

Legal Studies Research Paper Series



UNIVERSITY OF
CAMBRIDGE

Faculty of Law

PAPER NO. 14/2016

MARCH 2016

Reality and Illusion in EU Data Transfer Regulation Post Schrems

Christopher Kuner

Further information about the University of Cambridge Faculty of Law Legal Studies

Research Paper Series can be found at <http://www.law.cam.ac.uk/ssrn/>

Reality and illusion in EU data transfer regulation post *Schrems*

Christopher Kuner*

Version 1.0/March 2016

Abstract: In *Schrems v. Data Protection Commissioner*, the Court of Justice of the European Union invalidated the EU-US Safe Harbour arrangement allowing personal data to be transferred to the US. The judgment affirms the fundamental right to data protection, defines an adequate level of data protection for international data transfers under EU law, and extends data protection rights to third countries, all based on the EU Charter of Fundamental Rights. The judgment is a landmark in the Court's data protection case law, and illustrates the tension between the high level of legal protection for data transfers in EU law and the illusion of protection in practice. The judgment has undermined the logical consistency of the other legal bases for data transfer besides the Safe Harbour, and reactions to it have largely been based on formalism or data localization measures that are unlikely to provide real protection. *Schrems* also illustrates how many legal disagreements concerning data transfers are essentially political arguments in disguise. The EU and the US have since agreed on a replacement for the Safe Harbour (the EU-US Privacy Shield), the validity of which will likely be tested in the Court. It is crucial for data transfer regulation to go beyond formalistic measures and legal fictions, in order to move regulation of data transfers in EU law from illusion to reality.

“Dearer to us than a host of truths is an exalting illusion.”¹

I. Introduction

In a world that has been transformed by the Internet, the ability to transfer personal data across national borders, and to access information regardless of geography, has become crucial for social interaction, economic growth, and technological advancement. At the same time, concerns about the misuse of personal data have put increased emphasis on the protection of international transfers of personal data. The most important body of data transfer regulation is that contained in Articles 25 and 26 of the EU Data Protection Directive² (the “Directive”), which restricts the transfer of personal data outside the EU unless an “adequate level of data protection” is provided based on EU legal standards.

* Professor of Law and Co-Chair of the Brussels Privacy Hub, Vrije Universiteit Brussel (VUB), Brussels; Affiliated Lecturer, Faculty of Law, University of Cambridge; Visiting Professor, Department of Law, London School of Economics and Political Science; Senior Privacy Counsel, Wilson Sonsini Goodrich & Rosati, Brussels.

¹ Anton Chekhov, *Gooseberries*, in: *Selected Stories of Anton Chekhov*, locations 5793-5794 (Kindle edition), Random House (2009), paraphrasing Alexander Pushkin.

² Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, [1995] OJ L281/31.

On 6 October 2015, the Court of Justice of the European Union (CJEU) issued its most significant judgment to date dealing with EU data transfer regulation. In *Maximilian Schrems v. Data Protection Commissioner*,³ the CJEU invalidated the decision⁴ of the European Commission finding that the EU-US Safe Harbour agreement provided “adequate protection” for data transfers under Article 25 of the Directive. The *Schrems* judgment and the opinion of the Advocate General⁵ that preceded it provoked an intense public reaction, including front-page articles in major international newspapers;⁶ a press conference by top officials of the European Commission;⁷ reactions from US government officials;⁸ a paper released by the Article 29 Working Party (the group of data protection authorities from the EU and its Member States);⁹ concerned statements from US business organizations;¹⁰ reactions from civil society groups;¹¹ opinions of academic experts;¹² legal memoranda from business groups;¹³ and a newspaper interview by the President of the CJEU.¹⁴

³ Case C-362/14, 6 October 2015, ECLI:EU:C:2015:650.

⁴ European Commission Decision 2000/520 of 26 July 2000 pursuant to Directive 95/46 of the European Parliament and of the Council on the adequacy of the protection provided by the Safe Harbour privacy principles and related frequently asked questions issued by the US Department of Commerce, [2000] OJ L215/7. The alternative US spelling “Safe Harbor” will be used when it appears as such in original sources.

⁵ Opinion of Advocate General Bot, Case 362/14, *Maximilian Schrems v. Data Protection Commissioner*, 23 September 2015, ECLI:EU:C:2015:650.

⁶ See, e.g., Duncan Robinson, Richard Waters, and Murad Ahmed, “US tech companies overhaul operations after EU data ruling”, *Financial Times*, October 6 2015, <<http://www.ft.com/intl/cms/s/0/5d75e65a-6bf8-11e5-aca9-d87542bf8673.html#axzz3vvmkIE7x>>; Mark Scott, “Data Transfer Pact between U.S. and Europe is Ruled Invalid”, *New York Times*, 6 October 2015, <http://www.nytimes.com/2015/10/07/technology/european-union-us-data-collection.html?_r=0>.

⁷ European Commission, “First Vice-President Timmermans and Commissioner Jourová’s press conference on Safe Harbour following the Court ruling in case C-362/14 (*Schrems*)”, 6 October 2015, <http://europa.eu/rapid/press-release_STATEMENT-15-5782_en.htm>.

⁸ See speech by US FTC Commissioner Julie Brill, “Transatlantic Privacy after *Schrems*: Time for an Honest Conversation”, 23 October 2015, <https://www.ftc.gov/system/files/documents/public_statements/836443/151023amsterdamprivacy1.pdf>; United States Mission to the EU, “Safe Harbor Protects Privacy and Provides Trust in Data Flows that Underpin Transatlantic Trade”, 28 September 2015, <<http://useu.usmission.gov/st-09282015.html>>.

⁹ Article 29 Working Party, “The Court of Justice of the European Union invalidates the EU Commission Safe Harbour Decision”, 6 October 2015, <http://ec.europa.eu/justice/data-protection/article-29/press-material/press-release/art29_press_material/2015/20151006_wp29_press_release_on_safe_harbor.pdf>.

¹⁰ See, e.g., AmCham EU, “EU Court of Justice’s decision in the *Schrems* case could disrupt transatlantic business, hurt the EU economy and jeopardise a Digital Single Market”, 6 October 2015, <http://www.amchameu.eu/sites/default/files/press_releases/press_-_ecj_decision_on_schrems_will_disrupt_transatlantic_business.pdf>.

¹¹ EDRI, “EU and US NGOs propose privacy reforms post *Schrems*”, 18 November 2015, <<https://edri.org/eu-and-us-ngos-propose-privacy-reforms-post-schrems/>>.

¹² Peter Swire, “US Surveillance Law, Safe Harbor, and Reforms since 2013”, 18 December 2015, <<http://peterswire.net/wp-content/uploads/Schrems-White-Paper-12-18-2015.pdf>>.

¹³ Sidley Austin LLP, “Essentially equivalent: A comparison of the legal orders for privacy and data protection in the European Union and United States”, January 2016, <<http://www.sidley.com/~media/publications/essentially-equivalent---final.pdf>>. This was prepared by the law firm Sidley Austin LLP on behalf of a number of US associations in the technology industry.

¹⁴ See the interview with CJEU President Koen Lenaerts in Valentina Popp, “ECJ President on EU Integration, Public Opinion, Safe Harbor, Antitrust”, *The Wall Street Journal*, 14 October 2015, <<http://blogs.wsj.com/brussels/2015/10/14/ecj-president-on-eu-integration-public-opinion-safe-harbor-antitrust/tab/print/>>.

In February 2016 agreement between the EU and the US was announced on a replacement for the Safe Harbour, called the “Privacy Shield”,¹⁵ regarding which details and supporting documentation were released on 29 February.¹⁶ Further mechanisms to protect data transfers between the EU and the US are currently in the works, such as an agreement concerning data exchanges between law enforcement authorities,¹⁷ and changes to US law to grant additional data protection rights to EU individuals.¹⁸

The *Schrems* judgment is a landmark case that strengthens the fundamental right to data protection in EU law. The Court affirmed data protection rights with regard to data transfers; supported the right of data protection authorities (DPAs) to investigate the adequacy of protection transferred to third countries; and clarified what constitutes an adequate level of data protection under EU law. It is the first time the CJEU has analysed regulation of international data transfers in light of key constitutional provisions of EU law such as the Treaty on the Functioning of the EU (TFEU)¹⁹ and the EU Charter of Fundamental Rights (the Charter).²⁰

Viewed at a high level or “meta level”, the *Schrems* judgment shows how the regulation of international data transfers in EU law is caught between reality and illusion. The main strand of the Chekhov story quoted at the beginning of this article involves a character who lives in the illusion that the fruit produced by his gooseberry bushes are sweet, while in fact they are

¹⁵ European Commission, “EU Commission and United States agree on a new framework for transatlantic data flows: EU-US Privacy Shield”, 2 February 2016, <http://europa.eu/rapid/press-release_IP-16-216_en.htm>; US Department of Commerce, “EU-U.S. Privacy Shield”, 2 February 2016, <<https://www.commerce.gov/news/fact-sheets/2016/02/eu-us-privacy-shield>>.

¹⁶ European Commission, “Restoring trust in transatlantic data flows through strong safeguards: European Commission presents EU-U.S. Privacy Shield”, 29 February 2016, <http://europa.eu/rapid/press-release_IP-16-433_en.htm>, with links to the following documents that together comprise the Privacy Shield: Communication from the Commission to the European Parliament and the Council: Transatlantic Data Flows: Restoring Trust through strong Safeguards, COM(2016) 117 final, 29 February 2016; EU-US Privacy Shield: Frequently Asked Questions, 29 February 2016; Commission Implementing Decision of XXX pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of protection provided by the E.U.-U.S. Privacy Shield; Annex I, Letters from US Department of Commerce Secretary Penny Pritzker and US Under-Secretary for International Trade Stefan M. Selig, 23 February 2016; Annex II, EU-U.S. Privacy Shield Framework Principles Issued by the U.S. Department of Commerce; Annex III, Letter from US Secretary of State John Kerry, 22 February 2016; Annex IV, Letter from FTC Chairwoman Edith Ramirez, 23 February 2016; Annex V, Letter from US Secretary of Transportation Anthony R. Foxx, 19 February 2016; Annex VI, Letter from US General Counsel for the Office of the Director of National Intelligence Robert S. Litt, 22 February 2016; Annex VII, Letter from US Deputy Assistant Attorney General and Counselor for International Affairs for the Criminal Division Bruce C. Swartz, 19 February 2016.

¹⁷ Agreement between the United States of America and the European Union on the Protection of Personal Information relating to the Prevention, Investigation, Detection and Prosecution of Criminal Offenses (draft for initialling), 8 September 2015, <http://ec.europa.eu/justice/data-protection/files/dp-umbrella-agreement_en.pdf>. See also European Data Protection Supervisor, “Preliminary Opinion on the Agreement between the United States of America and the European Union on the protection of personal information relating to the prevention, investigation, detection and prosecution of criminal offenses”, 12 February 2016, <https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2016/16-02-12_EU-US_Umbrella_Agreement_EN.pdf>.

¹⁸ H.R. 1428 – Judicial Redress Act of 2015, 114th Congress (2015-2016), signed by President Obama on 24 February 2016, <<https://www.congress.gov/bill/114th-congress/house-bill/1428/all-actions?overview=closed>>.

¹⁹ Consolidated Version of the Treaty on the Functioning of the European Union (TFEU), Article 16, [2012] O.J. C 326/47.

²⁰ Charter of Fundamental Rights of the European Union, Article 8, [2010] O.J. C/83 389, 393

unripe and sour. EU data protection law similarly maintains the illusion that it can provide seamless, effective protection of EU personal data transferred around the world, a view that the *Schrems* judgment affirms. This is a beautiful illusion, at least to European eyes, since it envisions a world where the reach of EU data protection law extends globally; where attempts by foreign intelligence agencies to access the data of Europeans are repelled through the use of procedural mechanisms such as contractual clauses; and where DPAs police the Internet and quash attempts to misuse European data.

However, it remains an illusion, as can be seen by the measures that have been advocated in reaction to the *Schrems* judgment. Procedural mechanisms may satisfy formal requirements of data protection law, but cannot provide protection against the intelligence surveillance that the *Schrems* case involved. Data localization attempts to minimize or avoid the transfer of personal data to third countries, but cannot protect personal data on a broad scale, and raises other important legal issues.

The new EU-US Privacy Shield demonstrates both the reality and illusion of data transfer regulation. It represents a serious attempt to strengthen individual rights in line with the *Schrems* judgment, and is a much more detailed and weighty arrangement than the Safe Harbour. It also contains a number of novel mechanisms that could provide a basis for increasing trust in the protection given to international data transfers. However, it also demonstrates how EU data protection law tends to resolve questions concerning the regulation of international data transfers through verbose documentation and procedural mechanisms that are lengthy, untransparent, formalistic, and unintelligible to the average individual. It is also likely to be challenged before the CJEU.

In exploring the reality and illusion of protection for international data transfers, I will first summarize the judgment, before going on to examine its main holdings. In particular, I will analyse the Court's affirmation of the fundamental right to data protection and extension of its scope to third countries; its strengthening of the role of DPAs; and its definition of an adequate level of data protection for data transfers. I will explain why the correct legal measure of adequate protection for international data transfers is the EU Charter of Fundamental Rights, though some uncertainties remain because of the lack of EU competence over national security activities. I will also examine the concept of "essential equivalence" that the Court articulated, which both requires a high level of protection under the Charter, and raises questions as to how the DPAs and the courts will be able to cope with the burden that the CJEU has placed upon them. I will also consider some legal issues presented by the Privacy Shield.

I will then move from the positivistic level to the meta level, and will discuss the implications of the judgment for other data transfer mechanisms provided for both in the Directive and in the EU General Data Protection Regulation (GDPR)²¹ that will likely take effect in 2018. I will

²¹ Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), COM(2012) 11 final, 25 January, 2012. At this time the final version of the GDPR has not yet been published in the EU Official Journal, but a version of 15 December 2015 agreed on between the Council and the European Parliament is available on the web site of the LIBE Committee of the Parliament at the following link: <http://www.emeeeting.europarl.europa.eu/committees/agenda/201512/LIBE/LIBE%282015%291217_1/sitt-1739884>.

examine the reactions to the judgment, and explain why they do not provide meaningful protection for data transfers. I will show how legal issues of data transfer regulation are intertwined with the underlying political positions of the parties involved, and will discuss the implications of the judgment for third countries. Finally, I will provide some suggestions for a way forward to move regulation of international data transfers from illusion to reality.

II. The judgment and its holdings

A. Background and facts

The facts of the judgment will be briefly summarized here. Further information is provided on the plaintiff's web site,²² and in the judgment of the Irish High Court that resulted in the reference for a preliminary ruling being sent to the CJEU.²³

The complainant, Mr. Maximilian Schrems, brought several complaints against Facebook before the Irish Data Protection Commissioner (DPC), based on, among other things, Facebook's membership in the Safe Harbour. Safe Harbour was a self-regulatory mechanism that US-based companies could join to provide protection for personal data transferred from the EU to the US. It was comprised of a number of principles based on EU data protection law with which Safe Harbour member companies had to commit to comply, and was overseen by the US Federal Trade Commission (FTC). In 2000 the Commission issued a formal decision under Article 25²⁴ of the Directive finding that transfers provide adequate protection under EU data protection law.

Following the Snowden revelations of 2013, which contained allegations of widespread surveillance of Internet data by the US intelligence agencies, Schrems then filed further complaints with the DPC, alleging that there was no meaningful protection in US privacy law and practice with regard to intelligence surveillance. The DPC took the position that under Article 25(6) of the Directive, it could not question the Commission's determination of the Safe Harbour as providing adequate protection. Schrems argued that the DPC should use its statutory powers to find that no adequate protection existed under the Safe Harbour, and that it should order Facebook to cease its data transfers to the US. In 2013 he sought judicial review in the Irish High Court against the DPC's decision not to proceed against Facebook. In a judgment of 18 June 2014, Mr. Justice Hogan of the High Court referred the following two questions to the CJEU:

“(1) Whether in the course of determining a complaint which has been made to an independent office holder who has been vested by statute with the functions of administering and enforcing data protection legislation that personal data is being

²² See <<http://europe-v-facebook.org/EN/en.html>>.

²³ *Schrems v Data Protection Commissioner* [2014] IEHC 310; [2014] 2 ILRM 441; *Schrems v Data Protection Commissioner* (No.2) [2014] IEHC 351; [2014] 2 ILRM 506.

²⁴ Article 25(6) of the Directive (n 2) provides as follows: “The Commission may find, in accordance with the procedure referred to in Article 31 (2), that a third country ensures an adequate level of protection within the meaning of paragraph 2 of this Article, by reason of its domestic law or of the international commitments it has entered into, particularly upon conclusion of the negotiations referred to in paragraph 5, for the protection of the private lives and basic freedoms and rights of individuals. Member States shall take the measures necessary to comply with the Commission's decision.”

transferred to another third country (in this case, the United States of America) the laws and practices of which, it is claimed, do not contain adequate protections for the data subject, that office holder is absolutely bound by the Community finding to the contrary contained in [Decision 2000/520] having regard to Article 7, Article 8 and Article 47 of [the Charter], the provisions of Article 25(6) of Directive [95/46] notwithstanding?

(2) Or, alternatively, may and/or must the office holder conduct his or her own investigation of the matter in the light of factual developments in the meantime since that Commission decision was first published?”²⁵

On 23 September 2015, Advocate General Bot delivered his opinion. He found that the two questions referred to the CJEU should be answered so that “the existence of a decision adopted by the European Commission on the basis of Article 25(6) of Directive 95/46 does not have the effect of preventing a national supervisory authority from investigating a complaint alleging that a third country does not ensure an adequate level of protection of the personal data transferred and, where appropriate, from suspending the transfer of that data”, and that the Safe Harbour decision of the Commission should be held invalid.²⁶

B. Main holdings

On October 6, the Grand Chamber of the CJEU issued its judgment. The Court broadly agreed with the conclusions of Advocate General Bot concerning the two questions put to it, finding that the DPAs were not prevented by Article 25(6) from examining claims related to the adequacy of protection under a Commission decision, and that the decision underlying the Safe Harbour was invalid. The following were the main points that the Court made (in this section references in parentheses will be made to the relevant paragraphs of the judgment).

