of the principles of necessity and proportionality."* EC Adequacy Decision, para. 76.
[76] *Id.* paras. 25-31.
[77] 50 U.S.C. § 1803.
[78] *Id.* §§ 1805(e), 1824(e).
[79] *Id.* § 1881a(g).
[80] Swire, Ch. 5 paras. 62-107.

43. The USA FREEDOM Act further strengthens the FISC's ability to safeguard privacy interests. The law empowers the FISC to appoint *amici curiae* in cases presenting novel or significant issues. An *amicus* may have access to classified materials and may make *"legal arguments that advance the protection of individual privacy and civil liberties."*[81] The Act also strengthens appeal mechanisms by allowing the FISC to certify issues for review by the FISC-R where further review *"would serve the interests of justice."*[82] When an appeal is certified, the FISC-R may also appoint an *amicus*.[83]

44. *Second*, numerous oversight mechanisms are built into the Executive Branch.[84] All applications to the FISC to conduct electronic surveillance or physical searches must be personally approved by the Attorney General, the Deputy Attorney General, or the Assistant Attorney General for National Security, as well as by other relevant senior national security officials.[85] Each government agency that conducts intelligence collection activities has its own internal oversight staff who are required to report violations of the law and of applicable regulations to their agencies' leadership and to the FISC, when warranted. Moreover, these agencies have independent Inspectors General who are empowered to conduct investigations into wrongdoing and may review classified materials.[86] The DNI, as well as attorneys in the National Security Division at the Department of Justice, conduct further independent oversight of intelligence agencies' compliance with FISA and ensure the accuracy of applications made to the FISC.[87]

45. The PCLOB, as described above, is an additional oversight body within the Executive Branch empowered to conduct broader assessments of U.S. intelligence programs and to make independent recommendations. Board members are nominated by the President and

---

[81] 50 U.S.C. § 1803(i).
[82] 50 U.S.C. § 1803(j).
[83] This year, for example, the FISC certified a question for the FISC-R concerning FISA's pen register provision and the ability of the government to collect dialing information if that information includes numbers dialed after a call has been placed. The FISC-R appointed an *amicus* to argue against the government's position, received briefings from both sides and heard arguments, and then issued a public opinion with minimal redactions. *In re Certified Question of Law*, FISC-R No. 16-01 (Apr. 14, 2016), *available at* http://www.fisc.uscourts.gov/sites/default/files/FISCR%20Opinion%2016-01%20Redacted.pdf.
[84] For further discussion of internal oversight mechanisms, see Report of Mr John DeLong ("**DeLong**"), paras. 78-98; see also Swire Ch. 5, paras. 55-61.
[85] 50 U.S.C. §§ 1801(g), 1804(a), 1823(a).
[86] Litt Letter at 7-8.
[87] *Id.*

confirmed by the Senate, and may access classified information to conduct their oversight responsibilities. The PCLOB has not hesitated to criticise government surveillance activities. After the Snowden disclosures, it conducted extensive studies of the implementation of Section 702 and the government's bulk collection of certain non-content telephone metadata under the FISA Title V business records provision. The PCLOB's report on the telephony metadata programme concluded that it was not consistent with the statute, raised serious privacy concerns, and did not provide any uniquely significant intelligence value.[88] By contrast, the PCLOB concluded that Section 702 serves valuable public safety functions and has been implemented consistent with the law, though it also made recommendations to strengthen privacy protections.[89] Congress drew significantly from the report on the telephony metadata programme in enacting the USA FREEDOM Act, which expressly prohibits bulk collection in the U.S. under FISA and other laws.

46. *Third*, the U.S. Congress exercises numerous oversight authorities over intelligence collection activities. The House and Senate Select Committees on Intelligence were created in the 1970s to guard against abuses by government authorities. Members have access to classified information, and the President is required by law to keep the committees *"fully and currently informed of the intelligence activities"* of the government.[90] The committees have the authority to issue subpoenas for testimony or written materials and to hold hearings, in public or in private, and they receive frequent briefings from intelligence and oversight officials. The Attorney General and the DNI are required by law to make regular reports to the intelligence and judiciary committees of the House and the Senate regarding the use of FISA authorities (including Section 702) and to report compliance incidents.[91] Thus, all three branches of the U.S. government are actively involved in overseeing intelligence collection under FISA and ensuring that privacy and civil liberties are protected.

[88] See PCLOB, "Report on the Telephone Records Program Conducted Under Section 215 of the USA PATRIOT Act and on the Operations of the Foreign Intelligence Surveillance Court" (13 January 2014), *available at* https://www.pclob.gov/library/215-Report_on_the_Telephone_Records_Program.pdf.
[89] See generally PCLOB Section 702 Report.
[90] 50 U.S.C. § 3091(a).
[91] See 50 U.S.C. §§ 1808, 1826, 1846, 1862, 1871, 1873, 1881f.

4. Effective remedies exist for unwarranted invasions of privacy.

47. If the U.S. government exceeds the bounds of these provisions, effective remedies exist at the individual and systemic levels. U.S. law concerning individual remedies for privacy invasions operates primarily in two ways: through the exclusion of unlawfully obtained evidence in legal proceedings and through individual lawsuits. With respect to exclusion of evidence, the U.S. Supreme Court held over a century ago that, in order to give *"force and effect"* to the protections of the Fourth Amendment, evidence seized from an individual in violation of the Fourth Amendment generally cannot be used against him in a criminal trial.[92]

48. While the exclusionary rule was initially developed by the courts to remedy Fourth Amendment violations, Congress has expanded upon it in the context of FISA. FISA requires the government to notify any *"aggrieved person"* if it seeks to use evidence obtained or derived from FISA surveillance against that individual in any legal proceeding.[93] The person given notice can apply to exclude the evidence on the grounds that the surveillance was unlawful—*e.g.*, because it violated the Fourth Amendment, the terms of the statute, or the scope of a particular FISC order.[94] These provisions apply irrespective of nationality and have been invoked by non-U.S. persons charged with offences in the U.S. If the reviewing court determines that the collection was unlawful, it must exclude the evidence.[95] The same notice and exclusion mechanisms apply with respect to surveillance conducted under Section 702.[96] The government has given notice of the use of FISA-derived evidence in many criminal cases—including notice of Section 702 surveillance to non-U.S. persons—and defendants including non-U.S. persons have been able to challenge the lawfulness of the underlying collection before independent courts at their trials.[97]

---

[92] *Weeks v. United States*, 232 U.S. 383 (1914); see also *Mapp v. Ohio*, 367 U.S. 643 (1961).
[93] 50 U.S.C. §§ 1806(c), 1825(d), 1845(c). An "aggrieved person" is a person who was the target of the collection or whose communications or activities were subject to collection. *Id.* §§ 1801(k), 1821(1).
[94] *Id.* §§ 1806(e), 1825(f), 1845(e).
[95] *Id.* §§ 1806(g), 1825(h).
[96] *Id.* § 1881e.
[97] See, *e.g.*, *United States v. Turner*, 840 F.3d 336 (7th Cir. 2016); *United States v. Aldawsari*, 740 F.3d 1015, 1018-19 (5th Cir. 2014) (involving a Saudi national). In the *Mohamud* and *Hasbajrami* cases cited above, notice of

49. Of course, these notice and exclusion provisions only apply if the government seeks to use FISA-derived evidence in legal proceedings against an aggrieved person. As the Draft Decision notes, the exclusion remedy is not a *"free-standing mechanism."* But it is incorrect to conclude that the exclusion remedy is merely *"a defensive protection of the individual."* In addition to protecting individuals in specific cases, the exclusion of unlawfully obtained evidence serves to *"deter [government] misconduct"*[98] on a systemic level by ensuring that if officials cut corners or violate the law, they sabotage their own ability to bring effective prosecutions or other legal proceedings. Moreover, these provisions allow courts to consider broader questions, such as the lawfulness of collection authorities and programmes, that have implications far beyond any individual case.

50. Second, individuals may initiate civil lawsuits in federal courts for violations of FISA. An aggrieved person whose communications, records, or other information were used or disclosed unlawfully may sue the individual who committed the violation and recover compensatory damages, punitive damages, and attorney's fees.[99] Additionally, individuals have sought and in some cases have obtained a judicial remedy for allegedly unlawful government access to personal data through civil actions under the Administrative Procedure Act ("**APA**"), a statute that allows persons *"suffering legal wrong because of"* certain government conduct to seek a court order enjoining that conduct.[100] For example, a recent challenge under the APA resulted in a decision by a U.S. Court of Appeals holding both that the bulk collection of telephone metadata under Title V of FISA could be challenged as exceeding, and did in fact exceed, the Government's authority under the statute.[101]

Section 702 collection was given to defendants. In a pending case, *United States v. Mohammad*, No. 3:15-cr-00358 (N.D. Ohio), notice of Section 702 collection has been provided to several defendants, one of whom is a citizen of India.

[98] *Arizona v. Evans*, 514 U.S. 1, 11 (1995).

[99] 50 U.S.C. § 1810; see also *id.* § 1828 (similar provision with respect to physical searches); 18 U.S.C. § 2712 (providing a civil remedy against the U.S. Government for willful violations of various FISA provisions).

[100] 5 U.S.C. § 702.

[101] *ACLU v. Clapper*, 785 F.3d 787 (2d Cir. 2015). Other courts, agreeing with the Government, have reached contrary rulings on both points. See *Klayman v. Obama*, 957 F. Supp. 2d 1, 19-25 (D.D.C. 2013) (finding that plaintiffs could not bring suit under the APA alleging violations of the statute, but could bring suit alleging violations of the Fourth Amendment), *vacated*, 800 F.3d 559 (D.C. Cir. 2015); *In re Application of the FBI*, No. BR

51. The Draft Decision contends that these and other remedial provisions do not satisfy Article 47 of the Charter because, *e.g.*, certain remedies only apply against government employees but not the government itself, while others require demonstration of a "willful" violation. These alleged deficiencies ignore the fact that, while Article 47 provides a right to an "*effective remedy*," it certainly does not prescribe the exact form that such remedy must take, the appropriate standards of proof, and the appropriate defendant.[102] Moreover, suits against government employees can provide a mechanism for obtaining damages under U.S. law, and the government often indemnifies such employees and pays any damages awarded.[103]

52. More broadly, the Draft Decision is highly critical of U.S. constitutional standing doctrine. To bring a lawsuit for an invasion of privacy, an individual must plausibly allege that he or she is (or is about to be) the subject of surveillance activity.[104] The requirement that a plaintiff allege a concrete injury stems from Article III of the U.S. Constitution, which establishes the powers and limitations of federal courts. As the U.S. Supreme Court has explained,

> *"Article III of the Constitution confines the judicial power of federal courts to deciding actual 'Cases' or 'Controversies.' One essential aspect of this requirement is that any person invoking the power of a federal court must demonstrate standing to do so. This requires the litigant to prove that he has suffered a concrete and particularized injury that is fairly traceable to the challenged conduct, and is likely to be redressed by a favorable judicial decision. In other words, for a federal court to have authority under the Constitution to settle a dispute, the party before it must seek a remedy for a personal and tangible harm. The presence of a disagreement, however sharp*

13-109, 2013 WL 5741573, at *3-9 (FISC Aug. 29, 2013) (holding that the programme was consistent with the statute).

[102] See Opinion of AG Mengozzi in *Opinion 1/15* (E.U.-Canada PNR Agreement), para. 326. See also the discussion in S. Peers et al (eds.), "The E.U. Charter of Fundamental Rights: A Commentary" (Bloomsbury, 2013), at 47.53 and at 47.115 onwards, who consider that Article 47 requires damages to be payable only as a "last resort" in extreme cases.

[103] See Vladeck paras. 84-85.

[104] See *Clapper v. Amnesty Int'l USA*, 133 S. Ct. 1138 (2013).

and acrimonious it may be, is insufficient by itself to meet Art[icle] *III's requirements."*[105]

53. These basic jurisdictional requirements—which apply in all cases—serve an "*overriding and time-honored concern about keeping the Judiciary's power within its constitutional sphere"* and *"prevent the judicial process from being used to usurp the powers of the political branches."*[106]

54. The Draft Decision suggests that these constitutional principles may be "*incompatible with E.U. law"* because they *"operate to limit an individual's capacity to access a remedy"* where that individual claims a violation of the right to privacy. As an initial matter, however, the DPC is incorrect in stating that an individual must show an additional adverse consequence that has occurred as a result of surveillance; as Mr Vladeck notes, courts have held that one may show an "injury" for standing purposes by plausibly alleging that one's information is being collected without his or her consent.[107]