The CJEU first considered the powers of the national DPAs when the Commission has issued an adequacy decision under Article 25(6) of the Directive. It found that all provisions of the Directive must be interpreted in light of a high level of fundamental rights protection under the Charter and the Court’s case law interpreting the Charter (paras. 38-39). In considering the powers of the DPAs, the Court stressed the importance of their independence (paras. 40-43), and mentioned that their powers do not extend to data processing carried out in a third country (para. 44). However, it further held that the transfer of personal data to a third country is itself an act of data processing, and thus falls within Member State law (para. 45) and the supervisory powers of the DPAs (para. 47). Since a Commission decision concerning adequacy under Article 25(6) of the Directive is binding on the Member States and must be given full effect by them, the DPAs cannot take measures contrary to such a decision (para. 52).

However, a Commission decision cannot preclude an individual from filing a claim with a DPA concerning the adequacy of protection, nor can such a decision eliminate or reduce their powers (paras. 53-58). Such a claim is to be understood as essentially concerning “whether

²⁵ Reference for a preliminary ruling from High Court of Ireland (Ireland) made on 25 July 2014 – Maximillian Schrems v Data Protection Commissioner (Case C-362/14), <<http://curia.europa.eu/juris/document/document.jsf?docid=157862&doclang=EN>>.

²⁶ Opinion of Advocate General Bot (n 5), para. 237.

that decision is compatible with the protection of the privacy and of the fundamental rights and freedoms of individuals” (para. 59). Only the CJEU has the power to declare an EU act invalid, including a Commission adequacy decision (para. 61), and while national courts and the DPAs may consider the validity of an EU act, they may not themselves declare it invalid (para. 62).

Thus, when an individual makes a claim to a DPA contesting the compatibility of a data transfer based on an adequacy decision with the protection of privacy and fundamental rights, the DPA must examine the claim “with all due diligence” (para. 63). When the DPA rejects such a claim as unfounded, the individual must have access to judicial remedies allowing him to contest this decision before national courts, and such courts “must stay proceedings and make a reference to the Court for a preliminary ruling on validity where they consider that one or more grounds for invalidity put forward by the parties or, as the case may be, raised by them of their own motion are well founded ” (para. 64). Conversely, when the DPA finds such claim to be well-founded, it must “be able to engage in legal proceedings”, and the national legislature must “provide for legal remedies enabling the national supervisory authority concerned to put forward the objections which it considers well founded before the national courts in order for them, if they share its doubts as to the validity of the Commission decision, to make a reference for a preliminary ruling for the purpose of examination of the decision’s validity” (para. 65).

The Court then considered the validity of the Safe Haber itself, agreeing with Mr. Justice Hogan that it was necessary to consider this question in order to give a full answer to the questions referred (para. 67). The Court went on to find that, based on the EU Charter of Fundamental Rights, the term “an adequate level of protection” as used in the Directive must be understood as “requiring the third country in fact to ensure, by reason of its domestic law or its international commitments, a level of protection of fundamental rights and freedoms that is essentially equivalent to that guaranteed within the European Union by virtue of Directive 95/46 read in the light of the Charter”, while not requiring that the level be identical to that under EU law (para. 73). Without this requirement, “the high level of protection guaranteed by Directive 95/46 read in the light of the Charter could easily be circumvented by transfers of personal data from the European Union to third countries for the purpose of being processed in those countries” (para. 73). While the means to which a third country has recourse for ensuring a high level of protection may differ from those employed within the EU, they must prove to be effective in practice (para. 74).

When assessing the level of protection in a third country, this requires the Commission to “take account of all the circumstances surrounding a transfer of personal data to a third country” (para. 75), to check periodically whether the adequacy assessment is still justified (para. 76), and to take account of circumstances that have arisen after adoption of the decision (para. 77). All this means that “the Commission’s discretion as to the adequacy of the level of protection ensured by a third country is reduced, with the result that review of the requirements stemming from Article 25 of Directive 95/46, read in the light of the Charter, should be strict” (para. 78).

The Court then dealt with the validity of the adequacy decision regarding the Safe Harbour. While it found that “a system of self-certification is not in itself contrary to the requirement

laid down in Article 25(6) of Directive 95/46 that the third country concerned must ensure an adequate level of protection ‘by reason of its domestic law or ... international commitments’, the reliability of such a system is based on “the establishment of effective detection and supervision mechanisms enabling any infringements of the rules ensuring the protection of fundamental rights, in particular the right to respect for private life and the right to protection of personal data, to be identified and punished in practice” (para. 81). It noted that public authorities in the US are not required to comply with the Safe Harbour principles (para. 82), and that the Safe Harbour decision of the Commission does not contain sufficient findings explaining how the US ensures an adequate level of protection (para. 83).

The CJEU then noted that under the Safe Harbour decision, the applicability of the principles may be limited to meet, for example, national security, public interest, or law enforcement requirements (para. 84), and that the Decision states that “[c]learly, where US law imposes a conflicting obligation, US organisations whether in the safe harbour or not must comply with the law” (para. 85). It found that these provisions in effect give US law primacy over EU fundamental rights in situations where they conflict (paras. 86-87), and that to establish an interference with fundamental rights, “it does not matter whether the information in question relating to private life is sensitive or whether the persons concerned have suffered any adverse consequences on account of that interference” (para. 87). Moreover, the Safe Harbour decision does not contain any finding concerning limitations on the powers of public authorities (such as law enforcement authorities) in the US to interfere with fundamental rights (para. 88).

The Court then referred to previous statements by the Commission that “the United States authorities were able to access the personal data transferred from the Member States to the United States and process it in a way incompatible, in particular, with the purposes for which it was transferred, beyond what was strictly necessary and proportionate to the protection of national security” (para. 90). It mentioned the need under EU law for there to be clear and precise rules regarding the scope of application of a measure and for effective protection against the risk of abuse of data (para. 91), and that derogations and limitations in relation to data protection should apply only when strictly necessary (para. 92), and found that US law does not meet these standards (para. 93-95).

Of particular importance is the Court’s statement that “legislation is not limited to what is strictly necessary where it authorises, on a generalised basis, storage of all the personal data of all the persons whose data has been transferred from the European Union to the United States without any differentiation, limitation or exception being made in the light of the objective pursued and without an objective criterion being laid down by which to determine the limits of the access of the public authorities to the data, and of its subsequent use, for purposes which are specific, strictly restricted and capable of justifying the interference which both access to that data and its use entail” (para. 93). The Court found that “legislation permitting the public authorities to have access on a generalised basis to the content of electronic communications must be regarded as compromising the *essence* of the fundamental right to respect for private life, as guaranteed by Article 7 of the Charter” (para. 94), and that “legislation not providing for any possibility for an individual to pursue legal remedies in order to have access to personal data relating to him, or to obtain the rectification or erasure of such data, does not respect the *essence* of the fundamental right

to effective judicial protection, as enshrined in Article 47 of the Charter” (para. 95) (emphasis added in both cases).

The Court went on to note that the Commission did not state in its Safe Harbour decision that the US ensures an adequate level of protection (para. 97), and that the decision was accordingly invalid, without there being any need for it to examine the substance of the Safe Harbour principles (para. 98). Throughout this section of the judgment, the CJEU makes extensive reference to its earlier ruling in *Digital Rights Ireland*,²⁷ in which the Court strongly affirmed data protection rights in the digital context. The Court also found that Article 3 of the Safe Harbour decision contained impermissible limitations on the powers of the data protection authorities (paras. 99-104).

III. Main themes of the judgment

The importance of the judgment rests in four main themes that the Court focused on, and that will be discussed in turn.

A. Affirming the right to data protection

The judgment strongly affirms data protection as a fundamental right under EU law. The Court makes repeated reference to fundamental rights under the Charter, and to previous data protection judgments such as *Digital Rights Ireland* and *Google Spain*.²⁸ This emphasis on fundamental rights is further seen in statements such as that the Commission’s discretion in pronouncing on the adequacy of protection in third countries should be “strict” (para. 78).

Particularly significant is the fact that the Court found that generalized access to data by public authorities (i.e., law enforcement authorities) compromises the “essence” of the right to private life under Article 7 of the Charter, since this means that no proportionality or balancing analysis involving other rights and freedoms under the Charter is required with regard to such violation.²⁹ At the same time, it is unclear how the Court could find a violation of the essence of right to privacy under Article 7 but not one of the essence of the right to the protection of personal data under Article 8. The rights to data protection and privacy are closely linked, and surveillance of data by intelligence services self-evidently involves the processing of personal data. In its *Digital Rights Ireland* judgment in which the Court invalidated the EU Data Retention Directive,³⁰ it found that the essence of the right to data protection was not violated since the Directive required respect for “certain principles of data protection and data security”,³¹ an argument that seems questionable since data security, while certainly important, is not one of the central elements of data protection. The Court’s interpretation of the essence of the rights to privacy and data protection in *Schrems*

²⁷ *Digital Rights Ireland and Seitlinger*, Joined Cases C-293/12 and C-594/12, 8 April 2014, ECLI:EU:C:2014:238.

²⁸ *Google Spain v. AEPD and Mario Costeja Gonzalez*, Case C-131/12, 13 May 2014, ECLI:EU:C:2014:317.

²⁹ See Martin Scheinin, “The Essence of Privacy, and Varying Degrees of Intrusion”, *Verfassungsblog*, 7 October 2015, <<http://verfassungsblog.de/the-essence-of-privacy-and-varying-degrees-of-intrusion/>>.

³⁰ Directive (EC) 2006/24 of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive (EC) 2002/58, [2006] OJ L105/54.

³¹ *Digital Rights Ireland and Seitlinger* (n 27), para. 40. For a criticism of the Court’s analysis in *Digital Rights Ireland*, see Orla Lynskey, *The Foundations of EU Data Protection Law* 270-272 (Oxford University Press 2015).

may thus reflect its longstanding confusion about the distinction between these two rights.³²

B. Extending data protection rights to third countries

The Court indicated that while it was not directly applying EU law to third countries (para. 44), EU law applied to data transfers since “the operation consisting in having personal data transferred from a Member State to a third country constitutes, in itself, processing of personal data within the meaning of Article 2(b) of Directive 95/46”.³³ While it may be logical to distinguish between the direct application of EU law in a third country and the transfer of EU-based data to such country, in the end this is a distinction without a difference, since, as the *Schrems* judgment makes clear, such transfer is possible only when the third country provides protections that are “essentially equivalent” to those under EU law. The *Schrems* case thus illustrates that any distinction between extraterritorial and territorial jurisdiction has become meaningless in the context of regulation of international data transfers.³⁴

The Court’s only previous case dealing specifically with regulation of international data transfers was its *Lindqvist* judgment of 2003,³⁵ in which it found that there is no data transfer to a third country within the meaning of Article 25 of the Directive when an individual in a Member State loads personal data onto an Internet page stored on a site hosted within the EU. The judgment in *Schrems* goes beyond *Lindqvist* by relating the requirement of an adequate level of data protection under the Directive to the high level of data protection required by Charter.³⁶ It thus seems that the Court believes that a high level of data protection is required under the Charter for data transfers to third countries, and that, if it were faced today with a case involving facts similar to those in *Lindqvist*, it would be more hesitant to find that Article 25 does not apply to placing personal data on an Internet site, since this will result in access to EU data in countries where the level of data protection may not be adequate.

By determining the standard that third countries must meet to be declared “adequate” in the eyes of the EU, the CJEU has effectively set the global data protection bar at a high level. Many third countries will revise their data protection law and practice in an attempt to meet this standard, so that the conclusions of the Court will reverberate around the world.

Bradford has referred to the so-called “Brussels effect”, in which the EU is engaged in unilateral regulation of global markets,³⁷ which can be seen in the influence that EU data

³² See regarding the connection between the rights to data protection and privacy in the Court’s jurisprudence Lynskey (n 31), at 89-130 (Oxford University Press 2015); Juliane Kokott and Christoph Sobotta, “The distinction between privacy and data protection in the jurisprudence of the CJEU and the ECtHR”, 3 *International Data Privacy Law* 222 (2013); Hielke Hijmans and Alfonso Scirocco, “Shortcomings in EU Data Protection in the Third and the Second Pillars. Can the Lisbon Treaty Be Expected to Help?”, 46 *Common Market Law Review* 1485 (2009).

³³ *Schrems* (n 3), para. 45.

³⁴ For criticism of the distinction between territorial and extraterritorial jurisdiction in the context of regulation of international data transfers, see Christopher Kuner, “Extraterritoriality and regulation of international data transfers in EU data protection law”, 5 *International Data Privacy Law* 235 (2015).

³⁵ *Bodil Lindqvist*, Case C-101/01 [2003] ECR I-12971.

³⁶ *Schrems* (n 3), para. 73.

³⁷ See Anu Bradford, “The Brussels Effect”, 107 *Northwestern University Law Review* 1 (2013). For a critical view of the this argument, see Joanne Scott, “The new EU ‘extraterritoriality’”, 51 *Common Market Law Review*

protection law has had on the development of data protection legislation in many third countries.³⁸ The *Schrems* judgment can be seen as an indirect example of the Brussels effect, since it seems to be based on the rationale that withholding recognition of data transfers to the US may result in the US adopting standards closer to the European model.³⁹

The irony is that the judgment results in withdrawal of regulatory recognition from a mechanism (i.e., the Safe Harbour) that did influence such standards. Despite the criticisms that caused the CJEU to invalidate the Safe Harbour, research into compliance with privacy “on the ground” has found that EU law in general, and the Safe Harbour in particular, have played a major role in shaping how companies in the US process personal data.⁴⁰ For example, regulators in the US have explained that the invalidation of the Safe Harbour may weaken the protection of personal data transferred from the EU to the US, first by making the protection given to it less transparent, and second by limiting the ability of the US Federal Trade Commission to take action against companies in the US for misrepresenting their compliance with EU data protection standards.⁴¹ Time will tell if new Privacy Shield, which includes strengthened versions of the standards contained in the Safe Harbour and also provides for enforcement by the FTC, will lead to further influence of EU data protection concepts on US practices.

C. Increasing both the role of DPAs and their burdens

By confirming that DPAs may not be precluded from examining the level of data protection in a third country set out in Commission adequacy decisions, the Court has substantially strengthened their role at the expense of that of the Commission. At the same time, the judgment practically invites individuals to bring claims regarding adequacy to DPAs, who are then required to use “all due diligence” to examine them.⁴² The DPAs are notoriously short on personnel and resources,⁴³ and evaluating the level of data protection in third countries can be a complicated exercise, so this new role will put substantial pressure on them.

1343 (2014); Joanne Scott, “Extraterritoriality and Territorial Extension in EU Law”, 62 *American Journal of Comparative Law* 87 (2014).

³⁸ See Lee Bygrave, *Data Privacy Law: An International Perspective* (Oxford University Press 2014), at locations 6215-6216 (Kindle edition); Paul De Hert and Vagelis Papakonstantinou, “Three scenarios for international governance of data privacy: towards an international data privacy organization, preferably a UN agency?”, *I/S: A Journal of Law and Policy for the Information Society*, vol. 9, no. 2, 2013, 271-324, at 287-288; Graham Greenleaf, “The Influence of European Data Privacy Standards outside Europe: Implications for Globalization of Convention 108”, 2 *International Data Privacy Law* 68 (2012). See regarding the influence of EU data transfer regulation in other legal systems Christopher Kuner, *Transborder Data Flows and Data Privacy Law* (Oxford University Press 2013).

³⁹ See interview with CJEU President Koen Lenaerts (n 14), in which he states “If this is also affecting some dealings internationally, why would Europe not be proud to contribute its requiring standards of respect of fundamental rights to the world in general?”

⁴⁰ Kenneth Bamberger and Deirdre Mulligan, *Privacy on the Ground* (MIT Press 2015), at 65, noting with regard to a survey of company privacy officers in the US that “respondents explained that European law plays a large role in shaping such company-wide privacy policies”, and that “the influence of US law was evidenced by specific activities such as Safe Harbor certification”.

⁴¹ Brill (n 8), at 6.

⁴² *Schrems* (n 3), para. 78.

⁴³ European Union Agency for Fundamental Rights, “Data Protection in the European Union: the role of National Data Protection Authorities”, 2010, <http://fra.europa.eu/sites/default/files/fra_uploads/815-Data-protection_en.pdf>.

Article 25 was intended to lead to a harmonized procedure for Commission adequacy decisions,⁴⁴ but under the judgment, DPAs may investigate complaints from individuals concerning adequacy decisions, though they may not themselves declare a decision illegal. In such investigations, the DPAs may make use of the powers granted to them by national law under Article 28 of the Directive, which the Court lists as “in particular, investigative powers, such as the power to collect all the information necessary for the performance of their supervisory duties, effective powers of intervention, such as that of imposing a temporary or definitive ban on processing of data, and the power to engage in legal proceedings”.⁴⁵ If a DPA finds such a claim to be well-founded, then it must be able to engage in legal proceedings, which presumably means that it must be able to make use of the powers granted to it by legislation and to call on the national courts to help enforce them if necessary. The national legislator must enact legislation allowing the DPAs to provide for legal remedies, and if a national court is involved in a case in which it has doubts about the validity of a Commission adequacy decision, the court must make a reference for a preliminary ruling to the CJEU to examine the decision’s validity.

The judgment may result in a patchwork of different views among the DPAs and Member State courts on the level of protection in third countries, which could lead to uneven protection for individuals throughout the EU.⁴⁶ Such fragmentation effectively defeats the purpose of adequacy decisions by subjecting them to differing national interpretations, and by miring them in regulatory procedures and litigation as to their validity. Presumably the fact that the CJEU is the final arbiter of what constitute adequate protection will reduce the fragmentation, and with the GDPR being a highly-detailed EU regulation, under it the DPAs will have to take a harmonized view of what constitutes adequate protection.⁴⁷ The so-called consistency and cooperation mechanisms of the GDPR, which require the DPAs to cooperate in the scope of the work of the new EU Data Protection Board (replacing the Article 29 Working Party), should also hopefully lead to a more harmonised view of adequacy in third countries. However, it can take years for a case to reach the CJEU, and under the GDPR each individual DPA will have the power to suspend data transfers to third countries.⁴⁸ Thus, it seems there is the potential for a difference of views regarding adequate protection in third countries, with resultant legal uncertainty.

D. Defining an adequate level of data protection

⁴⁴ See Spiros Simitis and Ulrich Dammann, *EG-Datenschutzrichtlinie* (Nomos 1997), at 275.

⁴⁵ *Schrems* (n 3), para. 43.