55. Moreover, electronic communications service providers who receive directives under Section 702 may challenge those directives in the FISC, and the FISC may set aside a directive if it finds that it does not comply with the statute or is otherwise unlawful.[108] The same is true with respect to orders to produce business records under Title V, as to which FISA expressly provides a statutory mechanism for challenges.[109] Additionally, parties receiving other types of FISA orders that they believe to be unlawful may apply to the FISC to set the order aside or may decline to comply and contest any government application to compel compliance. The FISC-R case described above was initiated by Yahoo!, and the FISC-R found that Yahoo! *"easily exceed*[ed] *the constitutional threshold for standing"* with respect to its own rights and, under the applicable statutory review mechanism, could also raise Fourth Amendment challenges on behalf of its customers.[110]

---

[105] *Hollingsworth v. Perry*, 133 S. Ct. 2652, 2621 (2013).
[106] *Id.*
[107] Vladeck, para. 90; see *Clapper*, 785 F.3d at 801.
[108] 50 U.S.C. § 1881a(h)(4)(C).
[109] *id.* § 1861(f).
[110] *In re Directives*, 551 F.3d at 1008-09. A version of the opinion that has been further declassified is available at https://www.dni.gov/files/documents/0909/FISC%20Merits%20Opinion%2020080822.pdf.

Companies such as Microsoft have also challenged NSLs, which in at least one case has led the FBI to withdraw a request.[111]

56. In any event, Article 47 of the Charter cannot reasonably be interpreted to require remedies that the U.S. Constitution does not authorise courts to grant, and the U.S. cannot be expected to set aside a "bedrock requirement" that the Supreme Court has applied "[f]*rom its earliest history.*"[112] Indeed, even if the government chooses not to contest a plaintiff's standing, U.S. courts *"have an independent obligation to ensure that they do not exceed the scope of their jurisdiction, and therefore must raise and decide jurisdictional questions that the parties either overlook or elect not to press."*[113]

57. The U.S. legal system does, however, ensure that systemic constraints and enforcement mechanisms exist in addition to the redress measures available to individuals. As Mr Swire's report details, Congress created the FISC based on a recognition that intelligence collection within the U.S. should be subject to independent judicial oversight.[114] The Executive Branch has not hesitated to report compliance problems to the FISC and to implement corrective action where its oversight efforts identify unlawful activities.[115] And the recent enactment of the USA FREEDOM Act shows that Congress—spurred by public concerns—can exercise its powers to reform governmental authorities.

58. The oversight mechanisms described above all serve as remedial measures in a broad sense. The FISC can enforce compliance with its orders and demand follow-up from the government, and declassified opinions of the FISC demonstrate that its oversight has been robust.[116] Thus, even where individuals cannot act as private plaintiffs, the FISC's oversight role protects the privacy interests of people affected by the government's conduct. The provision of the USA FREEDOM Act regarding appointment of *amici*

[111] See Order, *In re National Security Letter*, No. 2:13-cv-01048 (W.D. Wash. May 21, 2014).
[112] *Raines v. Byrd*, 521 U.S. 811, 818 (1997); see also, *e.g.*, *Muskrat v. United States*, 219 U.S. 346, 356 (1911). Contrary to Mr Richards' report (para. 89), however, the Supreme Court did not "tighten" standing doctrine in its recent decision in *Spokeo v. Robbins*, 136 S. Ct. 1540 (2016); the Court merely remanded the case for further consideration of whether the plaintiff had alleged sufficiently "concrete" harms. See *id.* at 1551.
[113] *Henderson ex rel. Henderson v. Shinseki*, 562 U.S. 428, 434 (2011).
[114] Swire, Ch. 3, para. 27.
[115] *Id.* Ch. 5, paras. 62-64.
[116] *Id.* Ch. 5, paras. 66-107.

curiae further strengthens the FISC's oversight capabilities by empowering attorneys to argue for positions that "*advance the protection of individual privacy and civil liberties*."[117]

59. Oversight and enforcement mechanisms available within the Executive Branch can also address specific violations of applicable laws and regulations, including through disciplinary action against employees.[118] Moreover, FISA provides for criminal sanctions for intentional violations of its provisions, which serve as a powerful deterrent against abuses.[119] Individuals can refer alleged unlawful surveillance activities or other alleged violations of FISA to the FBI for review and criminal investigation as appropriate. They can also complain to Inspectors General of the relevant intelligence agencies, which may initiate investigations.[120] Additionally, Congress may act to remedy privacy violations by holding government officials accountable in public as well as in classified hearings—and, ultimately, by enacting legislation that may curtail surveillance authorities.

60. Lastly, the Privacy Shield framework provides, for the first time, a mechanism through which authorities in the E.U. will be able to submit requests on behalf of E.U. individuals regarding the legality of U.S. signals intelligence activities concerning their data. This mechanism will be available to all E.U. individuals whose information is transferred through SCCs and other commercial transfers, in addition to those whose information is transferred under the Privacy Shield framework. The U.S. Department of State has designated a new Ombudsperson, who is independent of intelligence agencies, to receive and process these requests. The Ombudsperson reports directly to the Secretary of State, who will ensure that its functions are carried out objectively and free from improper influence. The Ombudsperson will work closely with other U.S. government officials, including in intelligence agencies and independent oversight bodies such as the PCLOB and Inspectors General, as appropriate, to ensure that requests are resolved in accordance with applicable laws and policies. The U.S. has committed to responding to all completed

[117] 50 U.S.C. § 1803(i).
[118] See DeLong, paras. 33-34, 99-100.
[119] *Id.*, paras. 99-100; see 50 U.S.C. §§ 1809, 1827.
[120] Litt Letter at 7.

requests by confirming that the request has been properly investigated and that relevant U.S. laws have been complied with or that any non-compliance has been remedied.[121]

C. U.S. Provisions Governing Law Enforcement Investigations Meet European Essential Guarantees.

61. Though Mr Schrems' complaint and the Draft Decision focus principally on access to data under national security authorities, this submission also briefly discusses U.S. law enforcement provisions governing data access in ordinary criminal investigations. Many of these laws provide a basic framework upon which U.S. national security law was later built (and, indeed, upon which other countries have based their own laws).

1. Authorities are articulated in clear, accessible rules.

62. Several specific federal statutes and rules of criminal procedure clearly articulate the provisions through which prosecutors and investigators can gather information in a criminal investigation, consistent with the Fourth Amendment.[122] Key provisions include the Wiretap Act[123] and the Electronic Communications Privacy Act ("**ECPA**").[124] Both have existed for decades, are publicly available, and are well understood by prosecutors, judges, and defence lawyers.

63. The Wiretap Act applies where investigators seek to conduct live interceptions of voice or electronic communications. Absent a specific statutory exception (such as consent of a party to the communication), the Act requires investigators to receive authorisation for wiretaps from a federal judge, who must find probable cause to believe that the wiretap or electronic interception will produce evidence of one or more enumerated, serious federal crimes (or evidence about the location of a fugitive). Orders issued under the Act impose

[121] See E.U.-U.S. Privacy Shield Ombudsperson Mechanism Regarding Signals Intelligence, Privacy Shield Annex III, *available at* http://ec.europa.eu/justice/data-protection/files/privacy-shield-adequacy-decision-annex-3_en.pdf.
[122] These authorities are discussed in detail Swire Ch. 4 and in the Letter from Bruce Swartz, Deputy Assistant Attorney General and Counselor for International Affairs, dated 19 February 2016 (Annex VII to the Privacy Shield documents), *available at* http://ec.europa.eu/justice/data-protection/files/privacy-shield-adequacy-decision-annex-7_en.pdf.
[123] 18 U.S.C. §§ 2510-2522.
[124] 18 U.S.C. §§ 2701-2712.

rigorous minimisation requirements and generally require law enforcement to collect only relevant information.[125]

64. Title II of ECPA, also called the Stored Communications Act, sets out rules for government access to subscriber information, traffic data, and the stored content of communications held by internet service providers, telephone companies, and other third-party service providers. In conformance with a federal appeals court ruling, government investigators obtain search warrants from judges in order to collect the contents of any communication or stored data from a commercial communications service provider.[126] To obtain certain types of non-content information (*e.g.*, subscriber information or IP addresses), investigators must issue a subpoena. For most other stored, non-content information, such as email headers without the subject line, investigators must obtain a court order by presenting specific facts to a judge demonstrating that the requested information is relevant and material to an ongoing criminal investigation.[127]

65. Other federal statutes specify the rules governing pen registers and trap-and-trace devices in criminal investigations. Under these provisions, investigators must obtain a court order to acquire certain real-time, non-content data about a phone or an email account upon certification that the information sought is relevant to a pending criminal investigation.[128] Investigators may obtain other types of business records through a grand jury subpoena.[129]

2. These authorities are reasonably tailored to serve legitimate public safety needs.

66. In domestic criminal investigations, where an individual has a reasonable expectation of privacy, the Fourth Amendment generally requires the government to obtain a court-issued warrant before conducting a search.[130] Search warrants must be approved by a "neutral magistrate" without a stake in the investigation,[131] and must be supported by an affidavit

[125] 18 U.S.C. §§ 2510-2522; *see also* Swire, Ch. 4, paras. 12-13.
[126] *United States v. Warshak*, 631 F.3d 266 (6th Cir. 2010).
[127] See Swire, Ch. 4, paras.17-18.
[128] 18 U.S.C. §§ 3121-3127.
[129] See generally Fed. R. Crim. P. 6.
[130] See *Riley v. California*, 134 S. Ct. 2473, 2482 (2014); *Katz v. United States*, 389 U.S. 347, 357 (1967).
[131] See, *e.g.*, *Johnson v. United States*, 333 U.S. 10, 14 (1948).

establishing probable cause that evidence of a particular crime will be present at the place to be searched.[132] Moreover, all warrants must *"limit… the authorization to search to the specific areas and things for which there is probable cause to search."*[133] Subject to certain well-defined exceptions,[134] the requirement to obtain a warrant governs all law enforcement searches in the U.S., including searches for the contents of electronic communications that an individual (regardless of nationality) would reasonably expect to remain private.

67. Where investigators seek real-time interceptions of voice or electronic communications for criminal investigative purposes, they are bound by further restrictions in the Wiretap Act, described above. When authorities seek access to the contents of stored communications, they must generally seek a warrant.[135] This means that authorities must demonstrate probable cause to a judge that a search will reveal evidence of a particular crime, and that searches must be targeted to particular accounts.

68. Generally speaking, U.S. courts have held that when government authorities access non-content information, such as metadata, held by third parties, that activity does not constitute a "search" of the data subject for Fourth Amendment purposes.[136] Nonetheless, federal statutes contain restrictions protecting some types of information in the custody of third parties, including requirements that authorities in certain circumstances must obtain court orders.[137] Where authorities can collect this information by issuing subpoenas, the recipient can challenge the subpoena if it is unreasonably burdensome or overbroad.[138]

3. These authorities are subject to independent oversight.

69. The oversight measures described in Section II.B.3 exist in equivalent measure with respect to law enforcement authorities. Search warrants, wiretap orders, and warrants to

[132] *Illinois v. Gates*, 462 U.S. 213, 232 (1983).
[133] *Maryland v. Garrison*, 480 U.S. 79, 84 (1987). See generally Fed. R. Crim. P. 41.
[134] See, *e.g.*, *Kentucky v. King*, 563 U.S. 452, 460 (2011) (exigent circumstances).
[135] See 18 U.S.C. § 2703(a); *Warshak*, 631 F.3d at 282-88.
[136] See *Smith v. Maryland*, 442 U.S. 735 (1979); *United States v. Miller*, 425 U.S. 534 (1976).
[137] See 18 U.S.C. §§ 2703(d), 3121-27.
[138] Fed. R. Crim. P. 17(c).

collect stored communications must be issued by independent judges or magistrates. These activities are also subject to oversight by Congress (including by the Senate and House Committees on the Judiciary). Law enforcement officials and the federal courts are required to make annual reports to Congress respecting the number of state and federal wiretap applications from the preceding year and related data, such as the duration of any orders and the numbers of arrests or trials resulting from interceptions.[139] Within the Executive Branch, government bodies such as the Justice Department's Office of Enforcement Operations conduct oversight of the use of sensitive investigative tools.

4. Effective remedies exist for unwarranted invasions of privacy.

70. Law enforcement authorities generally must provide notice after executing search warrants.[140] Persons whose conversations are intercepted through wiretap orders must generally receive notice once the surveillance has terminated.[141] Thus, individuals subject to these measures will generally be aware of them and may bring any appropriate legal challenge. In certain circumstances private parties can sue government officials for violations of the Fourth Amendment.[142] Additionally, the Wiretap Act provides a private cause of action for "*any person*" whose communications are intercepted, disclosed, or intentionally used in violation of the law.[143] Moreover, as noted above, evidence collected unlawfully may be subject to the exclusionary rule.