⁴⁶ See European Commission, “Safeguarding Privacy in a Connected World, A European Data Protection Framework for the 21st Century”, COM(2012) 9 final, 25 January 2012, <<http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52012DC0009&from=en>>, at 7, stating that the current fragmentation of data protection law in the EU has led to “uneven protection for individuals”,

⁴⁷ See *Stefanio Melloni v Ministerio Fiscal*, Case C-399/11, 26 February 2013, ECLI:EU:C:2013:107, in which the CJEU found that when the EU legislator has harmonized fundamental rights protection in an exhaustive way, Member States are not allowed to “top up” fundamental rights protection. But see Peter Blume and Christian Wiese Svanberg, “The Proposed Data Protection Regulation: The Illusion of Harmonisation, the Private/Public Sector Divide and the Bureaucratic Apparatus”, in Catherine Barnard et al. (eds.), 15 *Cambridge Yearbook of European Legal Studies* 27 (Hart Publishing, 2012-2013), arguing that there will be many exceptions to harmonization under the GDPR.

⁴⁸ Article 53(1b)(h) of the GDPR version adopted by the Council and European Parliament on 15 December 2015 (n 21).

The most controversial issue dealt with in the judgment is the Court's definition of an adequate level of protection for international data transfers under the Directive, which it defines as protection that is "essentially equivalent" but not necessarily "identical" to that under EU law. The standard that the Court adopts is best understood as a high degree of protection as determined by reference to the EU Charter of Fundamental Rights. At the same time, the allocation to the Member States of responsibility for national security presents the risks of gaps in the level of data protection, which should be addressed by the EU legislator and the Court.

1. EU standards and third country standards

The "elephant in the room" in the debate about the definition of an adequate level of protection is the criticism in the judgment of US intelligence surveillance practices. The *Schrems* judgment does not make any explicit statements concerning the adequacy of the US legal system as a whole, US legal rules concerning intelligence surveillance, or the details of the Safe Harbour.⁴⁹ However, there is no doubt that the judgment is based on a condemnation of US intelligence gathering practices and their effect on fundamental rights under EU data protection law, as can be seen, for example, in its Court's mention of studies by the Commission finding that US authorities were able to access data in ways that did not meet EU legal standards in areas such as purpose limitation, necessity, and proportionality.⁵⁰

Some argue that it is hypocritical for EU policymakers and the CJEU to concern themselves in such detail with the standards of data protection for intelligence surveillance outside the EU, when the standards that apply in the EU seem lacking in many respects.⁵¹ Under Article 4(2) of the Treaty on European Union (TEU),⁵² national security remains the sole responsibility of the EU Member States, and activities concerning national security are outside the scope of the EU Data Protection Directive and the GDPR.⁵³ In addition, it seems that there is widespread sharing of information between the US and other intelligence services, such as under the "Five Eyes"⁵⁴ intelligence-sharing network which includes the UK (the other members are Australia, Canada, New Zealand, and the US).

⁴⁹ See *Schrems* (n 3), paras. 88 and 98. See also interview with CJEU President Koen Lenaerts (n 14), in which he states "We are not judging the U.S. system here, we are judging the requirements of EU law in terms of the conditions to transfer data to third countries, whatever they be".

⁵⁰ See *Schrems* (n 3), para. 90.

⁵¹ See, e.g., Opinion of Geoffrey Robertson QC for Facebook, 14 January 2016, <<http://blogs.ft.com/brusselsblog/files/2016/01/Geoffrey-Robertson-QC.docx>>; Sidley Austin LLP, "Essentially equivalent: A comparison of the legal orders for privacy and data protection in the European Union and United States" (n 13). See regarding oversight of intelligence surveillance in the Member States, European Union for Fundamental Rights, "Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU", November 2015, <http://fra.europa.eu/sites/default/files/fra_uploads/fra-2015-surveillance-intelligence-services_en.pdf>; Stefan Heumann and Ben Scott, "Law and Policy in Internet Surveillance Programs: United States, Great Britain and Germany", September 2013, <<http://www.stiftung-nv.de/publikation/law-and-policy-internet-surveillance-programs-united-states-great-britain-and-germany>>.

⁵² Consolidated Version of the Treaty on European Union, [2012] O.J. C 326/13.

⁵³ EU Data Protection Directive (n 2), Article 3(2)) and Recital 14 of the GDPR version adopted by the Council and European Parliament on 15 December 2015 (n 21), exempting matters of national security from the scope of the Directive and the GDPR.

⁵⁴ See regarding the Five Eyes alliance Glenn Greenwald, *No Place to Hide* (Penguin 2014), at locations 1581, 1854-1900 (Kindle edition).

However, it is pointless for the EU and the US to engage in arguments about which side's system of data protection is better, since this is irrelevant for the standard of protection articulated by the Court. A violation of fundamental rights by a third country cannot be excused because EU standards may themselves be lacking, and arguments along these lines are examples of a logical fallacy known as "tu quoque" ("you too"). While such objections may be understandable, there is no parallel in EU law to the common law doctrine of "unclean hands" which may underlie the arguments along these lines by US commentators.⁵⁵

2. The Charter as the standard, with questions regarding national security

From a legal point of view, the main issue is what standard should be used to measure essential equivalence as the Court has defined it. Despite uncertainties caused by the allocation of competence over national security to Member States, the correct measure is provided by the EU Charter of Fundamental Rights.

The Court states several times in the *Schrems* judgment that the fundamental right to data protection is to be measured against the Charter,⁵⁶ and makes frequent references both to the Charter and to previous judgments applying it, in particular *Digital Rights Ireland*. It also points out that the standard for an adequate level of protection is high,⁵⁷ and that the Commission's review of requirements deriving from Article 25 of the Directive should be read strictly in light of the Charter.⁵⁸ The Court's assessment of fundamental rights also seems to be based solely on the Charter in the vast majority of cases.⁵⁹ Thus, there seems little doubt that the Charter should be the measure of protection for international data transfers from the EU.

While provisions such as Article 4(2) TEU place the competence for national security with the Member States, the allocation of legislative competences in EU law is not the same as the scope of application of the Charter.⁶⁰ The Charter applies to the Member States when they implement EU law,⁶¹ and thus applies to situations covered by the Directive (for example, when EU companies acting as data controllers transfer data to EU or third country intelligence services).⁶² There are many data protection situations involving national security where the Charter does apply, such as to questions about whether national legislation

⁵⁵ See regarding the unclean hands doctrine and tu quoque arguments, Kevin W. Saunders, "Informal Fallacies in Legal Argumentation", 44 *South Carolina Law Review* 343, 373-374 (1992).

⁵⁶ See, e.g., *Schrems* (n 3), paras. 38 ("It should be recalled first of all that the provisions of Directive 95/46, inasmuch as they govern the processing of personal data liable to infringe fundamental freedoms, in particular the right to respect for private life, must necessarily be interpreted in the light of the fundamental rights guaranteed by the Charter") and 67 ("it should be examined whether that decision complies with the requirements stemming from Directive 95/46 read in the light of the Charter").

⁵⁷ *Ibid.*, paras. 39, 72, and 73.

⁵⁸ *Ibid.*, para. 78.

⁵⁹ Clara Rauegger, "The Interplay Between the Charter and National Constitutions after *Åkerberg Fransson* and *Melloni*", in: Sybe de Vries, Ulf Bernitz and Stephen Weatherill (eds.), *The EU Charter of Fundamental Rights as a Binding Instrument* 93, 122 (Hart 2015).

⁶⁰ Rauegger (n 59), at 97.

⁶¹ Charter, Article 51(1). See Rauegger (n 59), at 97.

⁶² European Union for Fundamental Rights, "Surveillance by intelligence services" (n 51), at 11.

restricting data protection rights for reasons of national security is valid under Article 13(1)(a) of the Directive,⁶³ and to investigations regarding such restrictions by DPAs under Article 28(4) of the Directive.⁶⁴

Nor does the fact that Article 4 place competence for national security with the Member States necessarily mean that the Charter does not apply to the activities of third countries when they violate fundamental rights of EU individuals. Neither the TEU nor the Directive explicitly or implicitly remove the activities of third countries from scrutiny under EU law. The territorial scope of the Charter is the same as that of EU law,⁶⁵ and to the extent that EU law can apply to the activities of third country intelligence agencies, the Charter should as well.

At the same time, the allocation of responsibility for national security to the Member States risks producing gaps in protection. On the one hand, the Charter sets a high standard for the fundamental right of data protection, as the *Schrems* judgment shows, but on the other hand, national security activities are wholly carried out by the Member State. There is thus a divergence between the level at which applicable fundamental rights law is enacted (i.e., at the EU level) and that at which national security activities are actually carried out (i.e., by the Member States). In many or most situations involving data protection rights either EU law applies or there is an overlap between EU and Member State law, which results in application of EU law and thus of the Charter. However, when EU law does not apply, such situations are governed solely by Member State constitutional law.⁶⁶ This could produce a gap in protection if Member State law produces a lower level of protection than the Charter.

It will also not always be possible to distinguish situations where personal data are processed for national security purposes. In most routine situations personal data are transferred for purposes that have nothing to do with national security (e.g., for commercial or personal reasons), but there are many situations where the purposes of transfer may be mixed so that it is impossible to distinguish them, i.e., when data are collected or transferred for commercial purposes but then accessed by national intelligence agencies after the fact.⁶⁷

⁶³ Article 13(1)(a) provides that “Member States may adopt legislative measures to restrict the scope of the obligations and rights provided for in Articles 6(1), 10, 11(1), 12 and 21 when such a restriction constitutes a necessary measures to safeguard: (a) national security...” Article 21 of the GDPR version adopted by the Council and European Parliament on 15 December 2015 (n 21) also allows restrictions to be put on data protection rights for national security reasons under strict conditions.

⁶⁴ Article 28(4) provides in part that “Each supervisory authority shall, in particular, hear claims for checks on the lawfulness of data processing lodged by any person when the national provisions adopted pursuant to Article 13 of this Directive apply.”

⁶⁵ See Violeta Moreno-Lax and Cathryn Costello, “The Extraterritorial Application of the EU Charter of Fundamental Rights: From Territoriality to Facticity, the Effectiveness Model”, in: Steve Peers, Tamara Harvey, Jeff Kenner and Angela Ward (eds.), *The EU Charter of Fundamental Rights, A Commentary* (Hart Publishing 2014), at 1657-1683.

⁶⁶ See Bruno de Witte, “Article 53—Level of Protection”, in: Peers et al. (n 65), at para. 53.12 (Kindle edition), stating “When a legal situation is outside the scope of EU law and within the scope of domestic law, there is no problem: Article 53 of the Charter simply confirms the evident rule that national constitutional rights will fully apply to such cases, notwithstanding any divergent formulation of those rights in the Charter”.

⁶⁷ See in this regard Fred H. Cate, James X. Dempsey, and Ira S. Rubenstein, “Systematic government access to private-sector data”, 2 *International Data Privacy Law* 195 (2012).

It seems likely that the Court would take a restrictive view of claims that the Charter should not apply to data protection issues involving national security. Under Article 53 of the Charter nothing in it can be interpreted as adversely affecting human rights, and the constitutional autonomy of EU law, which the Court has taken pains to emphasize,⁶⁸ would not tolerate a lowering of the level of fundamental rights under the Charter based on the positions of some Member States or a margin of discretion or margin of appreciation based on the European Convention of Human Rights.⁶⁹ The official Explanations to the Charter prepared under the authority of the Praesidium of the Convention that drafted it also state that the Charter does not follow a “lowest common denominator” approach, and that Charter rights should be interpreted to offer a high standard of protection.⁷⁰ The Charter is intended to prevent a “race to the bottom” in fundamental rights standards,⁷¹ such as could occur if low standards in certain Member States were taken as the measure for the fundamental right to data protection. Thus, allocation of legislative competence over national security to the Member States rather than the EU does not mean that they have unfettered discretion to interpret the concept in order to remove their activities from scrutiny under EU fundamental rights law.⁷²

However, the unclear delineation and definition of “national security” can produce confusion about the standards that should apply to Member State activities.⁷³ There is an urgent need for limitation or clarification of the meaning of “national security” in the context of data protection rights. The Charter requires that the meaning and scope of rights under it shall be “the same” as under the European Convention on Human Rights,⁷⁴ which is not limited by any derogation for national security, and clarification could come via challenges to Member State intelligence surveillance practices brought before the European Court of Human Rights.⁷⁵ It is to be hoped that a case involving the allocation of national security to the Member States will reach the CJEU as well, in order to clarify the conditions under which the Charter applies to data protection issues that are affected by national security activities.

⁶⁸ See Opinion 2/13 of the Court, 18 December 2014, CLI:EU:C:2014:2454.

⁶⁹ See Koen Lenaerts and Jose Antonio Gutierrez-Fons, “The Place of the Charter in the EU Constitutional Edifice”, in: Peers et al. (n 65), at para. 55.60 (Kindle edition), stating “if the ECtHR ever decides to lower the level of protection below that guaranteed by EU law, by virtue of Article 53 of the Charter, the CJEU will be precluded from interpreting the provisions of the Charter in a regressive fashion.”

⁷⁰ “Explanations Relating to the Charter of Fundamental Rights”, [2007] OJ C303/17, at C303/34.

⁷¹ Rauegger (n 59), at 125.

⁷² See *ZZ v. Secretary of State for the Home Department*, Case C-300/11, 4 June 2013, ECLI:EU:C:2013:363, para. 38, where the Court held that “the mere fact that a decision concerns State security cannot result in European Union law being inapplicable”. With regard to the related concepts of public policy and public security, see *P.I. v. Oberbürgermeisterin der Stadt Remscheid*, Case C-348/09, 22 May 2012, EU:C:2012:300, stating at para. 23 that “While Member States essentially retain the freedom to determine the requirements of public policy and public security in accordance with their national needs, which can vary from one Member State to another and from one era to another, particularly as justification for a derogation from the fundamental principle of free movement of persons, those requirements must nevertheless be interpreted strictly, so that their scope cannot be determined unilaterally by each Member State without any control by the institutions of the European Union”. See also Hielke Hijmans, *The European Union as a Constitutional Guardian of Internet Privacy and Data Protection: the story of Article 16 TFEU 157-162* (PhD thesis, University of Amsterdam and Vrije Universiteit Brussel, 2016).

⁷³ See European Union for Fundamental Rights, “Surveillance by intelligence services” (n 51), at 11.

⁷⁴ Charter, Article 52(3).

⁷⁵ *Big Brother Watch and Others v. The United Kingdom*, Case No. 58170/13 (pending).

3. The meaning of “essentially equivalent”

In the *Schrems* judgment, the Court explained that the standard of protection that third countries must meet under Article 25 of the Directive is one that is “essentially equivalent” to that under the Directive in light of the Charter.⁷⁶ It did so despite the fact that when the Directive was adopted, the EU legislator specifically preferred the term “adequate protection” over “equivalent protection”.⁷⁷ The Court gave a number of points of orientation to interpret the concept of essential equivalence, including the following (with parenthetical citations to the judgment):

- There must be a high level of fundamental rights protection under the Charter and the Court’s case law interpreting the Charter (paras. 38-39, 73), which should be judged strictly (para. 78).
- The third country in question must have a means for ensuring a high level of protection that is effective in practice (para. 74), in light of all the circumstances surrounding a transfer of personal data to a third country (para. 75). This must include periodic checks as to whether the adequacy assessment is still justified (para. 76) and take into account all circumstances that have arisen after adoption of the decision (para. 77).
- Adequate protection must take into account the country’s domestic law or international commitments (para. 71).
- Any system of self-certification must be reliable based on effective detection and supervision mechanisms enabling infringements of the rules, in particular the right to respect for private life and the protection of personal data, to be identified and punished in practice (para. 81).
- An adequacy decision must include a detailed explanation of how a country ensures an adequate level of protection (para. 83).
- There must not be limitations based on national security, public interest, or law enforcement requirements that give third country law primacy over EU law (paras. 85-87).
- Limitations must be placed on the power of public authorities (such as law enforcement authorities) to interfere with fundamental rights (para. 88). In particular, any such access must be strictly necessary and proportionate to the protection of values such as national security (para. 90), there must be clear and precise rules regarding the scope of application of a measure, and for effective protection against the risk of abuse of data (para. 91), and derogations and limitations in relation to data protection should apply only when strictly necessary (para. 92).
- Third country legislation must not authorize, on a generalised basis, storage of all the personal data transferred without any differentiation, limitation or exception being made in light of the objective pursued and without an objective criterion being laid down to determine the limits to the data, and its subsequent use, for purposes which are specific, strictly restricted and capable of justifying the interference entailed by access to that data and its use (para. 93).

This is a high standard that results from the Court’s strict interpretation of the Charter, and its previous judgments such as *Google Spain* and *Digital Rights Ireland*. The Court further emphasized the primacy that must be given to EU fundamental rights over conflicting third

⁷⁶ *Schrems* (n 3), para. 73.

⁷⁷ *Simitis and Dammann* (n 44), at 273.

country norms. The Article 29 Working Party has condensed these factors into a rather superficial four-part test for determining adequacy:⁷⁸

- “A. Processing should be based on clear, precise and accessible rules: this means that anyone who is reasonably informed should be able to foresee what might happen with her/his data where they are transferred;
- B. Necessity and proportionality with regard to the legitimate objectives pursued need to be demonstrated: a balance needs to be found between the objective for which the data are collected and accessed (generally national security) and the rights of the individual;
- C. An independent oversight mechanism should exist, that is both effective and impartial: this can either be a judge or another independent body, as long as it has sufficient ability to carry out the necessary checks;
- D. Effective remedies need to be available to the individual: anyone should have the right to defend her/his rights before an independent body.”

The term “essentially equivalent” seems to imply a comparison between third country data protection standards and EU standards, an enterprise that is fraught with difficulty. Data protection and privacy are “context-bound and linked to culture”,⁷⁹ making them difficult areas for comparative analysis. There are numerous theories used to compare different systems and concepts of constitutional and public law,⁸⁰ and selecting and refining the correct methodological approach in order to evaluate foreign legal systems of data protection is a lengthy and highly complex process. The European Commission has internal guidelines for conducting such studies, which have never been made public, but it is known that they typically can take several years and involve extensive participation by outside academic experts in foreign law. Comparison of legal systems is not a mechanical exercise, and particularly in an area like data protection requires going beyond analysis of legal texts to consider non-legal and social factors,⁸¹ including ones such as constitutional protection, treaty protection, human rights institutions, civil law protection, criminal law and administrative law, and self regulation.⁸²

The *Schrems* judgment foresees DPAs being able to question Commission adequacy decisions, and individuals being able to challenge them before national courts. One can be sceptical about how a DPA, with its limited resources, or a national court, with its focus on national or EU law, can conduct a sufficient examination of foreign law and a comparison with EU data protection law, particularly with regard to third countries like the US that have

⁷⁸ “Statement of the Article 29 Working Party on the Consequences of the Schrems Judgment”, 3 February 2016, <http://ec.europa.eu/justice/data-protection/article-29/press-material/press-release/art29_press_material/2016/20160203_statement_consequences_schrems_judgement_en.pdf>.