71. The Judicial Redress Act, signed into law in February 2016, will provide individuals in designated countries with the right to seek judicial redress in a U.S. court if personal data is shared with U.S. authorities by their home countries (or by private entities within their home countries) for law enforcement purposes and is wrongfully disclosed by U.S. authorities.[144] The E.U. countries covered by the U.S.-E.U. Data Privacy and Protection

[139] 18 U.S.C. § 2519.
[140] Fed. R. Crim. P. 41(f)(1)(C).
[141] See 18 U.S.C. § 2518(8)(d).
[142] See *Bivens v. Six Unknown Named Agents of the Federal Bureau of Narcotics*, 403 U.S. 388 (1971); 42 U.S.C. § 1983.
[143] 18 U.S.C. § 2520. The Stored Communications Act also contains a civil liability provision. See 18 U.S.C. § 2707.
[144] Pub. L. No. 114-126 (2016).

Agreement are expected to be designated in the near future. E.U. individuals will also have rights concerning access to and correction of such data in an equivalent manner as U.S. persons, subject to the same exemptions and exceptions.

72. Other systemic checks and balances apply in the law enforcement context. Because courts generally must authorise orders permitting searches, wiretaps, or access to stored communications, they are empowered to enforce compliance with those orders. Congress exercises oversight regarding the use of these authorities. In certain contexts, such as the Stored Communications Act, communications providers may also act as an additional check against law enforcement officials by applying to quash warrants if the provider considers that the warrant exceeds the bounds of the law.[145]

III. U.S. Privacy Protections Compare Favourably to Those Afforded in E.U. Member States.

73. To determine whether privacy protections afforded in the U.S. are "essentially equivalent" to those afforded under E.U. law (again, assuming *arguendo* that such a determination is necessary), it is important to view U.S. laws and practices alongside the laws and practices within the E.U. and its Member States. These practices illuminate the manner in which the basic rights enumerated in the Charter are applied.[146] Furthermore, Member States' practices are a significant factor in determining whether personal data transferred to the U.S. is actually protected to a similar degree as it would be in the E.U.[147] Directive 95/46/EC requires assessing "*the adequacy of the level of protection afforded by a third country . . . in light of all the circumstances surrounding"* the transfer of data.[148] Clearly, the privacy protections actually afforded by E.U. Member States are significant circumstances when assessing whether a transfer of E.U. citizens' data to the U.S. jeopardises the privacy of the data. Otherwise the analysis of any privacy concerns raised

[145] See, *e.g.*, *Matter of Warrant to Search a Certain E-mail Account Controlled and Maintained by Microsoft Corp.*, 829 F.3d 197 (2d Cir. 2016) (granting Microsoft's motion to quash a warrant issued under the Stored Communications Act where information sought was stored overseas).
[146] *Cf.* Article 52(4) of the Charter.
[147] See Report of Mr Geoffrey Robertson QC ("**Robertson**"), paras. 12, 19-21.
[148] Directive 95/46, Recital 56 and Art. 25(2).

by the transfer of data to the U.S. would be artificial. Moreover, it would be anomalous to apply higher standards for data transferred outside the E.U. than to data transferred within the E.U. or that remains within an E.U. Member State.

74. Conducting a relative comparison between the U.S. and E.U. Member States is also consistent with the E.U.'s and Member States' international trade obligations toward the U.S., particularly with respect to non-discrimination obligations under the World Trade Organization ("**WTO**") General Agreement on Trade in Services ("**GATS**"). The E.U. and Member States have committed under the GATS to provide no less favourable treatment to certain U.S. companies in many service sectors as compared to Member State companies, including with respect to such U.S. companies that rely on data transmissions from the E.U. to supply their services. If a ruling invalidated SCCs for data transfers to the U.S., these U.S. companies would be prevented from receiving personal data from E.U. customers. Where U.S. law provides the same or greater privacy protections as E.U. Member States, this would put the E.U. and E.U. Member States at considerable risk of providing less favourable treatment to these U.S. companies than their competitors in E.U. Member States, contrary to the E.U.'s and Member States' GATS obligations. In addition, this would put the E.U. and Member States at considerable risk of providing U.S. companies less favourable treatment than their competitors in other non-E.U. countries continuing to benefit from SCCs, contrary to separate GATS obligations of the E.U. and Member States to provide no less favourable treatment to U.S. service suppliers as compared to such companies in other non-EU states.[149] While the GATS provides an exception for measures necessary to comply with laws such as those respecting data privacy, it only permits such measures if they do not constitute "*a means of arbitrary or unjustifiable discrimination between countries where like conditions prevail, or a disguised restriction on trade in services.*"[150] Where the U.S. provides data protections that are in

[149] For example, the European Commission in 2011 found that Israel ensures adequate data protections based on an analysis only of Israel's privacy laws. Commission Decision 2011/61, 2011 J.O. (L 27) 39-42. Observers have noted the Israeli government's access to data for national security purposes (which the Commission did not consider) lacks safeguards available in the United States. See Ravia and Hammer, *Israel*, in The Privacy, Data Protection, And Cybersecurity L. Rev. (2nd ed., A.C. Raul ed.) 190, 198 (2015). Major E.U. trading partners likewise may have lesser safeguards regarding government access to data than the U.S. See Swire Ch. 1, paras. 90-98.

[150] GATS Article XIV, available at https://www.wto.org/english/docs_e/legal_e/26-gats.pdf. .

fact equivalent to or greater than those in E.U. Member States, restricting the flow of data from the E.U. to the U.S. may constitute arbitrary or unjustified discrimination.

75. The CJEU has held that E.U. law must, as far as possible, be interpreted consistently with WTO law,[151] and that generally E.U. international agreements must have primacy over E.U. secondary legislation, such that secondary legislation (including Directives) must be interpreted consistently with these international agreements wherever feasible.[152] Accordingly, Directive 95/46/EC should be interpreted to require that authorities consider the protections actually afforded in E.U. Member States when considering the validity of the safeguards afforded by SCCs under Article 26 (or, for that matter, when considering the "adequacy" of a third country's protections under Article 25).

76. Member States employ a broad range of practices in balancing the right to privacy against the protection of national security and other state interests. With respect to national security surveillance, many Member States afford substantial discretion to government authorities to conduct interceptions. Member States' oversight and redress mechanisms in national security cases, where available, take account of the nature of the activities at issue, providing reasonable accommodations for the protection of sensitive information. The U.S. legal regime compares favourably in each of the key benchmarks: (1) existence of clear and accessible laws; (2) necessity and proportionality; (3) oversight; and (4) redress.[153]

A. Existence of Clear and Accessible Laws

77. Member States generally permit governmental authorities to engage in electronic surveillance for national security purposes. As the European Union Agency for

[151] See, *e.g.*, Judgment of 16 June 1998, *Hermès International*, Case C-53/96, ECLI:EU:C:1998:292, para. 28; Judgment of 14 December 2000, *Dior*, Joined Cases C-300 and 392/98, ECLI:EU:C:2000:688, para.47; Judgment of 16 November 2004, *Anheuser-Busch*, Case C-245/02, ECLI:EU:C:2004:717, para. 55.
[152] See, *e.g.*, Judgment of 1 April 2004, *Bellio F.lli*, Case C-286/02, ECLI:EU:C:2004:212, para. 33; Judgment of 10 January 2006, *R. (IATA and European Low Fares Airline Association) v Department for Transport*, Case C-344/04, ECLI:EU:C:2006:10, para. 35.
[153] While this comparison focuses on access to data for national security purposes, a similar comparison between U.S. and E.U. Member State laws could be drawn with respect to access to law enforcement provisions.

Fundamental Rights has observed in its recent report ("**FRA Report**"), however, State intelligence communities are "*greatly diverse*" in their organisational structures and have evolved due to unique "*historical developments, wars, and threats.*"[154] Indeed, "*the enactment of laws*" to govern states' intelligence activities is "*a relatively recent process.*"[155]

78. Under these laws, electronic surveillance may be conducted for a broad range of purposes. In Ireland, for example, interception of telecommunications or postal mail may be authorised where there are "*reasonable grounds for believing that particular activities*" are "*endangering or* [are] *likely to endanger the security of the State,*" as well as for criminal investigative purposes.[156] In the United Kingdom, warrants for interception may be issued "*in the interests of national security*"; "*for the purpose of preventing or detecting serious crime*"; and for purposes "*of safeguarding the economic well-being of the United Kingdom*" where those interests are also relevant to the interests of national security.[157] In France, state security interests for purposes of surveillance may include "*national independence, territorial integrity, and national defense,*" "*major interests of foreign policy,*" and "*major economic, industrial and scientific interests of France.*"[158] German law permits the use of "*strategic intelligence*" surveillance to intercept communications to and from Germany or other countries to prevent, among other things, armed attacks against Germany, terrorism, arms proliferation, drug trafficking, human trafficking, or money laundering in cases of "*substantial importance.*"[159] These varying standards are effectively equivalent to, and in some cases more permissive than, the defined law enforcement and "*foreign intelligence*" purposes described in U.S. law.

---

[154] FRA, *Surveillance by Intelligence Services: Fundamental Rights and Remedies in the E.U.* ("**FRA Report**"), at 13 (2015). The FRA Report is exhibited to Mr Robertson's affidavit and is also available online at http://fra.europa.eu/sites/default/files/fra_uploads/fra-2016-surveillance-intelligence-services_en.pdf.

[155] *Id.* at 14.

[156] Interception of Postal Packets and Telecommunications Messages (Regulation) Act 1993 ("**1993 Act**") sections 4(a)(i), 5(a). Ireland's Criminal Justice (Surveillance) Act 2009 governs other types of surveillance activities, including covert installation of recording equipment.

[157] Regulation of Investigatory Powers Act 2000 ("**RIPA**") section 5(3); see also Investigatory Powers Act 2016 ("**IPA**") section 20(2)(c). The IPA has been signed into law and is expected to take effect at the end of 2016, at which point it will largely replace RIPA.

[158] France, Internal Security Code Art. L 811-3.

[159] Germany, Act on Restricting the Privacy of Correspondence, Posts, and Telecommunications § 5 ("**G-10 Act**"), discussed in the FRA Report at 26.

B. Necessity and proportionality

79. Under European law, necessity and proportionality considerations are based on factors such as the scale of authorised surveillance; applicable standards for suspicion; whether surveillance measures require prior authorisation and from whom; and whether surveillance measures restrict further use or transmission of data.[160] Across each of these areas, U.S. law compares favourably to those of E.U. Member States.

80. First, several Member States permit large-scale interceptions of communications within their territories that are not targeted at individuals.[161] In Germany, the Federal Intelligence Service (BND) is authorised to conduct interceptions *"in bundled form"* for certain authorised purposes.[162] The FRA Report notes that selectors used for such interceptions may include not only telephone numbers and e-mail addresses but also search terms such as "holy war"—*i.e.*, the types of "key word" searches not permitted under Section 702 of FISA.[163] Dutch authorities are permitted to conduct "non-specific" surveillance on "non-cable-bound" telecommunications, such as satellite communications.[164] In France, the 2015 Intelligence Law allows government authorities to order communications providers to conduct automatic large-scale processing of data based on certain algorithms designed to detect terrorist threats.[165] In the U.K., the newly enacted Investigatory Powers Act 2016 permits the issuance of *"bulk interception warrants"* in certain circumstances where communications are either sent from or received by individuals who are outside *"the British Islands."*[166] In the U.S., by contrast, the government may not compel any type of collection from private parties absent the use of specific selectors.

---

[160] *Schrems I*, para. 91; *Szabo and Vissy*, para 56.
[161] E.U. Member States may also conduct intelligence collection that is wholly outside their borders, and much of this activity is largely unregulated. See, *e.g.*, FRA Report at 21; Germany, Act on the Foreign Intelligence Service ("**BND Act**") § 1(2) (permitting authorities, without further restriction, to "*collect and analyze information required for obtaining foreign intelligence, which is of importance for the foreign and security policy of . . . Germany*").
[162] Germany, G-10 Act, § 5; see FRA Report at 22.
[163] FRA Report at 22.
[164] *Id.*; Netherlands, Intelligence and Security Services Act 2002, Art. 27.
[165] See FRA Report at 23-24; France, Internal Security Code Art. L851-3.
[166] IPA sections 136, 138.