⁷⁹ Manuel José Cepeda Espinosa, “Privacy”, in: Michel Rosenfeld and Andrés Sajó, *The Oxford Handbook of Comparative Constitutional Law* (Oxford University Press 2012), at 967 (Kindle edition). This is true even between the different EU Member States. See M Cartabia, “Europe and Rights: Taking Dialogue Seriously”, 5 *European Constitutional Law Review* 5, 20 (2009).

⁸⁰ Vicki C. Jackson, “Comparative Constitutional Law: Methodologies”, in Rosenfeld and Sajó (n 79), at 54 (Kindle edition), mentioning classificatory, historical, normative, functional, and contextual approaches.

⁸¹ See, e.g., Günter Frankenberg, “Critical Comparisons: Re-thinking Comparative Law”, 26 *Harvard International Law Journal* 411 (1985).

⁸² Graham Greenleaf, *Asian Data Privacy Laws* (Oxford University Press 2014), at 53.

not enacted a horizontal system of data protection similar to EU law. Since the determinations of national courts will generally be accepted by the CJEU without further inquiry if a reference for a preliminary ruling is sent to it,⁸³ there is a risk that the decision of whether essential equivalence exists could be made on the basis of an insufficient evaluation of foreign law or on political pressures. Since intervention in references to the CJEU for a preliminary ruling is not possible,⁸⁴ there is no chance for third parties (such as foreign governments or academic experts) to intervene in such proceedings in order to provide further clarification on data protection standards in third countries.

There is thus a risk that determinations about essential equivalency may become another example of illusory protection. This makes it important in the future for third countries to monitor proceedings in national courts regarding the validity of adequacy decisions concerning them and attempt to intervene in such proceedings at the national level when possible, since all parties to the main proceedings at the national level may then participate in the procedure before the CJEU.⁸⁵ The CJEU could also consider ordering measures of inquiry (such as expert reports) pursuant to its Rules of Procedure,⁸⁶ which is permitted in a preliminary ruling on the validity of an EU act (for example, the European Data Protection Supervisor (EDPS) was invited to submit observations to the Court in the *Schrems* case based on this provision).

Perhaps too much attention has been given to the term “essentially equivalent” as used by the Court. The Court’s intention seems to have been to emphasize that the level of protection that third countries must meet must be high and come close to that under EU law, without being absolutely identical. This could well have been expressed in other terms with the same meaning, such as by saying that third countries “must meet a high standard of protection under the Charter” or something similar. Thus, parsing the linguistic meaning of the terms “essentially” and “equivalent” is less likely to lead to a meaningful understanding of the standard the Court requires than does examining the data protection standards required by the Charter and its interpretation by the CJEU in cases like *Digital Rights Ireland* and *Schrems*.

4. Coda: The EU-US Privacy Shield

On 2 February 2016, the EU and the US announced that they had agreed on the Privacy Shield as a replacement for the Safe Harbour,⁸⁷ and a draft adequacy decision, together with supporting documents, was published on 29 February. The documentation is voluminous (130 pages) and cannot be discussed in detail here, but the European Commission summarizes the Privacy Shield as comprising “strong obligations on companies and robust

⁸³ See Koen Lenaerts, Ignace Maselis, and Kathleen Gutman, *EU Procedural Law* (Oxford University Press 2014), at location 15562 (Kindle edition), noting that “under settled case-law, in the context of preliminary ruling proceedings, the Court of Justice is not entitled to rule on facts or points of national law, or to verify whether they are correct”.

⁸⁴ *Ibid.*, at location 23573 (Kindle edition).

⁸⁵ *Ibid.*

⁸⁶ *Ibid.*, at locations 19002-19015 (Kindle edition), noting that in such cases “it would be perfectly possible for measures of inquiry to be ordered pursuant to Art. 64(2) of the ECJ Rules of Procedure”. Article 64(2) foresees such measures as “the commissioning of an expert’s report”.

⁸⁷ See n 15.

enforcement”, “clear safeguards and transparency obligations on U.S. government access”, “effective protection of EU citizens’ rights with several redress possibilities”, and an “annual joint review mechanism”.⁸⁸

The Privacy Shield is much more detailed than the Safe Harbour, and includes stronger protections in certain areas.⁸⁹ In contrast with the Safe Harbour, it includes commitments from US national security officials concerning protections given to data from EU citizens, as well as letters and statements from other US government officials. Reflecting two years of negotiation,⁹⁰ the Privacy Shield represents a bold attempt to put transatlantic data transfers back on a solid legal footing.

At the same time, there are a number of questions that can be raised about it. Presumably because of political pressures to have it enacted quickly, there will apparently not be any assessment of the Privacy Shield by independent academic experts before the Commission proposes it for approval. The documentation that comprises the Privacy Shield is lengthy and structured in a haphazard way, making it difficult for individuals and small companies to interpret it. Many of the supporting letters from US officials are written in US legalese and will be difficult for many people in the EU to understand.

The way the Privacy Shield was drafted and presented demonstrates how regulation of international data transfers is dealt with in a predominantly untransparent and bureaucratic way. The *Schrems* judgment presented the ideal opportunity to reflect on the effectiveness and coherence of EU regulation of data transfers, and to hold an open discussion with experts and the public as to how it should be improved. Instead, the EU and the US intensified their secret negotiations on a successor to the Safe Harbour, and then revealed the final package while stressing the need to adopt it as quickly as possible.⁹¹

Several further steps are necessary before the Privacy Shield comes into force (i.e., approval by the Article 29 Working Party and the EU Member States), so it could be some time before the first data transfers are carried out under it. The Privacy Shield will also no doubt be the subject of legal challenges before the DPAs and, ultimately, before the CJEU, and will remain under a cloud until they are resolved. An as instrument of EU law, implementation of the Privacy Shield will have to meet strict standards of proportionality, legality, legitimate interest, and compliance with fundamental rights under the Charter.⁹²

The following are a few major legal questions that will have to be answered (most likely by

⁸⁸ European Commission, “Restoring trust in transatlantic data flows through strong safeguards: European Commission presents EU-U.S. Privacy Shield” (n 16).

⁸⁹ For example, with regard to onward transfers of personal data transferred to the US under the Shield. See U.S.-EU Privacy Shield Framework Principles Issued by the U.S. Department of Commerce (n 16), para. III, at 5-6.

⁹⁰ See Annex I, Letters from US Department of Commerce Secretary Penny Pritzker and US Under-Secretary for International Trade Stefan M. Selig (n 16), at 1, stating that the Privacy Shield is “the product of two years of productive discussions”.

⁹¹ See, e.g., Zoya Sheftalovich, “5 takeaways from the privacy shield”, politico.com, 29 February 2016, <<http://www.politico.eu/article/privacy-shield-agreement-takeaways-text-released/>>, stating that “the Council’s biggest concern is how quickly the new arrangement can be up and running”.

⁹² Lenaerts and Gutierrez-Fons (n 69), at location 50666 (Kindle edition).

the CJEU) if the Privacy Shield is not to suffer the same fate as the Safe Harbour:

--The CJEU in *Schrems* found that “legislation permitting the public authorities to have access on a generalised basis to the content of electronic communications must be regarded as compromising the essence of the fundamental right to respect for private life, as guaranteed by Article 7 of the Charter” (para. 94). Thus, under the Charter, such access is per se unlawful, without the need for a balancing test. The Privacy Shield presents a confusing picture with regard to its coverage of mass surveillance or the bulk collection of data by US intelligence or national security agencies. On the one hand, in the documentation the European Commission states that “The US assures there is no indiscriminate or mass surveillance on the personal data transferred to the US under the new arrangement”,⁹³ and the US notes that under US law, bulk collection of data or mass surveillance is “prohibited”.⁹⁴ On the other hand, the US also states in the documentation that “signals intelligence collected in bulk can only be used for six specific purposes”,⁹⁵ and that “any bulk collection activities regarding Internet communications that the U.S. Intelligence Community performs through signals intelligence operate on a small proportion of the Internet”,⁹⁶ suggesting that bulk collection does occur. The European Commission itself seems lukewarm about the degree of protection that the Privacy Shield provides with regard to US national intelligence activities: while the Commission’s draft adequacy decision states that the Privacy Shield principles issued by the US Department of Commerce as a whole ensure a level of protection of personal data that is “essentially equivalent” to that under EU law,⁹⁷ it refers to the protection granted by the Privacy Shield against interference by US law enforcement and other public authorities merely as “effective”.⁹⁸

--In *Schrems* the Court criticized the Safe Harbour for giving US law primacy over EU fundamental rights.⁹⁹ However, the obligations contained in the Privacy Shield are to be interpreted under US law,¹⁰⁰ and it provides broad derogations from its principles in situations when this is necessary “to meet national security, public interest or law enforcement requirements”,¹⁰¹ or in situations where US law may create conflicting

⁹³ EU-US Privacy Shield: Frequently Asked Questions (n 16), at 2.

⁹⁴ Annex VI, Letter from US General Counsel for the Office of the Director of National Intelligence Robert S. Litt (n 16), at 13, stating that the USA Freedom Act “prohibits bulk collection of any records, including of both U.S. and non-U.S. persons...”

⁹⁵ *Ibid.*, at 4.

⁹⁶ *Ibid.*

⁹⁷ Commission Implementing Decision of XXX pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of protection provided by the E.U.-U.S. Privacy Shield (n 16), at 29 (Recital 113).

⁹⁸ *Ibid.* at 28-29 (Recitals 111 and 116).

⁹⁹ See *Schrems* (n 3), para. 86, stating “Thus, Decision 2000/520 lays down that ‘national security, public interest, or law enforcement requirements’ have primacy over the safe harbour principles, primacy pursuant to which self-certified United States organisations receiving personal data from the European Union are bound to disregard those principles without limitation where they conflict with those requirements and therefore prove incompatible with them.”

¹⁰⁰ See U.S.-EU Privacy Shield Framework Principles Issued by the U.S. Department of Commerce (n 16), para. I(7), at 2. The emphasis on the primacy of US law is further emphasized by the fact that for arbitration proceedings under the Privacy Shield, it is stated that “arbitrators...must be admitted to practice law in the U.S. and be experts in U.S. privacy law, with expertise in EU data protection law” (Annex II, EU-U.S. Privacy Shield Framework Principles Issued by the U.S. Department of Commerce (n 16), at 33).

¹⁰¹ Commission Implementing Decision (n 16), para. 52; U.S.-EU Privacy Shield Framework Principles Issued by the U.S. Department of Commerce (n 16), at 2.

obligations.¹⁰² It also gives priority to freedom of expression under the First Amendment to the US Constitution over conflicting obligations, which may be interpreted to include the “right to be forgotten” that the CJEU recognized in *Google Spain*.¹⁰³ It could be difficult for the Court to tolerate giving US law priority over EU fundamental rights, particularly in light of its other judgments that emphasize the status of EU law as an autonomous legal system.¹⁰⁴

--Many of the guarantees in the Privacy Shield are based on assurances given in letters and other supporting documents from US officials, some of whom are political appointees. It seems that such assurances could be changed or revoked at will, and that many of these officials may change jobs or leave the government when the Obama Administration leaves office. While these documents are all to be published in the US Federal Register,¹⁰⁵ such publication merely “provides the public official notice of a document’s existence, specifies the legal authority of the agency to issue the document, and gives the document evidentiary status.”¹⁰⁶ The Charter requires that any limitation of fundamental rights must be “provided by law”,¹⁰⁷ which the Court has generally interpreted to mean a legal measure of the EU or of a Member State,¹⁰⁸ and which it requires to meet certain qualitative standards such as being clear, accessible, and foreseeable.¹⁰⁹ The question is whether the underlying assurances granted by US officials that constitute a key part of the guarantees to be included in the proposed Commission decision would fulfil the requirement of “provided by law” under the Charter.

--A new “Privacy Shield Ombudsman” function is to be created within the US Department of State, which is to be independent from the intelligence agencies and is supposed to follow up complaints and inquiries from individuals regarding intelligence surveillance. Questions can be raised as to whether the Ombudsman, who is a high official in the US Department of State,¹¹⁰ would fulfil the criteria set by the CJEU for an independent regulator. In particular, the Court has emphasized that data protection regulators must be independent from external influence (including that from inside the government), not just independent vis-à-vis the entity being regulated.¹¹¹ The European Ombudsman has already questioned whether this new function would actually be independent under internationally-recognized

¹⁰² U.S.-EU Privacy Shield Framework Principles Issued by the U.S. Department of Commerce (n 16), at 2, stating “Adherence to these Principles may be limited: ... (b) by statute, government regulation, or case law that creates conflicting obligations or explicit authorizations, provided that, in exercising any such authorization, an organization can demonstrate that its non-compliance with the Principles is limited to the extent necessary to meet the overriding legitimate interests furthered by such authorization”.

¹⁰³ *Ibid.*, para. III(2), at 8.

¹⁰⁴ See Opinion 2/13 of the Court, 18 December 2014, CLI:EU:C:2014:2454; Joined Cases C-402 & 415/05P, *Kadi & Al Barakaat Int'l Found. v. Council & Commission*, [2008] ECR I-6351.

¹⁰⁵ “EU-US Privacy Shield: Frequently Asked Questions” (n 16), at 2.

¹⁰⁶ Amy Bunk, “Federal Register 101”, <https://www.federalregister.gov/uploads/2011/01/fr_101.pdf>.

¹⁰⁷ Charter, Article 52(1).

¹⁰⁸ Steve Peers and Sacha Prechal, “Article 52—Scope and Interpretation of Rights and Principles”, in: Peers et al. (n 65), at para. 52.39 (Kindle edition),

¹⁰⁹ *Ibid.*, at para. 52.42. See in this regard *ibid.*, para. 52.44, and the Opinion of Advocate General Leger in Joined Cases C-317/04 and C-318/04 *European Parliament v. Council and Commission*, ECLI:EU:C:2005:710, paras. 216-221.

¹¹⁰ The Ombudsman is to be US Under Secretary of State Catherine Novelli. See Annex III, Letter from US Secretary of State John Kerry (n 16).

¹¹¹ *Commission v. Germany*, Case C-518/07, 9 March 2010, ECLI:EU:C:2010:125, para. 19. See Herke Kranenbourg, “Article 8—Protection of Personal Data”, in: Peers et al. (n 65), at para. 08.146.

standards for ombudsmen.¹¹²

--The Privacy Shield has a complex structure for resolution of complaints by individuals, which includes lodging a complaint with a member company; taking it to their national DPA; using an alternative dispute resolution mechanism; and, as a last resort, appealing to the “Privacy Shield Panel”, which seems to be a kind of arbitration body. Article 47 of the Charter requires that an individual whose rights are violated have an “effective remedy before a tribunal”, and in *Schrems* the CJEU held that “legislation not providing for any possibility for an individual to pursue legal remedies in order to have access to personal data relating to him, or to obtain the rectification or erasure of such data, does not respect the essence of the fundamental right to effective judicial protection, as enshrined in Article 47 of the Charter”.¹¹³ This suggests that the Court may take a dim view of complaint systems that do not involve a court, or those that place too much emphasis on dispute resolution by US entities not subject to control under EU law. On the other hand, the Court also found that “recourse by a third country to a system of self-certification is not in itself contrary to the requirement laid down in Article 25(6) of Directive 95/46 that the third country concerned must ensure an adequate level of protection”,¹¹⁴ suggesting that it may be willing to take a more flexible view.

IV. Effect on other data transfer mechanisms

A. Introduction

The rule of law requires the consistent application of legal rules to similar situations,¹¹⁵ and the CJEU strives to insure that its judgments enjoy legitimacy based on criteria such as coherency with existing case law, predictability, and avoidance of arbitrariness.¹¹⁶ It is therefore important to look beyond the Safe Harbour and investigate the implications of the *Schrems* judgment on the other mechanisms in the Directive that may be used to create a legal basis for data transfers.

The criticisms made of the Safe Harbour by the Court can be applied by analogy to the other legal bases for data transfer under the Directive, and thus raise questions about their continued viability. The broader applicability of the judgment will be demonstrated with regard to the three sets of legal bases for data transfers set forth in Articles 25 and 26 of the Directive, namely adequacy decisions issued by the European Commission (Article 25), derogations (Article 26(1)), and “adequate safeguards” (Article 26(2)).

B. Adequacy decisions of the Commission

¹¹² Letter of European Ombudsman Emily O’Reilly to European Commissioner Věra Jourová, 22 February 2016, <<http://www.ombudsman.europa.eu/resources/otherdocument.faces/en/64157/html.bookmark>>.

¹¹³ *Schrems* (n 3), para. 95.

¹¹⁴ *Ibid.* para. 81.

¹¹⁵ Gunnar Beck, *The Legal Reasoning of the Court of Justice of the EU* (Hart Publishing 2012), at 234 (Kindle edition).

¹¹⁶ See Koen Lenaerts, “How the ECJ Thinks: A Study on Judicial Legitimacy”, 36 *Fordham International Law Journal* 1302, 1306 (2013).

Article 25 of the Directive provides that transfers of personal data require that the third country provide an adequate level of data protection. The most prominent method of ensuring adequate protection is via a formal adequacy decision of the European Commission, of which the Safe Harbour was an example. The *Schrems* judgment is based on a strict interpretation of the standards of data protection in third countries, and on a strong emphasis on the protection of data protection rights when transferring data internationally.¹¹⁷ These criteria must be applied to other adequacy decisions as well, which raises questions about their continued viability.

In particular, the same points made by the Court concerning access to data by the US intelligence services could be raised concerning several other adequacy decisions. Two of the countries that participate in the international “Five Eyes”¹¹⁸ intelligence sharing network, which includes the United States, have also been found adequate by the Commission (i.e., Canada¹¹⁹ and New Zealand¹²⁰). The judgment in *Schrems* is based on findings of the Irish High Court that US surveillance programs revealed “the large scale collection and processing of personal data”,¹²¹ that there was a “significant over-reach’ on the part of the NSA and other federal agencies”,¹²² and that in the US there has been “indiscriminate surveillance and interception carried out by them on a large scale”.¹²³ In light of these findings, it seems that, at the least, explanation is required as to how countries that have deep and longstanding intelligence-sharing arrangements with the US can provide a level of data protection that is “essentially equivalent” to that under EU law.¹²⁴

The Privacy Shield forms the basis of a proposed adequacy decision of the Commission.¹²⁵ As explained above, the Shield presents a number of legal questions that will likely have to be answered eventually by the CJEU. Such a judgment of the Court would also provide clarification on the extent to which the factors discussed in *Schrems* would apply to adequacy decisions of other countries as well.

¹¹⁷ See, e.g., *Schrems* (n 3), para. 78 (stating “review of the requirements stemming from Article 25 of Directive 95/46, read in the light of the Charter, should be strict”).

¹¹⁸ See regarding the Five Eyes alliance (which comprises Australia, Canada, New Zealand, the UK, and the US) Greenwald (n 54), at locations 1581, 1854-1900 (Kindle edition).

¹¹⁹ See Commission Decision (EC) 2002/2 of 20 December 2001 pursuant to Directive (EC) 95/46 of the European Parliament and of the Council on the adequate protection of personal data provided by the Canadian Personal Information Protection and Electronic Documents Act, [2002] OJ L2/13; Commission Decision of 6 September 2005 on the adequate protection of personal data contained in the Passenger Name Record of air passengers transferred to the Canada Border Services Agency, [2005] OJ L91/49.

¹²⁰ Commission Implementing Decision of 19 December 2012 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data by New Zealand, [2013] OJ L28/12.

¹²¹ *Schrems* (n 3), para. 11.

¹²² *Ibid.*, para. 30.

¹²³ *Ibid.*, para. 31.

¹²⁴ This question could be asked of other countries that have been found by the Commission to provide adequate protection and that have strong national security states, for example Israel (European Commission, Commission Decision 2011/61/EU of 31 January 2011 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data by the State of Israel with regard to automated processing of personal data, [2011] OJ L27/39). See Greenwald (n 54), at location 1904 (Kindle edition), stating that “the NSA has a surveillance relationship with Israel that often entails cooperation as close as the Five Eyes partnership, if not sometimes even closer”.

¹²⁵ Commission Implementing Decision of XXX pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of protection provided by the E.U.-U.S. Privacy Shield (n 16).

C. Derogations

Article 26(1) of the Directive includes derogations for the restrictions on data transfers to third countries. These derogations apply in the following situations: “the data subject has given his consent unambiguously to the proposed transfer” (26(1)(a)); or “the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of precontractual measures taken in response to the data subject's request” (26(1)(b)); or “the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and a third party” (26(1)(c)); or “the transfer is necessary or legally required on important public interest grounds, or for the establishment, exercise or defence of legal claims” (26(1)(d)); or “the transfer is necessary in order to protect the vital interests of the data subject” (26(1)(e)); or “the transfer is made from a register which according to laws or regulations is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate legitimate interest, to the extent that the conditions laid down in law for consultation are fulfilled in the particular case” (26(1)(f)).

In its press release responding to the *Schrems* judgment, the European Commission noted that these derogations may still be used for data transfers,¹²⁶ which is correct in a formal legal sense, since they were not at issue in the judgment. However, the justification for relying on the derogations is undermined by the judgment.

By definition, the derogations are to be used in situations where there is no adequate level of data protection in the country to which the data are to be transferred,¹²⁷ and they must be applied narrowly.¹²⁸ The Article 29 Working Party has made it clear that in particular, consent cannot generally provide a long-term framework for “repeated or structural data transfers” (i.e., for repeated and large-scale transfers).¹²⁹ Thus, the derogations cannot fully replace the Safe Harbour as a means to conduct large-scale data transfers.

Moreover, since they are to be used in situations where no adequate data protection exists, use of the derogations does not address the issues with intelligence surveillance that caused the CJEU to invalidate the Safe Harbour. For example, it is self-evident that the fact that an individual has consented to a data transfer, or that the transfer is necessary to perform a contract, can provide no protection against data access by intelligence services. Therefore, while they remain valid in a formal legal sense, the derogations are subject to the same

¹²⁶ European Commission, “First Vice-President Timmermans and Commissioner Jourová’s press conference on Safe Harbour” (n 7).

¹²⁷ See Article 26(1) of the Directive (n 2), providing that the derogations provide a legal basis for data transfers to a third country “which does not ensure an adequate level of protection within the meaning of Article 25(2)...”

¹²⁸ See Article 29 Working Party, “Working Document: Transfers of personal data to third countries: Applying Articles 25 and 26 of the EU data protection directive” (WP 12, 24 July 1998), at 24, stating “These exemptions, which are tightly drawn, for the most part concern cases where risks to the data subject are relatively small or where other interests...override the data subject’s right to privacy. As exemptions from a general principle, they must be interpreted restrictively”.

¹²⁹ Article 29 Working Party, “Working document on a common interpretation of Article 26(1) of Directive 95/46/EC of 24 October 1995” (WP 114, 25 November 2005), at 11.

criticisms concerning intelligence surveillance that resulted in the invalidation of the Safe Harbour.

D. Adequate safeguards

The final possibility to provide a legal basis for data transfers is through the use of so-called “adequate safeguards”. Article 26(2) of the Directive provides that transfers may be carried out absent adequate protection in the third country to which data are transferred “where the controller adduces adequate safeguards with respect to the protection of the privacy and fundamental rights and freedoms of individuals and as regards the exercise of the corresponding rights; such safeguards may in particular result from appropriate contractual clauses”. In practice, two types of “adequate safeguards” are recognized, namely (1) contractual clauses, or (2) so-called binding corporate rules (BCRs). Contractual clauses are concluded between the data exporter in the EU and the party outside the EU to whom the data are sent, and contain obligations on each to provide certain protections to the data. They can either be “standard contractual clauses”, the text of which is standardized and adopted by a formal decision of the European Commission,¹³⁰ or “ad hoc” clauses that are drafted in each specific case and may need to be approved by the DPAs before use.¹³¹ Binding corporate rules are legally-binding internal codes that are adopted by a corporate group and approved by DPAs, and provide a legal framework for data transfers within the group.¹³²

As is the case with derogations under Article 26(1), adequate safeguards under Article 26(2) were not at issue in the *Schrems* case, so that in a formal legal sense they remain valid.¹³³ This is brought out in a Communication on the judgment issued by the European Commission in November 2015,¹³⁴ in which it emphasized that other data transfer mechanisms under the Directive may still be used, such as derogations (e.g., consent) under Article 26(1) of the Directive, and adequate safeguards (i.e., binding corporate rules or standard contractual clauses) under Article 26(2).

However, adequate safeguards suffer from the same defects as does the Safe Harbour with regard to intelligence surveillance by third countries. In the first place, it is clear that a contractual agreement between two private parties, or a binding set of data protection rules within a corporate group, can not legally restrain government intelligence activities of third countries. Moreover, in a practical sense, the powers of intelligence services to access data

¹³⁰ See European Commission, “Model contracts for the transfer of personal data to third countries”, <http://ec.europa.eu/justice/data-protection/international-transfers/transfer/index_en.htm>.

¹³¹ See regarding the use of contractual clauses to transfer data Christopher Kuner, *European Data Protection Law: Corporate Compliance and Regulation* (2nd ed. Oxford University Press, 2007), at 191-208.

¹³² See regarding BCRs Lokke Moerel, *Binding Corporate Rules: Corporate Self-Regulation of Global Data Transfers* (Oxford University Press 2012).

¹³³ This was mentioned in the Commission press release issued post-*Schrems*. See European Commission, “First Vice-President Timmermans and Commissioner Jourová’s press conference on Safe Harbour” (n 7).

¹³⁴ European Commission, “Communication from the Commission to the European Parliament and the Council on the Transfer of Personal Data from the EU to the United States of America under Directive 95/46/EC following the Judgment by the Court of Justice in Case C-362/14 (*Schrems*)”, COM(2015) 566 final, 6 November 2015.

far exceed any protections that can be granted by paper-based protections such as contracts or compliance policies.

In his submission to the CJEU, Schrems implied that use of the standard contractual clauses results in a higher level of protection than does the Safe Harbour, since transfers under the clauses are “under supervision by DPAs”.¹³⁵ However, not all Member States require that the standard clauses be filed with the DPAs.¹³⁶ Under the GDPR, the use of the standard clauses does not require DPA authorisation.¹³⁷ In addition, under the Directive, the DPAs’ statutory enforcement powers end at their national borders,¹³⁸ so there is no way for them to enforce EU law with regard to data processing by foreign intelligence services. While the standard contractual clauses do include provisions giving the DPAs rights with regard to data importers in third countries,¹³⁹ they cannot allow the DPAs to exercise their statutory powers in third countries, nor do they have any powers against public authorities in third countries (such as intelligence services). Thus, the argument that the use of adequate safeguards provides added protection because of DPA involvement is essentially a legal fiction. Schrems apparently has come to change his views about the standard clauses, since in December 2015 he filed complaints against Facebook with DPAs in Belgium, Germany, and Ireland that attacked the use by the company of contractual clauses to transfer personal data.¹⁴⁰ Some DPAs have also raised questions about the use of adequate safeguards in light of the *Schrems* judgment.¹⁴¹

Neither the standard clauses nor BCRs provide legal protection against data access by foreign law enforcement. The standard contractual clauses allow for suspension of data flows by the DPAs when “it is established that the law to which the data importer or a sub-processor is subject imposes upon him requirements to derogate from the applicable data protection law which go beyond the restrictions necessary in a democratic society as provided for in Article 13 of Directive 95/46/EC where those requirements are likely to have a substantial adverse effect on the guarantees provided by the applicable data protection

¹³⁵ See Maximilian Schrems v. Data Protection Commissioner, Written Submissions of Applicant, <http://www.europe-v-facebook.org/CJEU_subs.pdf>, at 24.

¹³⁶ See Article 29 Working Party, “Working Document Setting Forth a Co-Operation Procedure for Issuing Common Opinions on “Contractual clauses” Considered as compliant with the EC Model Clauses” (WP 226, 24 November 2014), at 2, <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp226_en.pdf>.

¹³⁷ See Article 42(2) of the GDPR version adopted by the Council and European Parliament on 15 December 2015 (n 21).

¹³⁸ EU Data Protection Directive (n 2), Article 28(6). See also *Weltimmo*, Case C-230/14, 1 October 2015, para. 60.

¹³⁹ E.g., Commission Decision (EC) 2010/87/EU of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive (EC) 95/46/EC of the European Parliament and of the Council, [2010] OJ L39/5, Clause 8, which gives DPAs the right to conduct an audit of the data importer.

¹⁴⁰ See <http://www.europe-v-facebook.org/EN/Complaints/PRISM_2_0/prism_2_0.html>.

¹⁴¹ See “ULD Position Paper on the Judgment of the Court of Justice of the European Union of 6 October 2015, C-362/14”, 14 October 2015, <https://www.datenschutzzentrum.de/uploads/internationales/20151014_ULD-PositionPapier-on-CJEU_EN.pdf>, at 4, in which the data protection authority of the German federal state of Schleswig-Holstein stated “In consistent application of the requirements explicated by the CJEU in its judgment, a data transfer on the basis of Standard Contractual Clauses to the US is no longer permitted.”

law and the standard contractual clauses”,¹⁴² and provide for notification of data access to the data exporter.¹⁴³ Binding corporate rules must contain a commitment that when a member of the corporate group has reason to believe that the law applicable to it prevents the company from fulfilling its obligations under the BCRs and has substantial effect on the guarantees provided by them, it will inform the EU headquarters or the EU member with delegated data protection responsibilities (except where prohibited by criminal law), and that when there is conflict between national law and the commitments in the BCR, the company must “take a responsible decision on what action to take” and consult the competent DPAs in case of doubt.¹⁴⁴ Informing other members of the company or the DPAs about conflicts with third country law can by itself provide no protection to data processing, and DPAs can take no action to do so besides blocking data transfers outside the EU, which does not provide effective protection on a large scale and raises legal issues of its own.

E. The GDPR

It seems that the GDPR will take effect some time in 2018, at which time it will replace the Directive. The question thus arises of what effect it will have on data transfers in light of the *Schrems* judgment.

The GDPR includes a much more detailed definition of what constitutes “adequacy” for data transfers to third countries, which incorporates the standards adopted by the CJEU in *Schrems*.¹⁴⁵ Thus, entry into force of the GDPR will not change the situation regarding the standards for adequacy that the Court adopted. The GDPR retains the three major grounds for data transfers under the Directive, namely adequacy decisions,¹⁴⁶ derogations,¹⁴⁷ and appropriate safeguards¹⁴⁸ (the new designation for “adequate safeguards” under Article 26 of the Directive). It makes a number of changes to the legal framework, including explicit recognition of binding corporate rules,¹⁴⁹ the possibility of transferring data on a limited basis based on a “compelling legitimate interest of the data controller”,¹⁵⁰ the possibility for EU law or Member State law to set limits for transfers of specific categories of personal data,¹⁵¹ and the potential use of codes of conduct to transfer personal data.¹⁵² There is also a new provision with rules regarding requests for disclosure of data by third country courts and administrative authorities.¹⁵³

¹⁴² See, e.g., Commission Decision (EC) 2010/87/EU of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors (n 139), Article 4(1).

¹⁴³ *Id.*, Clauses 5(b) and 5(d).

¹⁴⁴ See Article 29 Working Party, “Working Document setting up a framework for the structure of Binding Corporate Rules” (WP 154, 25 June 2008), at 8.

¹⁴⁵ Article 41 and Recitals 81 and 81b of the GDPR version adopted by the Council and European Parliament on 15 December 2015 (n 21).

¹⁴⁶ *Ibid.*, Article 41.

¹⁴⁷ *Ibid.*, Article 44.

¹⁴⁸ *Ibid.*, Article 42.

¹⁴⁹ *Ibid.*, Article 43.

¹⁵⁰ *Ibid.*, Article 44(1)(h).

¹⁵¹ *Ibid.*, Article 44(5)(a).

¹⁵² *Ibid.*, Article 38.

¹⁵³ *Ibid.* Article 43a, providing: “Any judgment of a court or tribunal and any decision of an administrative authority of a third country requiring a controller or processor to transfer or disclose personal data may only be recognised or enforceable in any manner if based on an international agreement, such as a mutual legal

None of the changes implemented by the GDPR affect the points made here concerning the consequences of the *Schrems* judgment for regulation of international data transfers. In addition, the GDPR incorporates the standards of the *Schrems* judgment. Thus, the arguments made here will remain relevant once the GDPR enters into force.

V. Reactions to the judgment

The predominant reactions to the *Schrems* judgment prior to the issuance have focused on what I will call formalism (of which the Privacy Shield proposal is another example) and data localization. As will be seen, neither of these is sufficient to provide real protection for international data transfers. This strengthens the conclusion that regulation of international data transfers under EU data protection law often represents illusion more than reality.

A. Formalism

A formalistic approach attempts to protect international data transfers through the implementation of procedural safeguards. Regulation of data transfers is filled with such safeguards, which include individuals clicking consent boxes on websites; signature of standard contractual clauses; formal approval of data transfers by DPAs; and formal determinations of the adequacy of third countries by the European Commission.

The Court in *Schrems* puts considerable emphasis on the fact that protections provided for data transferred from the EU to third countries must “prove, *in practice, effective* in order to ensure protection essentially equivalent to that guaranteed within the European Union” (emphasis added).¹⁵⁴ This reflects case law of the European Court of Human Rights, which requires that remedies for data protection violations be effective in practice as well as in law,¹⁵⁵ as well as similar statements by the Article 29 Working Party.¹⁵⁶ Individuals in the EU whose data are being transferred internationally are interested in ensuring that their rights are protected in practice, as is indicated by the widespread concern among Europeans about misuse of their data online.¹⁵⁷ Like any fundamental right, data protection cannot be reduced to a set of formalistic or bureaucratic procedures if it is to have any meaning.

Access to data transferred under Safe Harbour by the US intelligence services was one of the main factors in the Court’s judgment, as can be seen in its emphasis on the fact that the Safe

assistance treaty, in force between the requesting third country and the Union or a Member State, without prejudice to other grounds for transfer pursuant to this Chapter”.

¹⁵⁴ *Schrems* (n 3), para. 74. See also para. 39 (referring to the need for “effective and complete” protection), para. 41 (referring to the importance of ensuring the “effectiveness” of monitoring of compliance with the law by DPAs), and paras. 81, 89, 91, and 95 (in which the Court stresses the need for protection of the fundamental right to data protection to be “effective”).

¹⁵⁵ See, e.g., *Rotaru v Romania* (2000) ECHR 191, at para. 67.

¹⁵⁶ Article 29 Working Party, “Working Document: Transfers of personal data to third countries: Applying Articles 25 and 26 of the EU data protection directive” (WP 12, 24 July 1998), at 5, stating that “data protection rules only contribute to the protection of individuals if they are followed in practice”.

¹⁵⁷ See Special Eurobarometer 431, Data Protection, June 2015, <http://ec.europa.eu/public_opinion/archives/ebs/ebs_431_sum_en.pdf>, at 25.

Harbour principles can be limited by national security or law enforcement requirements,¹⁵⁸ the lack of limits mentioned in the Safe Harbour on data use under US law for national security purposes,¹⁵⁹ and the failure in the Safe Harbour to mention any legal protection dealing with US intelligence surveillance.¹⁶⁰ In light of this, one can only conclude that the judgment requires meaningful and effective protection against intelligence surveillance by third countries. However, it is self-evident that procedures such as checking consent boxes on online forms, signing contractual clauses, or having binding corporate rules approved by DPAs cannot restrain data access by foreign intelligence services. At a legal level, such third country agencies are not constrained by EU law, and at a practical level their capabilities are not in any way hindered by such procedural mechanisms.