81. Second, when conducting targeted surveillance, Member States employ a range of required levels of suspicion. Some Member States do not articulate any particular standard of suspicion, nor do they all specifically require authorities to assess that there is no alternative to the proposed surveillance measure. Ireland requires a *"reasonable prospect"* that an interception would be of *"material assistance"* in investigating or preventing a crime or addressing a threat to national security.[167] The Netherlands authorises interceptions where there is *"serious suspicion"* that the actions of an individual or organisation pose a risk to the democratic rule of law, national security, or other important interests of the state.[168] French law governing surveillance activities does not specify any particular level of suspicion, but instead requires that surveillance be conducted within the general principles of proportionality.[169]

82. Third, most Member States do not require prior authorisation by a judge or other independent authority to conduct surveillance activities for national security purposes.[170] For example, Ireland[171] and the Netherlands[172] permit executive or intelligence authorities to authorise surveillance measures without prior judicial approval. As the FRA's Report notes, only three Member States actually require *ex ante* approval from an independent body.[173]

83. Fourth, E.U. Member States do not have uniform rules in the national security context about the use or retention of data and its transmission to other parties. Notably, Directive 95/46/EC does not govern retention or transmission of data in national security and several other contexts, because the Directive *"does not apply to the processing of personal data in the course of an activity which falls outside the scope of Community law,"* including

[167] 1993 Act, sections 4 and 5. For covert installation of recording devices, Irish law requires *"reasonable grounds"* for believing that the surveillance is *"necessary"* to investigate or prevent a crime or to *"maintain…the security of the State."* Criminal Justice (Surveillance) Act 2009, section 4(1).
[168] Netherlands, Intelligence and Security Services Act 2002, Art. 6(2)(a).
[169] France, Internal Security Code Arts. L801-1, L851-3.
[170] See Robertson para. 43.
[171] See 1993 Act, sections 1 and 2 and Criminal Justice (Mutual Assistance) Act 2008, section 25. Ireland does, however, require prior judicial authorisation (except in certain emergency circumstances) for covert installation of surveillance devices. *See* Criminal Justice (Surveillance) Act 2009, sections 4 and 7.
[172] See Netherlands, Intelligence and Security Services Act 2002, Art. 25.
[173] FRA Report at 53 (describing procedures for Germany, Austria, and Belgium). The U.K. may potentially be added to this list following the enactment of the IPA.

"processing operations concerning public security, defence, State security . . . and the activities of the State in areas of criminal law."[174] The FRA Report notes that Data Protection Authorities *"in most Member States have no competences over national intelligence services, or their powers are limited."*[175] Importantly, the data protection laws of most Member States contain specific carve-outs where data is processed for national security (or, in some cases, law enforcement) purposes.[176]

C. Oversight Mechanisms

84. Member States also employ a range of oversight mechanisms.[177] Some Member States rely largely on internal controls within executive channels for routine oversight, rather than on independent courts.[178] Others have hybrid oversight bodies whose members consist of legislators, are appointed by a legislative body, and/or are appointed by the prime minister.[179] They may also have specialised parliamentary panels that conduct oversight activities.[180] However, routine oversight by an independent judiciary, as in the U.S., appears to be the exception rather than the rule; and many oversight bodies lack independent authority to order remedies if they find violations of the law.[181]

D. Redress

85. Article 47 provides for a right to an *"effective remedy"* where there is interference with an individual's right to privacy. But as the ECtHR has recognised, a categorical requirement to provide individual notification in all cases (thus enabling such individuals to pursue

---

[174] Directive 95/46/EC, Art. 3(2).
[175] FRA Report at 47. The Report notes that DPAs *"have no power over intelligence services in 12 Member States"*; in Ireland and in eight other Member States, DPAs *"have limited power over intelligence services." Id.*; see also Robertson, para. 46.
[176] See, *e.g.*, Germany, BND Act § 11 ("[f]or the performance of the functions of the [BND]," various provisions of Germany's Federal Data Protection Act "shall not apply"); Denmark, Act on Processing of Personal Data, Title I, Ch. 1, §2, para. 11, *available at* https://www.datatilsynet.dk/english/the-act-on-processing-of-personal-data/read-the-act-on-processing-of-personal-data/compiled-version-of-the-act-on-processing-of-personal-data/.
[177] See Robertson, paras. 44-47; FRA Report at 57.
[178] FRA Report at 32-34; Robertson, para. 43.
[179] FRA Report at 41-46.
[180] *Id.* at 34.
[181] See, *e.g.*, FRA Report at 31 (France's oversight body, if it discovers a violation of the law, may inform the prime minister and bring a case before the Council of State).

private causes of action) would jeopardise the very purpose of any surveillance measure.[182] The FRA Report notes that notice obligations can be restricted under the legal frameworks of all E.U. Member States for national security reasons.[183]

86. In the intelligence context, eight Member States provide for no right of notification whatsoever, while the remaining 20 provide for notification subject to restrictions, including national security interests.[184] As noted above, Directive 95/46/EC and most Member States' data protection laws contain a national security exemption, so these data protection provisions may not by their terms offer a means for notification and redress where national security information is involved. In other instances, Member States' underlying intelligence laws may provide notification requirements, but subject to restrictions. Germany provides that a subject should be informed after a surveillance measure has been discontinued, but that notice *"shall be withheld as long as it cannot be ruled out that informing the data subject might jeopardize the purpose of the* [measure] *or as long as any general disadvantages to the interests of* [Germany] *are foreseeable."*[185] The Netherlands provides that, five years after a measure has been carried out, authorities should assess whether notice can be provided; but notification is not required if it can reasonably be expected to compromise sources or methods.[186] Disclosure of the existence of authorisations may also be lawfully restricted in Ireland.[187]

87. If an individual does not receive notification of surveillance and cannot show that he or she has been subject to surveillance measures, then Member States' own "standing" requirements may restrict the ability to bring a claim.[188] A threshold requirement of a particular interest in the outcome of a claim, and a requirement that harm be proved before damages can be awarded in respect of most torts, are common features in many E.U.

[182] See *Klass*, para. 58; *Zakharov*, para. 287.
[183] FRA Report at 62; see also Robertson, para. 50.
[184] FRA Report at 75.
[185] G-10 Act § 12(1).
[186] Netherlands, Intelligence and Security Services Act 2002 Art. 34. See also FRA Report at 63 (describing other examples).
[187] 1993 Act, section 12 (also applied to requests under the Criminal Justice (Mutual Assistance) Act 2008 by section 29 of that Act).
[188] See Robertson, para. 51; FRA Report at 67.