EU data protection law is partially based on legal fictions. Thus, Member States are required to consider all other Member States as complying with fundamental rights law, and may not check whether they do so in a specific case, based on the principle of mutual trust under EU law.¹⁶¹ A concrete application of this principle can be seen in Article 1 of the Directive, which provides that Member States may not restrict data transfers to other Member States based on the level of data protection they provide, so that, legally speaking, all Member States are presumed to offer an adequate level of data protection.¹⁶² This situation has been affirmed by the CJEU, which has ruled several times that harmonisation of national data protection laws in the Member States is “generally complete”.¹⁶³

At the same time, in announcing its legislative reform package for data protection in 2012, the European Commission stated that existing rules do not provide the degree of harmonization required, and that in particular there is a substantial lack of harmonisation in important areas.¹⁶⁴ The EU Fundamental Rights Agency has also found substantial divergences in the powers of national DPAs.¹⁶⁵ The principle that data protection standards are uniform among the Member States is thus a legal fiction, and there is a gulf between the presumption of harmonisation among Member State laws and the reality on the ground. Of course, data protection law, like any form of law, must to some extent rely on formalistic procedures, which further important values such as predictability and impartiality of the law. The problem arises when formalism becomes an end in itself, which is particularly inappropriate when fundamental rights are at stake.

The proposed Privacy Shield is another example of formalistic responses to regulation of international data transfers. The procedure for approval of adequacy decisions by the

¹⁵⁸ *Schrems* (n 3), paras. 84-86.

¹⁵⁹ *Ibid.*, para. 88.

¹⁶⁰ *Ibid.*, para. 89.

¹⁶¹ Opinion 2/13 of the Court, 18 December 2014, CLI:EU:C:2014:2454, para. 192.

¹⁶² EU Data Protection Directive (n 2), Article 1, stating “Member States shall neither restrict nor prohibit the free flow of personal data between Member States for reasons connected with the protection afforded under paragraph 1.”

¹⁶³ *Bodil Lindqvist*, Case C-101/01, [2003] ECR I-12971, at para. 96, stating “The harmonisation of those national laws...amounts to harmonisation which is generally complete”; *ASNEF*, Joined Cases C-468/10 and C-469/10, [2011] ECR I-12181, at para. 29, stating “Accordingly, it has been held that the harmonisation of those national laws is not limited to minimal harmonisation but amounts to harmonisation which is generally complete.”

¹⁶⁴ European Commission, “Safeguarding Privacy in a Connected World” (n 20), at 4-7.

¹⁶⁵ See European Union Agency for Fundamental Rights (n 43).

European Commission under the Directive has been criticized as inefficient,¹⁶⁶ untransparent,¹⁶⁷ and subject to influence based on political factors.¹⁶⁸ The ground-breaking *Schrems* judgment provided the opportunity for the EU to re-think its approach to reaching adequacy determinations, and to consider what mechanisms could actually lead to data protection in the real world of international data transfers, but instead it moved to negotiate an adequacy decision with little transparency or chance for public input. The result is a massive package that will be difficult for individuals or smaller companies to implement or even understand.

B. Data localization

The second response to *Schrems* has been based on what can be referred to as data localization, which includes measures or policies to encourage or require the storage of personal data inside the borders of the EU, so that there is no need for data transfers.¹⁶⁹ Incentives have been proposed to store the data of European companies on servers located within the EU,¹⁷⁰ and, as the European Commission noted in its Communication following the judgment,¹⁷¹ a number of US-based companies have announced plans to store data in Europe.¹⁷²

Locating data storage in a particular place is normally a decision made on business and technical considerations. However, following the *Schrems* judgment, it is important to investigate whether data localization in Europe can provide effective protection against data access by the intelligence services; the answer seems to be “no”.

¹⁶⁶ See regarding problems with the EU system for reaching adequacy determinations Article 29 Working Party, “The Future of Privacy” (WP 168, 1 December 2009), at 10-11, stating that the process for reaching adequacy decisions should be “redesigned”.

¹⁶⁷ See Kuner, *Transborder Data Flows and Data Privacy Law* (n 38), at 48.

¹⁶⁸ For example, in July 2010 the government of Ireland delayed an EU adequacy decision for Israel based on alleged Israeli government involvement in the forging of Irish passports. See “Ireland blocks EU data sharing with Israel”, 8 July 2010, <<http://jta.org/news/article/2010/07/08/2739965/ireland-backs-out-of-data-sharing-with-israel>>. Israel later received an adequacy decision from the European Commission; see Commission Decision 2011/61/EU of 31 January 2011 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data by the State of Israel with regard to automated processing of personal data, [2011] OJ L27/39. Also, a failed bid for adequacy by Australia in the early 2000s caused tensions between that country and the EU.

¹⁶⁹ See generally regarding data localization Anupam Chander and Uyê P. Lê, “Data nationalism”, 64 *Emory Law Journal* 677 (2015); Christopher Kuner, “Data nationalism and its discontents”, 64 *Emory Law Journal Online* 2089 (2015), <http://law.emory.edu/elj/_documents/volumes/64/online/kuner.pdf>

¹⁷⁰ See “Atos CEO calls for ‘Schengen for data’”, <<http://www.thierry-breton.com/lire-lactualite-media-41/items/atos-ceo-calls-for-schengen-for-data.html>>; “Ein Internet nur für Deutschland”, *Frankfurter Allgemeine Zeitung*, 10 November 2013, <<http://www.faz.net/aktuell/wirtschaft/netzwirtschaft/plaene-der-telekom-ein-internet-nur-fuer-deutschland-12657090.html>>.

¹⁷¹ European Commission, “Communication from the Commission to the European Parliament and the Council on the Transfer of Personal Data from the EU to the United States of America” (n 134), at 12.

¹⁷² See, e.g., Murad Ahmed and Richard Waters, “Microsoft unveils German data plan to tackle US Internet spying”, *Financial Times*, 11 November 2015, <<http://www.ft.com/intl/cms/s/0/540a296e-87ff-11e5-9f8c-a8d619fa707c.html#axzz3vvmkIE7x>>; Karlin Lillington, “Oracle keeps European data within its EU-based data centres”, *Irish Times*, 28 October 2015, <<http://www.irishtimes.com/business/technology/oracle-keeps-european-data-within-its-eu-based-data-centres-1.2408505?mode=print&ot=example.AjaxPageLayout.ot>>.

It is obvious that not all data processing services can be located in the EU. Thus, expecting data processing to be located in the EU in order to avoid data transfers to third countries may help in isolated cases, but cannot be a large-scale solution. From the popularity of Internet services,¹⁷³ it seems clear that Europeans want to use such services and communicate with parties in third countries.

There are also legal limits to creating incentives or requirements to locate data processing in a particular place. Under both EU and international human rights law, individuals have a right to communicate and transfer data “regardless of frontiers”,¹⁷⁴ suggesting that the ability to communicate across national borders is a necessary component of the right to freedom of expression.¹⁷⁵ The exact meaning of the phrase “regardless of frontiers” with regard to freedom of expression in international human rights instruments remains unclear, as it never seems to have been specifically clarified by UN human rights agencies or the European Court of Human Rights.¹⁷⁶ A logical interpretation of the phrase would seem to be that the right to communicate across borders is subject to the same conditions and restrictions as other components of the right to freedom of expression. For example, in General Comment No. 34, the UN Human Rights Committee has taken a restrictive view of the possibility for states to put conditions on freedom of expression online, noting that they can only be imposed insofar as they are compatible with paragraph 19(3) of the ICCRP.¹⁷⁷ Given that communication on the Internet has an inherent cross-border element, it would seem that this view of the Human Rights Committee has particular relevance to any restrictions placed on the right to communicate across borders. That is, such restrictions may be permissible, but only as provided for by law and in order to protect important public values.

It is also not clear how much protection in practice data localization can provide against access by intelligence agencies. Storing data on computers physically located in the EU Member States will remove them from the direct enforcement jurisdiction of third countries, since under international law public authorities may generally not enforce laws abroad without the consent of the relevant country.¹⁷⁸ It may also be easier for EU individuals to

¹⁷³ For example, as of June 2015, 57% of Europeans use an online social network at least once a week, and 53% use instant messaging or chat websites. See Special Eurobarometer 431, Data Protection, June 2015, <http://ec.europa.eu/public_opinion/archives/ebs/ebs_431_sum_en.pdf>, at 24.

¹⁷⁴ See Universal Declaration of Human Rights (1948), Article 19; International Covenant of Civil and Political Rights (ICCRP) (1966), Article 19(2); European Convention on Human Rights (1953), Article 10(1).

¹⁷⁵ In each of the three human rights conventions referred to above in n 174, the phrase “regardless of frontiers” is mentioned in the article dealing with freedom of opinion and of expression (i.e., in the articles cited therein).

¹⁷⁶ See, e.g., UN Human Rights Committee, “General Comment No. 34”, UN Doc. CCPR/C/GC/34, 12 September 2011, which mentions once the phrase “regardless of frontiers” but offers no interpretation of what it means; Lorna Woods, “Article 11”, in: Peers (et al.) (n 69), at 314, noting that there have been no cases brought as of yet regarding the territorial scope of the right to freedom of expression under Article 11 of the European Convention on Human Rights.

¹⁷⁷ General Comment No. 34 (n 176), para. 43. Article 19(3) of the ICCRP provides that the right to freedom of expression (including that across borders) may be subject to restrictions only as “provided by law and are necessary: (a) For respect of the rights or reputations of others; (b) For the protection of national security or of public order (ordre public), or of public health or morals”.

¹⁷⁸ See, e.g., Ian Brownlie, *Principles of Public International Law* (7th ed Oxford University Press 2008), at 309, stating “the governing principle is that a state cannot take measures on the territory of another state by way of enforcement of national laws without the consent of the latter”; F A Mann, ‘The Doctrine of Jurisdiction in

assert their data protection rights with regard to data stored in EU Member States, since EU law provides individuals and regulators with a framework that allows the assertion of rights between the Member States.¹⁷⁹ Some companies have begun constructing services that purport to provide stronger protection against data access based on the localization of data storage within the EU, though the efficacy of such claims remains untested.¹⁸⁰

However, as the Snowden revelations have shown, there seems to be widespread data sharing going on between EU intelligence services and those of third countries, in particular the US services and those of the “Five Eyes” intelligence sharing network.¹⁸¹ It seems that the cooperation between the US National Security Agency (NSA) and the UK signals intelligence service Government Communication Headquarters (GCHQ) is particularly close.¹⁸²

Thus, there is strong evidence to suggest that data sharing is being conducted on a broad scale between intelligence agencies in many countries, and that once data are accessed by one agency, they may be made available to those in other countries, so that the place of the computer where data are stored may be largely irrelevant to whether it may be accessed by the intelligence services. It is also not clear that the place of data storage affects the technical capabilities of intelligence services of third countries to access data stored in the EU, given the globally-networked nature of data processing. The factual record concerning data sharing between intelligence agencies is unclear and subject to controversy, so that it is difficult to know exactly how and to what extent data are being shared between particular agencies. But the available evidence gives reason to doubt that the place of data storage has a strong influence on the level of protection it receives in practice.

International Law’ (1964) 111 *Recueil des Cours de l’Académie de Droit International* 9, reprinted in F A Mann, *Studies in International Law* (Clarendon Press Oxford 2008) , at 145-146.

¹⁷⁹ See, e.g., EU Data Protection Directive (n 2), Article 28(6), which obliges EU data protection authorities to cooperate with each other; Council Regulation (EC) 44/2001 of 22 December 2000 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters, [2001] OJ L12/1, which allows court decisions from one EU Member State to be enforced in another Member State.

¹⁸⁰ See, e.g., Murad and Waters (n 172), regarding a plan by Microsoft to allow customers to store their data in Germany under facilities that are under the control of Deutsche Telekom, in order to protect them from legal access by US law enforcement authorities.

¹⁸¹ See, e.g., Greenwald (n 54), at locations 1852-1926 (Kindle edition), stating that there is a wide-ranging intelligence sharing network between US intelligence agencies such as the National Security Agency (NSA) and those of other countries, including both the Five Eyes countries and others such as Israel; SPIEGEL Online, “Spying Close to Home: German Intelligence under Fire for NSA Cooperation”, 24 April 2015, <<http://www.spiegel.de/international/germany/german-intelligence-agency-bnd-under-fire-for-nsa-cooperation-a-1030593.html>>, criticizing cooperation between the German intelligence services and those of the US; Julian Border, “GCHQ and European spy agencies worked together on mass surveillance”, *The Guardian*, 1 November 2013, <<http://www.theguardian.com/uk-news/2013/nov/01/gchq-europe-spy-agencies-mass-surveillance-snowden>>, alleging close cooperation between the British, French, German, Spanish, and Swedish intelligence agencies.

¹⁸² Greenwald (n 181), at location 1857 (Kindle edition), stating that the GCHQ is the “closest NSA ally”. See also Marko Milanovic, “Human Rights Treaties and Foreign Surveillance: Privacy in the Digital Age”, 56 *Harvard International Law Review* 81, 126 (2015).

Specifically with regard to the US, certain constitutional protections do not apply to non-US individuals abroad,¹⁸³ so that moving data processing to the EU does not necessarily create extra protection under US law. US courts have also ruled that companies can be compelled to comply with orders from US authorities no matter where in the world the data are stored;¹⁸⁴ this issue is currently the subject of a legal challenge in the US courts involving a warrant issued by the US to access data held by Microsoft at its servers in Ireland.¹⁸⁵

VI. Conclusions

A. Reality and illusion in data transfer regulation

The *Schrems* judgment demonstrates both the reality and the illusion of EU regulation of international data transfers. The Court's strong affirmation of data protection rights clarifies the application of the Charter to data transfers, and thus continues the reality of legal protections for data protection rights that were advanced in *Digital Rights Ireland* and other judgments.

At the same time, it shows how EU law maintains the "exalting illusion" of global protection of data transfers based on EU standards. The points upon which the Court relied to invalidate the Safe Harbour can be applied to other legal mechanisms for data transfers under the Directive as well, and the system the judgment sets up for having adequacy decisions evaluated at the national level will not be workable in practice. While it seems clear that the Charter provides the measure of adequate protection for data transfers in most cases, the exemption of national security from EU competence may lead to gaps in protection. The judgment thus lays bare the internal contradictions of the regulation of data transfers under EU law, and shows how the unilateral application of EU law cannot provide effective protection in practice for data transfers to third countries.

B. The politics of international data transfers

¹⁸³ For example, the warrant clause of the Fourth Amendment. See *United States v. Verdugo-Urquidez*, 494 US 259, 271 (1990). See also Kai Raustiala, *Does the Constitution Follow the Flag?* (Oxford University Press 2011); José A. Cabranes, "Our Imperial Criminal Procedure: Problems in the Extraterritorial Application of US Constitutional Law", 118 *Yale Law Journal* 1660 (2009).

¹⁸⁴ See, e.g., *In re Grand Jury Proceedings (Bank of Nova Scotia)*, 740 F.2d 817 (11th Cir. 1984) (affirming sanctions against the defendant for refusing to produce documents held abroad in response to a grand jury subpoena); *In re Marc Rich & Co., A.G.*, 707 F.2d 663 (2d Cir. 1983) (affirming a grand jury subpoena ordering the defendant to produce records held in Switzerland); *United States v. Vetco, Inc.*, 691 F.2d 1281 (9th Cir. 1981) (affirming a summons from the Internal Revenue Service to produce tax records held in Switzerland); *United States v. Chase Manhattan Bank, N.A.*, 584 F. Supp. 1080 (S.D.N.Y. 1984) (granting a motion to force the defendant to produce records held in Hong Kong).

¹⁸⁵ *In the matter of a warrant to search a certain e-mail account controlled and maintained by Microsoft Corporation*, Memorandum and Order 13 Mag. 2814 (S.D.N.Y., US Magistrate Judge James C. Francis IV), 25 April 2014. At the time this article was written, the case was being appealed to the US Court of Appeals for the Second Circuit. See *Microsoft Corporation v. United States of America*, Case 14-2985-CV (Second Circuit). See regarding the case Ned Schultheis, "Warrants in the Clouds: How Extraterritorial Application of the Stored Communications Act Threatens the United States' Cloud Storage Industry", 9 *Brooklyn Journal of Corporate, Financial and Commercial Law* 661 (2014-2015); Case Note, "In re Warrant to Search a Certain Email Account Controlled & Maintained by Microsoft Corp.", 15 *F Supp. 3d* 466 (S.D.N.Y. 2014)", 128 *Harvard Law Review* 1019 (2014-2015).

One reason that regulation of international data transfers often provides only the illusion of protection is that the legal arguments made are only reflections of deep-seated political positions. This can be seen particularly in the EU-US relationship, where the legal positions of each side are determined by their underlying political beliefs.

Parties in the EU want to have the US adopt an EU-style data protection framework¹⁸⁶ and to change its law.¹⁸⁷ For its part, the US side would like the EU to make it easier to transfer personal data internationally, both to further economic growth¹⁸⁸ and for reasons of US national security.¹⁸⁹ This has produced resentment in the EU about the extent of US lobbying on data protection,¹⁹⁰ and in the US about the EU trying to have it change its law.¹⁹¹ The political nature of the transatlantic disagreement is shown by the fact that the EU-US Privacy Shield was only finalised by a last-minute agreement at the highest political level on a call between European Commission First Vice-President Frans Timmermans and US Vice-President John Kerry.¹⁹²

Transatlantic political disagreements about data protection rights are to be expected, since “rights to do not exist as such—‘fact-like’—outside the structures of political deliberation. They are not a limit but an effect of politics”.¹⁹³ Legal disagreements that are essentially political arguments in disguise cannot provide a solution to clashes between different conceptions of data protection and privacy, since they are determined, as Koskineemi states,

¹⁸⁶ See, e.g., Press Release of the Transatlantic Consumer Dialogue (TACD), <<http://tacd.org/wp-content/uploads/2015/10/TACD-Statement-in-response-to-the-European-Court-of-Justice-ruling-on-Safe-Harbor-agreement-.pdf>>, stating that “It is also more than high time for the United States to enact a comprehensive set of data protection rules, to bring it in line with 100 plus other countries round the world”. The TACD includes dozens of consumer organizations in both the EU and the US, with the majority being European.

¹⁸⁷ See “Commissioner Jourová’s remarks on Safe Harbour EU Court of Justice judgement before the Committee on Civil Liberties, Justice and Home Affairs (Libe)”, 26 October 2015, <http://europa.eu/rapid/press-release_SPEECH-15-5916_en.htm>, in which EU Commissioner Jourová urged the US to pass the proposed Judicial Redress Act, which would grant enhanced rights to EU individuals to bring privacy-related claims in the US. The Act was signed into law by President Obama on 24 February 2016 (n 18).

¹⁸⁸ See, e.g., Robert D. Atkinson, “Don’t just fix Safe Harbour, fix the data protection regulation”, EurActiv, 18 December 2015, <<http://www.euractiv.com/sections/digital/dont-just-fix-safe-harbour-fix-data-protection-regulation-320567>>, in which the president of a Washington-based think-tank urges reform of EU data protection law in order to facilitate data flows.

¹⁸⁹ See, e.g., Stewart Baker, “Time to get serious about Europe’s sabotage of US terror intelligence programs”, Washington Post, 5 January 2016, <<https://www.washingtonpost.com/news/volokh-conspiracy/wp/2016/01/05/time-to-get-serious-about-europes-sabotage-of-us-terror-intelligence-programs/>>.

¹⁹⁰ See, e.g., April Dembosky and James Fontanella-Kahn, “US tech groups criticized for EU lobbying”, Financial Times, 4 February 2013, <<http://www.ft.com/intl/cms/s/0/e29a717e-6df0-11e2-983d-00144feab49a.html#axzz40hMUmieK>>; “Francesco Guarascio, “US lobbying waters down EU data protection reform”, euractiv.com, 21 February 2012, <<http://www.euractiv.com/section/digital/news/us-lobbying-waters-down-eu-data-protection-reform/>>.

¹⁹¹ See, e.g., Katie Bo Williams, “Last-minute change to privacy bill adds tension to US-EU talks”, The Hill, 28 January 2016, <<http://thehill.com/policy/cybersecurity/267401-last-minute-change-to-privacy-bill-adds-tension-to-us-eu-negotiations>>, quoting Member of the US House of Representatives John Cornyn as stating with regard to adoption by the US of the proposed Judicial Redress Act, which would give rights under the US Privacy Act to Europeans, “U.S. companies should not have to endure regulatory threats in an attempt to change our policy or laws”. The Act was signed into law by President Obama on 24 February 2016 (n 18).

¹⁹² Zoya Sheftalovich, “The phone call that saved safe harbor”, Politico, 13 February 2016, <<http://www.politico.eu/article/the-phone-call-that-saved-safe-harbor-john-kerry-frans-timmermans/>>.

¹⁹³ Martti Koskineemi, *The Politics of International Law* (Hart 2011), at location 4421 (Kindle edition).

“by policy choices that seem justifiable only by reference to alternative conceptions of the good society”.¹⁹⁴ Neither the EU nor the US positions can be separated from their political priorities, and arguments about issues such as where to set the balance between protecting data transferred internationally and furthering economic growth and national security only lead back to the policy assumptions that underlie each position.¹⁹⁵ This is why transatlantic arguments about regulation of international data transfers tend to go around in circles, with each side justifying its own position based on its own legal framework, without realizing that there can be no legal solution short of one side adopting the other’s framework.

C. The way forward

Former European Data Protection Supervisor Peter Hustinx has written that the standards for international data transfers under the Directive are “based on a reasonable degree of pragmatism in order to allow interaction with other parts of the world”.¹⁹⁶ But the *Schrems* judgment shows how EU data protection law leaves narrow room for accommodation with the data protection systems of third countries. EU law does not view data transfer regulation as a way to reach a reasonable accommodation between EU standards and those of other countries, but focuses on a unilateral assertion of EU values. It is thus unrealistic to imagine that there could be a single, overarching “solution” to disputes between the EU and third countries regarding the regulation of international data transfers such as were the issue in *Schrems*.

However, while legal instruments cannot provide a full solution, they may serve as a “gentle civilizer of social systems”,¹⁹⁷ based on finding lines of compatibility and communication between different data protection systems. Protecting international data transfers is unlikely to be possible under rigid, formalistic mechanisms that are based on strict criteria under national or regional law (such as EU formal adequacy decisions issued by the European Commission or the signing of standard contractual clauses), or by measures of pure formalism that cannot provide real protection in practice (such as the use of consent clauses).

If one believes that EU data protection law cannot and should not shut itself off from other legal systems, and that EU individuals want to be able to communicate internationally, then it is necessary to find a way to reach some kind of accommodation between EU data protection law and legal regimes in other regions. Regulation of international data transfers is marked by legal pluralism and fragmentation,¹⁹⁸ and scholarly consideration of ways to

¹⁹⁴ *Ibid.*, at location 3995 (Kindle edition). See also J.H.H. Weiler, “Fundamental Rights and Fundamental Boundaries: On the Conflict of Standards and Values in the Protection of Human Rights in the European Legal Space”, in: J.H.H. Weiler, *The Constitution of Europe* (Cambridge University Press 1999), 102, 106, stating that “Human rights are almost invariably the expression of a compromise between competing social goods in the polity”.

¹⁹⁵ See Koskeniemi (n 193), at location 3939 (Kindle edition).

¹⁹⁶ Peter Hustinx, “EU Data Protection Law: The Review of Directive 95/46/EC and the Proposed General Data Protection Regulation”, https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Speeches/2014/14-09-15_Article_EUI_EN.pdf

¹⁹⁷ Andreas Fischer-Lescano and Gunther Teubner, “Regime-Collisions: the Vain Search for Legal Unity in the Fragmentation of Global Law”, 25 *Michigan Journal of International Law* 999, 1045 (2003).

¹⁹⁸ Kuner, *Transborder Data Flows and Data Privacy Law* (n 38), at 160-165.

manage these phenomena could be applied to data protection as well.¹⁹⁹ The Privacy Shield is an example of an attempt to build bridges between different legal systems of data protection that, if it is adopted and not subject to a successful legal challenge, could prove to be an innovative solution that may have significance for data flows from the EU to other regions as well. However, the EU needs to modernize and open up its working methods to allow such schemes to be commented on in public while they are being devised, rather than being negotiated in secret with third countries and then adopted hurriedly without proper debate.

The fact that the perspective one takes on many of the privacy disagreements between the EU and the US determines the amount of difference between them gives hope that they may be less intractable than they seem. For example, at first glance there is considerable difference between the EU position that fundamental rights apply to all human beings, and the fact that US constitutional protections do not apply to the activities of its intelligence services operating abroad.²⁰⁰ However, viewed at a broader comparative level, it turns out that French constitutional protections also do not apply to the activities abroad of national intelligence services,²⁰¹ and that this may be the case under German law as well.²⁰² Historians of human rights such as Mony have also shown how until fairly recently even in European polities there was an “umbilical connection between rights and citizenship”.²⁰³ This illustrates how many questions of fundamental rights protection depend on the perspective of the observer: if one is determined to find differences and disagreements between the EU and the US, then it is easy to do so, while if one wants to find possibilities for agreement, then they can also be found.

Three points are crucial to a workable system of data transfer regulation in EU law. First, the EU must move beyond formalistic and political measures and legal fictions to implement

¹⁹⁹ See, e.g., Paul Schiff Berman, *Global Legal Pluralism* 152 (Cambridge University Press 2014), who mentions as possible mechanisms “dialectical legal interactions, margins of appreciation, limited autonomy regimes, subsidiarity schemes, hybrid participation arrangements, mutual recognition regimes, safe harbor agreements, and regime interaction”.

²⁰⁰ See on this point Christopher Kuner, “Foreign Nationals and Data Protection Law: A Transatlantic Analysis”, in: *Data Protection 2014: How to Restore Trust* 213 (Hielke Hijmans and Herke Kranenbourg eds.) (intersentia 2014)

²⁰¹ Assemblée Nationale, “Rapport d’information déposé en application de l’article 145 du Règlement par la commission des Lois constitutionnelles, de la législation et de l’administration générale de la République, en conclusion des travaux d’une mission d’information sur l’évaluation du cadre juridique applicable aux services de renseignement”, 14 May 2013, at <<http://www.assemblee-nationale.fr/14/pdf/rap-info/i1022.pdf>>. See also Winston Maxwell, “The legal framework for access to data by French law enforcement and intelligence agencies”, (2014) 4 *International Data Privacy Law* 4, at 9, noting that, according to French newspaper reports, “France’s intelligence agencies take the position that their collection of data outside of France does not fall under French legal constraint”.

²⁰² Compare Bethold Huber, “Die Strategische Rasterfahndung des Bundesnachrichtendienstes – Eingriffsbefugnisse und Regelungsdefizite”, (2013) 35 *Neue Juristische Wochenschrift* 2576, who finds that in theory the Basic Law does apply in such situations but criticizes the failure to implement such protections in legislation governing the intelligence services, with an interview with Prof. Dr. Christoph Gusy (“Die BND-Auslandsaufklärung im rechtsfreien Raum”, 2 September 2013, <<http://www.golem.de/news/datenueberwachung-die-bnd-auslandsaufklaerung-im-rechtsfreien-raum-1309-101324.html>>), who states that surveillance of non-Germans outside Germany by the intelligence services is not covered by the Basic Law.

²⁰³ Samuel Mony, *The Last Utopia: Human Rights in History* (Harvard University Press 2010), location 444 (Kindle edition).

actual protection in practice. Second, it must discard illusions, such as the idea that DPAs and national courts can perform meaningful assessments of the adequacy of non-EU data protection systems. Third, data protection law cannot by itself resolve issues relating to surveillance for national security or intelligence-gathering purposes, which will require further reform and transparency regarding intelligence-gathering practices. In particular, it is necessary for the Court or the EU legislator to clarify the application of data protection rights under the Charter to situations involving national security, in order to remove any gaps in protection.

The *Schrems* judgment forces us to look at the contradictions of EU data transfer regulation squarely in the face. It is no longer possible to ignore the legal and logical incoherency of EU data transfer regulation, or to pretend that they can be cured by formalistic measures. Perhaps the common deficiencies in the legal systems of data protection in both sides of the transatlantic debate can provide common ground to overcome the illusions of the current data protection debate, and to bring the discussion back to reality.



EUROPEAN COMMISSION
DIRECTORATE-GENERAL JUSTICE AND CONSUMERS

Director-General

Brussels, 11/03/2016
DG JUST/TA/Ares(2016)1305722

Mr. Giovanni Butarelli
European Data Protection
Supervisor
Rue Montoyer 30
Brussels

Dear Mr Butarelli,

I hereby wish to send to you the draft adequacy decision on the EU – U.S. Privacy Shield, as well as a new Commission Communication on "*Transatlantic Data Flows: Restoring Trust through Strong Safeguards*".

The enclosed package includes all the documents from the United States government pertaining to the new arrangement. They contain the binding commitments, representations and assurances, which, together with the overall U.S. legal framework, allow the Commission to propose an adequacy decision regarding the EU-US Privacy Shield.

The draft decision is being sent to the Article 29 Working Party for its opinion pursuant to Article 30(1)(b) of Directive 95/46/EC.

We would like to consult you on this draft decision and look forward to receiving your opinion. The draft decision would then go through the comitology procedure before it can be adopted by the European Commission, as an implementing measure, under Directive 95/46/EC.

The Commission Communication takes stock of how far we have come in fulfilling the objectives formulated in our Communication of November 2013¹. We have made significant improvements in the protection of personal data of EU citizens, through the conclusion of the EU data protection reform as well as the draft agreements with the US. In particular, we have achieved an important change in the U.S. legislation by the adoption of the Judicial Redress Act, which was signed into law by President Obama on 24th of February. The effective enjoyment of these rights by Europeans is subject to the ratification by the EU of the EU-U.S. "Umbrella" Agreement.

¹ Communication from the Commission to the European Parliament and the Council: Rebuilding Trust in EU-US Data Flows, COM(2013) 846final of 27.11.2013.

As this is an international agreement, the Commission will soon propose to the Council to adopt the decision enabling the signature of the agreement. Thereafter, the agreement will be submitted to the European Parliament for its consent.

I look forward to hearing from you.

Yours sincerely,



Tiina ASTOLA

Privacy Shield's Prospects: The Good, the Bad, and the Ugly

By Peter Margulies

Thursday, March 3, 2016, 8:50 AM

Link: <https://www.lawfareblog.com/privacy-shields-prospects-good-bad-and-ugly>

If the devil is in the details, then the announcement early Monday of the inner workings of the new US-EU data-transfer agreement, Privacy Shield, may lack the granularity the deal needs to flourish. There is much to applaud in the new agreement, including extraordinary transparency from the US and a new safeguard to address EU privacy complaints in the form of a State Department Ombudsperson. Those virtues, however, may not be sufficient to ensure the viability of Privacy Shield, which replaces the Safe Harbor framework invalidated by the Court of Justice of the European Union (CJEU) in *Schrems v. Data Commissioner*.

The CJEU struck down Safe Harbor on the grounds that it lacked both substantive and independent procedural protections against US intelligence collection. The Privacy Shield roll-out is short on concrete information regarding the State Department Ombudsperson's authority and is instead reliant on broad US "representations" regarding substantive limits on foreign intelligence collection. The CJEU may not be impressed, especially since the CJEU rarely provides European officials with the deference supplied by the European Court of Human Rights (ECHR).

First, the good in Privacy Shield: ODNI General Counsel Bob Litt's [letter](#) reinforces a salutary trend toward transparency that ODNI has championed since the Snowden revelations. To my knowledge, no intelligence service has provided close to the level of detail about intelligence community (IC) structure and decision making that the ODNI letter provides, as it builds on the commitment announced by President Obama in his PPD-28 initiative. The ODNI letter painstakingly describes several layers of review within the IC, including the setting of priorities by the National Signals Intelligence Committee (SIGCOM). In comparison, most European states continue to keep mum about their own internal processes.

The ODNI letter also reaffirms substantive limitations in PPD-28. Bulk collection abroad, which ODNI says may sometimes be necessary to "identify new or emerging threats" concealed in the forest of global data, is limited to the grounds specified in PPD-28, including counterterrorism, combating weapons proliferation, addressing transnational illegality including sanctions evasion, detecting threats to US or allied forces, and learning about certain activities of foreign powers. The US also reiterates its PPD-28 pledge not to collect information in bulk for the purposes of suppressing dissent, disadvantaging individuals or groups based on criteria such as race, gender, or religion, or supplying US firms with a competitive advantage. Moreover, the IC cannot engage in the "arbitrary or indiscriminate collection" of data regarding "ordinary European citizens."

The ODNI letter commits the IC to tailoring collection. Analysts will focus on "specific foreign intelligence targets or topics through the use of discriminants (e.g., specific facilities, selection terms and identifiers)" whenever that specific approach is "practicable." Moreover,

the IC has multiple layers of internal review, including the ODNI Civil Liberties and Privacy Office. I would add that my own conversations with ODNI and NSA privacy officials—who regularly engage with the public and the privacy community—reinforce my view that this internal control is indeed robust. Other constraints within the executive branch include inspectors general who report regularly to Congress, and the Privacy and Civil Liberties Oversight Board (PCLOB), which has authored well-received reports on U.S. surveillance. In addition, ODNI notes that the Foreign Intelligence Surveillance Court (FISC) now has statutory authority to appoint independent advocates, including noted privacy advocates. And, of course, Congress can also monitor the IC, exerting budgetary pressure if it sees something untoward. The FISC’s authority to appoint independent attorneys stems from statutory changes, including the USA Freedom Act, negotiated with the Administration in the wake of Snowden’s disclosures.

That’s the good in the Privacy Shield roll-out; now for the bad. First, the US representations that it won’t engage in “arbitrary or indiscriminate” collection on Europeans are described only in general terms. The European Commission (EC) [statement](#) that the new framework has “adequate” protections for Europeans relies on “explicit assurances” provided by the US. However, the EC statement shares nothing on what those assurances entail. Since the US and the EC have significant business interests dependent on a new privacy agreement, some may question whether those assurances are as robust as the CJEU or EU privacy regulators would prefer. There is simply no way to judge, based on the materials disclosed thus far.

Moreover, the ODNI letter does not address a central EU concern with the status quo: the vagueness of the “foreign affairs” basis for collection under section 702 of the Foreign Intelligence Surveillance Amendments Act (for more, see Tim Edgar’s [analysis](#)). I’ve [written previously](#) that the foreign affairs prong of section 702 is limited by language that confines such collection to matters concerning a “foreign power” or “territory.” I continue to believe that this language focuses the foreign affairs prong on collection relating to foreign officials and does not extend to monitoring of foreign persons’ routine activities. Perhaps the assurances that US officials provided to the EC confirm this view. Moreover, perhaps the FISC can provide a check to unduly broad interpretation of this provision, since the EC adequacy analysis states that the IC has agreed to a PCLOB recommendation to provide the FISC with a random sample of analysts’ tasked searches. However, the lack of public reassurance on this score underlines a concern of the EC Working Group that the CJEU highlighted in Schrems.

Furthermore, procedural safeguards outlined by ODNI may not be as robust as the CJEU wishes. The inspectors general, for example, are hampered by a recent Justice Department Office of Legal Counsel [opinion](#) that allows executive branch agencies to limit disclosure of data to inspectors general conducting investigations. Moreover, the FISC has no control over the United States’ biggest foreign collection program, which is based on Executive Order 12333. The State Department Ombudsperson may have the authority to address complaints that involve EO 12333, but the announcement is not clear on this point. The Ombudsperson description in [Annex III](#) of the roll-out says that this official will “work closely” with other government officials. Nevertheless, the description does not specify that the Ombudsperson will have full access to IC data and procedures.

Similarly, according to the EC statement, the Ombudsperson will have to “confirm” that each complaint received has been “properly investigated.” To confirm this, the Ombudsperson must ascertain that surveillance has complied with US law, including the “representations”

and “explicit assurances” that the US has provided, or that any violation has been remedied. However, this confirmation brings us back to the lack of specificity in the public version of those US “representations.” It is difficult to see how robust the Ombudsperson’s review will be, when so much depends on assurances that are not accessible to the public, the CJEU, or European data regulators.

As Privacy Shield is implemented, the Ombudsperson may develop a course of dealing with the IC that addresses these concerns. Experience might demonstrate that the Ombudsperson has access to all the information that she needs, and uses that information to keep the IC honest. But that experience will be outside of the four corners of the Privacy Shield’s founding documents, making consideration of experience’s teachings a tougher sell with skeptical actors such as the CJEU.