Member States, including Ireland.[189] A German court has held inadmissible, for example, a complaint against strategic surveillance because it lacked evidence that the claimant had been affected.[190] As Mr Robertson notes, there may in fact be no instances in which a person in the E.U. has been notified of unlawful surveillance undertaken for national security purposes and has then been able to successfully challenge and obtain compensation for that violation.[191]

88. The ECtHR has held that, because individuals may by necessity be restricted from learning of surveillance measures, other meaningful safeguards against abuses must be in place.[192] But while Member States have created various other redress mechanisms, there is little uniformity concerning the remedies that these mechanisms provide.[193] Because data protection statutes in most Member States contain carve-outs for national security matters, the remedies provided through those laws are also circumscribed. In many instances, claimants often must rely on a government agency's certification that their data is being handled in line with Charter rights.[194]

89. In some instances, individuals who believe they have been subject to unlawful surveillance may lodge complaints through DPAs or other bodies. While the complainant may not be party to the proceedings—or may be barred from accessing sensitive information—the investigatory authority can examine a complaint on that person's behalf. For example, the FRA Report notes that the DPAs and other oversight bodies in Austria, Belgium, France, Italy, and Luxembourg may verify the legality of surveillance measures on behalf of a complaining individual, but they may not confirm or deny the existence of any such measures to the complainant if doing so would threaten national security.[195] Other

[189] As regards *locus standi*, see e.g. *State (Lynch) v Cooney* [1982] IR 337, 369; *Lancefort Limited v An Bord Pleanála (No.2)* [1999] 2 IR 270. As regards proof of harm in the context of a data privacy claim see *Collins v FBD Insurance plc* [2013] IEHC 137.
[190] FRA Report at 67.
[191] Robertson, paras. 4, 113.
[192] *Klass*, para. 55.
[193] See FRA Report at 59 (noting that "*the powers of remedial bodies* [are] *curtailed when safeguarding national security is involved"*).
[194] For example, in France the Commission Nationale de l'Informatique et des Libertés (CNIL) accesses national and public security files on behalf of citizens to enforce their rights indirectly. Commission Nationale de L'Informatique et des Libertés, Rights And Obligations, https://www.cnil.fr/en/rights-and-obligations .
[195] FRA Report at 64-65.

Member States have created specialised tribunals to hear complaints and investigate claims about unlawful surveillance. Ireland is one such example: a "Complaints Referee" is appointed by the Taoiseach and empowered to investigate complaints and, if a violation has been found, to provide certain remedies.[196]

E. Summary

90. In summary, E.U. Member States employ a wide range of legal regimes governing national security surveillance, and they ensure that privacy rights are protected through a variety of safeguards unique to their authorities and infrastructures. Not all Member States provide clear, accessible rules; many authorise surveillance measures for broad purposes and/or without use of individual discriminants; and most do not require independent authorisations from judges. Oversight and redress mechanisms also vary and range from internal executive controls to measures afforded by legislative authorities or by hybrid bodies. By comparison, the privacy safeguards afforded by U.S. law are equivalent to, if not in many respects greater than, the safeguards afforded in practice throughout the E.U. Critically, the variety of manners by which E.U. Member States protect their citizens' privacy through regulation of national security surveillance highlights that the E.U.'s "Essential Guarantees" cannot be imposed in a rigid or uniform manner.

IV. Questions of Equivalence Should Be Guided by Due Consideration of the European Commission's Adequacy Finding and of International Comity.

91. To the extent there is any remaining doubt about whether the protections afforded by the U.S. concerning government access to personal data are essentially equivalent to those afforded in the E.U., this Court should also afford due weight to the findings of the European Commission with respect to the E.U.-U.S. Privacy Shield and to principles of international comity.

[196] 1993 Act, section 9.

92. First, while the transfer of data to which this case relates was not conducted under the Privacy Shield, it is important to note that, in assessing that framework, the European Commission conducted a careful analysis, including through intensive engagement with U.S. authorities between 2014 and 2016, of the U.S. legal regime governing access to data. The U.S. provided extensive written material concerning U.S. law, including FISA, PPD-28, and associated redress mechanisms. No other country has publicly explained in detail and justified to foreign officials its core national security provisions in this way. The Commission, after considering this wealth of information, concluded that the U.S. legal system affords strong privacy protections against indiscriminate access to data by governmental authorities.[197]

93. In *Schrems I*, the CJEU held that data protection authorities must be fully empowered to conduct investigations and to ensure that data transfers to third countries comply with the requirements of Directive 95/46/EC. But in conducting such investigations, authorities must also *"ensure a fair balance between, on the one hand, observance of the fundamental right to privacy and, on the other hand, the interests requiring free movement of personal data."*[198] Further, under Directive 95/46/EC, third countries *"cannot be required to ensure a level of protection identical to that guaranteed in the E.U. legal order."*[199] The means through which a third country protects the right to privacy *"may differ from those employed within the European Union."*[200]

94. In analogous legal contexts where nations must cooperate in service of common purposes, such as those involving extradition and mutual legal assistance, American and European courts have acknowledged that different legal systems can protect basic rights through different means. Rather than compare systems by reference to each individual provision in a country's laws, courts have asked whether the system as a whole functions to provide adequate safeguards.[201] At the least, the "margin of appreciation" principles applied by the

[197] See EC Adequacy Decision, paras. 64-141.
[198] *Schrems I*, para. 42.
[199] *Id.* para. 73.
[200] *Id.* para. 74.
[201] In proceedings concerning extradition, U.S. courts have held that "[i]*t is not the business of our courts to assume the responsibility for supervising the integrity of the judicial system of another sovereign nation. Such an assumption would directly conflict with the principle of comity upon which extradition is based." Jhirad v.*

ECtHR regarding state measures to protect national security should apply here, especially where a decision to enjoin data transfers could have sweeping commercial ramifications for transatlantic data flows and risk undermining international cooperation to confront common threats.[202]

95. In summary, while respect for privacy and the protection of personal data undoubtedly calls for appropriate scrutiny by Data Protection Authorities and by courts, this Court should afford due regard to the significantly enhanced privacy protections put in place by the U.S. government in recent years; the thorough review of the U.S. legal system conducted by the European Commission; and the important economic interests served by the free flow of data between the United States and E.U. Member States.

Word count: [15,036]

SUZANNE KINGSTON
EILEEN BARRINGTON SC

23 December 2016

Ferrandia, 536 F.2d 478, 484-85 (2d Cir. 1976). The ECtHR has likewise held that, although extradition may be barred in certain circumstances implicating fundamental human rights, the Convention *"cannot be read as justifying a general principle to the effect that . . . a Contracting State may not surrender an individual unless satisfied that the conditions awaiting him in the country of destination are in full accord with each of the safeguards of the Convention." Soering v. United Kingdom*, para. 186, No. 14038/88 (ECtHR 1989).

[202] See Swire Ch. 1, para. 107-120; Affidavit of Joshua P. Meltzer. This is precisely the approach taken by the ECtHR to the E.U. legal order pursuant to the *Bosphorus* doctrine mentioned above, see *supra* note 7.