That brings us to the ugly. The CJEU should provide some deference to the EC, particularly on matters involving national security. That deference is apparent in decisions of the ECHR on surveillance, such as *Weber v. Germany*, which upheld a substantial overseas surveillance program conducted by the German Republic. However, the CJEU has in practice diminished deference to near-microscopic levels in cases like *Schrems* and *Kadi v. Council*, which invalidated the EU’s implementation of the UN’s terrorist sanctions framework. Indeed, the framework invalidated in *Kadi II* also involved an ombudsperson, who had been effective in ensuring fairness to subjects of sanctions. This real-world efficacy made no difference to the CJEU. Instead, the CJEU insisted on a more formal due process mechanism, which was unworkable because of states’ reluctance to disclose intelligence sources and methods supporting terrorist designations.

The CJEU may also have concerns about the independence of the State Department Ombudsperson for Privacy Shield. True, that official will not formally be part of the IC, and in this sense will be independent. Nevertheless, the State Department is also an executive branch department, and is a customer of the IC, making use of intelligence that the IC provides. The President can fire the Ombudsperson, as he or she can fire IC officials. The Ombudsperson may as a practical matter retain independence, as inspectors general do, because of her different constituency. But that belief hinges on institutional culture more than formal legal guarantees. Institutional culture may be too weak a reed to support Privacy Shield, particularly for a court as activist as the CJEU.

In sum, Privacy Shield brings much to the table, including a welcome US candor that will hopefully rub off on our more reticent European allies. The Ombudsperson proposal has significant promise. However, it is too early to tell whether the Ombudsperson can develop a track record of effectiveness that persuades the CJEU and European regulators who found Safe Harbor wanting.

NYT - Penny Pritzker on the Privacy Shield Pact With Europe

By MARK SCOTT MARCH 8, 2016

Secretary of Commerce Penny Pritzker led the American negotiating team at the privacy talks. Credit Rebecca Blackwell/Associated Press

The E.U.-U.S. Privacy Shield may, at first blush, sound like a pretty boring group of superhero characters. But the agreement, whose details [were released](#) late last month, will have a major impact on how companies collect, manage and use digital data transferred from Europe to the United States.

It places a greater onus on companies like Google and General Electric to ensure people's digital information — from social media posts to employee payroll data — is not misused. The deal also forces the United States government to further limit what access the country's intelligence agencies have to Europeans' data when it is moved across the Atlantic.

The European Court of Justice, the region's highest court, [ruled last year](#) that the previous data-transfer agreement was invalid because it did not provide sufficient protection for European citizens when their data was transferred to the United States.

The new deal, though, did not come without a fight. American and European negotiators [bickered](#) over many of the proposals, partly because both sides [took different views](#) on how individuals' data protection rights should be handled. In Europe, privacy is seen as a fundamental right on par with freedom of expression, while in the United States, a number of privacy laws apply only to specific sectors, like health and credit.

[Penny Pritzker](#), the United States commerce secretary who led the American negotiating team, recently talked with The New York Times about the new data-transfer deal, what it means for people and how privacy is viewed differently on the two sides of the Atlantic. This interview has been condensed and edited for clarity.

Q. *What is the importance of the new Privacy Shield?*

A. It allows us to acknowledge that even though we have different systems when it comes to privacy, they are both strong enough to protect the \$260 billion of trans-Atlantic commerce that depends on having the Privacy Shield in place.

Q. *There has been criticism that the deal does not go far enough to protect people's privacy. What's your response to that?*

A. We feel very strongly that we have met Europe's privacy conditions. The college of European Commissioners also came to the same conclusion. We looked very carefully at all of the provisions to make sure that the new framework fully met the standards set by the European Court of Justice.

Q. *What were the hardest compromises that you had to make to reach a final agreement?*

A. The issues in the end that took the longest time were around the ombudsman proposal (an official in the State Department that will review European complaints about American intelligence agencies' access to their data) and the arbitration proposal (the ability for Europeans to seek legal remedies from American companies when they believe their digital information is misused).

The issue with the ombudsman was to ensure she had the ability to access the information required from our intelligence community, and to explain to the Europeans that she reported through the secretary of state, not through the intelligence community, so that she is independent.

On the arbitration proposal, there were questions on how was it going to work in practice, and to make sure that it would not be overly onerous for either European citizens or U.S. companies.

Q. *How did you balance the American view on privacy with the somewhat different European view?*

A. The U.S. has a different structure than Europe, but both systems offer robust privacy protection. Part of the challenge was to make sure that the European negotiators understood how our system works.

Unlike the E.U., we don't have a single overarching privacy law. We have sectoral laws. It was important to explain to them how our system works. Now, the Privacy Shield provides a bridge between the two regions, acknowledging the effectiveness of both systems.

Q. *Do you think the United States has sufficient privacy protections in place for people's day-to-day activities?*

A. Yes. We have a very robust privacy structure, and the issues that were called into question by Europe have been addressed by the president (who has issued a number of executive orders to bolster privacy rights). The awareness of privacy by digital companies has only risen, and you have seen some of those companies take their own actions to protect privacy.

Q. *The negotiations at times were pretty difficult. And even now, privacy campaigners are threatening to take the new agreement to court. So can the Privacy Shield be seen as a success?*

A. We did our best to get a strong agreement to make sure that people understood that their privacy would be protected. Trust in the Internet and trust in the ability to send data back and forth is fundamental to the global economy.

What we tried to do is get a durable agreement so that in the long term, individuals and businesses can rely on the Privacy Shield.

Source: http://www.nytimes.com/2016/03/09/technology/penny-pritzker-on-the-privacy-shield-pact-with-europe.html?ref=business&_r=0

ANNEX I



UNITED STATES DEPARTMENT OF COMMERCE
The Secretary of Commerce
Washington, D.C. 20230

February 23, 2016

Ms. Věra Jourová
Commissioner for Justice, Consumers
and Gender Equality
European Commission
Rue de la Loi / Wetstraat 200
1049 Brussels
Belgium

Dear Commissioner Jourová:

On behalf of the United States, I am pleased to transmit herewith a package of EU-U.S. Privacy Shield materials that is the product of two years of productive discussions among our teams. This package, along with other materials available to the Commission from public sources, provides a very strong basis for a new adequacy finding by the European Commission.

We should both be proud of the improvements to the Framework. The Privacy Shield is based on Principles that have strong consensus support on both sides of the Atlantic, and we have strengthened their operation. Through our work together, we have the real opportunity to improve the protection of privacy around the world.

The Privacy Shield Package includes the Privacy Shield Principles, along with a letter, attached as Annex 1, from the International Trade Administration (ITA) of the Department of Commerce, which administers the program, describing the commitments that our Department has made to ensure that the Privacy Shield operates effectively. The Package also includes Annex 2, which includes other Department of Commerce commitments relating to the new arbitral model available under the Privacy Shield.

I have directed my staff to devote all necessary resources to implement the Privacy Shield Framework expeditiously and fully and to ensure the commitments in Annex 1 and Annex 2 are met in a timely fashion.

The Privacy Shield Package also includes other documents from other United States agencies, namely:

- A letter from the Federal Trade Commission (FTC) describing its enforcement of the Privacy Shield;
- A letter from the Department of Transportation describing its enforcement of the Privacy Shield;

- A letter prepared by the Office of the Director of National Intelligence (ODNI) regarding safeguards and limitations applicable to U.S. national security authorities;
- A letter from the Department of State and accompanying memorandum describing the State Department's commitment to establish a new Privacy Shield Ombudsperson for submission of inquiries regarding the United States' signals intelligence practices; and
- A letter prepared by the Department of Justice regarding safeguards and limitations on U.S. Government access for law enforcement and public interest purposes.

You can be assured that the United States takes these commitments seriously.

Within 30 days of final approval of the adequacy determination, the full Privacy Shield Package will be delivered to the *Federal Register* for publication.

We look forward to working with you as the Privacy Shield is implemented and as we embark on the next phase of this process together.

Sincerely,

A handwritten signature in black ink, appearing to read "Penny Pritzker". The signature is fluid and cursive, with the first name "Penny" and last name "Pritzker" clearly distinguishable.

Penny Pritzker

FEB 23 2016



UNITED STATES DEPARTMENT OF COMMERCE
The Under Secretary for International Trade
Washington, D.C. 20230

The Honorable Věra Jourová
Commissioner for Justice, Consumers and Gender Equality
European Commission
Rue de la Loi/Westraat 200
1049 Brussels
Belgium

Dear Commissioner Jourová:

On behalf of the International Trade Administration, I am pleased to describe the enhanced protection of personal data that the EU-U.S. Privacy Shield Framework ("Privacy Shield" or "Framework") provides and the commitments the Department of Commerce ("Department") has made to ensure that the Privacy Shield operates effectively. Finalizing this historic arrangement is a major achievement for privacy and for businesses on both sides of the Atlantic. It offers confidence to EU individuals that their data will be protected and that they will have legal remedies to address any concerns. It offers certainty that will help grow the transatlantic economy by ensuring that thousands of European and American businesses can continue to invest and do business across our borders. The Privacy Shield is the result of over two years of hard work and collaboration with you, our colleagues in the European Commission ("Commission"). We look forward to continuing to work with the Commission to ensure that the Privacy Shield functions as intended.

We have worked with the Commission to develop the Privacy Shield to allow organizations established in the United States to meet the adequacy requirements for data protection under EU law. The new Framework will yield several significant benefits for both individuals and businesses. First, it provides an important set of privacy protections for the data of EU individuals. It requires participating U.S. organizations to develop a conforming privacy policy, publicly commit to comply with the Privacy Shield Principles so that the commitment becomes enforceable under U.S. law, annually re-certify their compliance to the Department, provide free independent dispute resolution to EU individuals, and be subject to the authority of the U.S. Federal Trade Commission ("FTC"), Department of Transportation ("DOT"), or another enforcement agency. Second, the Privacy Shield will enable thousands of companies in the United States and subsidiaries of European companies in the United States to receive personal data from the European Union to facilitate data flows that support transatlantic trade. The transatlantic economic relationship is already the world's largest, accounting for half of global economic output and nearly one trillion dollars in goods and services trade, supporting millions of jobs on both sides of the Atlantic. Businesses that rely on transatlantic data flows come from all industry sectors and include major Fortune 500 firms as well as many small and medium-sized enterprises (SMEs). Transatlantic data flows allow U.S. organizations to process data required to offer goods, services, and employment opportunities to European individuals. The Privacy Shield supports shared privacy principles, bridging the differences in our legal approaches, while furthering trade and economic objectives of both Europe and the United States.



While a company's decision to self-certify to this new Framework will be voluntary, once a company publicly commits to the Privacy Shield, its commitment is enforceable under U.S. law by either the Federal Trade Commission or Department of Transportation, depending on which authority has jurisdiction over the Privacy Shield organization.

Enhancements under the Privacy Shield Principles

The resulting Privacy Shield strengthens the protection of privacy by:

- requiring additional information be provided to individuals in the Notice Principle, including a declaration of the organization's participation in the Privacy Shield, a statement of the individual's right to access personal data, and the identification of the relevant independent dispute resolution body;
- strengthening protection of personal data that is transferred from a Privacy Shield organization to a third party controller by requiring the parties to enter into a contract that provides that such data may only be processed for limited and specified purposes consistent with the consent provided by the individual and that the recipient will provide the same level of protection as the Principles;
- strengthening protection of personal data that is transferred from a Privacy Shield organization to a third party agent, including by requiring a Privacy Shield organization to: take reasonable and appropriate steps to ensure that the agent effectively processes the personal information transferred in a manner consistent with the organization's obligations under the Principles; upon notice, take reasonable and appropriate steps to stop and remediate unauthorized processing; and provide a summary or a representative copy of the relevant privacy provisions of its contract with that agent to the Department upon request;
- providing that a Privacy Shield organization is responsible for the processing of personal information it receives under the Privacy Shield and subsequently transfers to a third party acting as an agent on its behalf, and that the Privacy Shield organization shall remain liable under the Principles if its agent processes such personal information in a manner inconsistent with the Principles, unless the organization proves that it is not responsible for the event giving rise to the damage;
- clarifying that Privacy Shield organizations must limit personal information to the information that is relevant for the purposes of processing;
- requiring an organization to annually certify with the Department its commitment to apply the Principles to information it received while it participated in the Privacy Shield if it leaves the Privacy Shield and chooses to keep such data;
- requiring that independent recourse mechanisms be provided at no cost to the individual;
- requiring organizations and their selected independent recourse mechanisms to respond promptly to inquiries and requests by the Department for information relating to the Privacy Shield;
- requiring organizations to respond expeditiously to complaints regarding compliance with the Principles referred by EU Member State authorities through the Department; and
- requiring a Privacy Shield organization to make public any relevant Privacy Shield-related sections of any compliance or assessment report submitted to the FTC if it becomes subject to an FTC or court order based on non-compliance.

Administration and Supervision of the Privacy Shield Program by the Department of Commerce

The Department reiterates its commitment to maintain and make available to the public an authoritative list of U.S. organizations that have self-certified to the Department and declared their commitment to adhere to the Principles (the "Privacy Shield List"). The Department will keep the Privacy Shield List up to date by removing organizations when they voluntarily withdraw, fail to complete the annual re-certification in accordance with the Department's procedures, or are found to persistently fail to comply. The Department will also maintain and make available to the public an authoritative record of U.S. organizations that had previously self-certified to the Department, but that have been removed from the Privacy Shield List, including those that were removed for persistent failure to comply with the Principles. The Department will identify the reason each organization was removed.

In addition, the Department commits to strengthening the administration and supervision of the Privacy Shield. Specifically, the Department will:

Provide Additional Information on the Privacy Shield Website

- maintain the Privacy Shield List, as well as a record of those organizations that previously self-certified their adherence to the Principles, but which are no longer assured of the benefits of the Privacy Shield;
- include a prominently placed explanation clarifying that all organizations removed from the Privacy Shield List are no longer assured of the benefits of the Privacy Shield, but must nevertheless continue to apply the Principles to the personal information that they received while they participated in the Privacy Shield for as long as they retain such information; and
- provide a link to the list of Privacy Shield-related FTC cases maintained on the FTC website.

Verify Self-Certification Requirements

- prior to finalizing an organization's self-certification (or annual re-certification) and placing an organization on the Privacy Shield List, verify that the organization has:
 - provided required organization contact information;
 - described the activities of the organization with respect to personal information received from the EU;
 - indicated what personal information is covered by its self-certification;
 - if the organization has a public website, provided the web address where the privacy policy is available and the privacy policy is accessible at the web address provided, or if an organization does not have a public website, provided where the privacy policy is available for viewing by the public;
 - included in its relevant privacy policy a statement that it adheres to the Principles and if the privacy policy is available online, a hyperlink to the Department's Privacy Shield website;

- identified the specific statutory body that has jurisdiction to hear any claims against the organization regarding possible unfair or deceptive practices and violations of laws or regulations governing privacy (and that is listed in the Principles or a future annex to the Principles);
 - if the organization elects to satisfy the requirements in points (a)(i) and (a)(iii) of the Recourse, Enforcement and Liability Principle by committing to cooperate with the appropriate EU data protection authorities (“DPAs”), indicated its intention to cooperate with DPAs in the investigation and resolution of complaints brought under the Privacy Shield, notably to respond to their inquiries when EU data subjects have brought their complaints directly to their national DPAs;
 - identified any privacy program in which the organization is a member;
 - identified the method of verification of assuring compliance with the Principles (*e.g.*, in-house, third party);
 - identified, both in its self-certification submission and in its privacy policy, the independent recourse mechanism that is available to investigate and resolve complaints;
 - included in its relevant privacy policy, if the policy is available online, a hyperlink to the website or complaint submission form of the independent recourse mechanism that is available to investigate unresolved complaints; and
 - if the organization has indicated that it intends to receive human resources information transferred from the EU for use in the context of the employment relationship, declared its commitment to cooperate and comply with DPAs to resolve complaints concerning its activities with regard to such data, provided the Department with a copy of its human resources privacy policy, and provided where the privacy policy is available for viewing by its affected employees.
- work with independent recourse mechanisms to verify that the organizations have in fact registered with the relevant mechanism indicated in their self-certification submissions, where such registration is required.

Expand Efforts to Follow Up with Organizations That Have Been Removed from the Privacy Shield List

- notify organizations that are removed from the Privacy Shield List for “persistent failure to comply” that they are not entitled to retain information collected under the Privacy Shield; and
- send questionnaires to organizations whose self-certifications lapse or who have voluntarily withdrawn from the Privacy Shield to verify whether the organization will return, delete, or continue to apply the Principles to the personal information that they received while they participated in the Privacy Shield, and if personal information will be retained, verify who within the organization will serve as an ongoing point of contact for Privacy Shield-related questions.

Search for and Address False Claims of Participation

- review the privacy policies of organizations that have previously participated in the Privacy Shield program, but that have been removed from the Privacy Shield List to identify any false claims of Privacy Shield participation;
- on an ongoing basis, when an organization: (a) withdraws from participation in the Privacy Shield, (b) fails to recertify its adherence to the Principles, or (c) is removed as a participant in the Privacy Shield notably for “persistent failure to comply,” undertake, on an *ex officio* basis, to verify that the organization has removed from any relevant published privacy policy any references to the Privacy Shield that imply that the organization continues to actively participate in the Privacy Shield and is entitled to its benefits. Where the Department finds that such references have not been removed, the Department will warn the organization that the Department will, as appropriate, refer matters to the relevant agency for potential enforcement action if it continues to make the claim of Privacy Shield certification. If the organization neither removes the references nor self-certifies its compliance under the Privacy Shield, the Department will *ex officio* refer the matter to the FTC, DOT, or other appropriate enforcement agency or, in appropriate cases, take action to enforce the Privacy Shield certification mark;
- undertake other efforts to identify false claims of Privacy Shield participation and improper use of the Privacy Shield certification mark, including by conducting Internet searches to identify where images of the Privacy Shield certification mark are being displayed and references to Privacy Shield in organizations’ privacy policies;
- promptly address any issues that we identify during our *ex officio* monitoring of false claims of participation and misuse of the certification mark, including warning organizations misrepresenting their participation in the Privacy Shield program as described above;
- take other appropriate corrective action, including pursuing any legal recourse the Department is authorized to take and referring matters to the FTC, DOT, or another appropriate enforcement agency; and
- promptly review and address complaints about false claims of participation that we receive.

The Department will undertake reviews of privacy policies of organizations to more effectively identify and address false claims of Privacy Shield participation. Specifically, the Department will review the privacy policies of organizations whose self-certification has lapsed due to their failure to re-certify adherence to the Principles. The Department will conduct this type of review to verify that such organizations have removed from any relevant published privacy policy any references that imply that the organizations continue to actively participate in the Privacy Shield. As a result of these types of reviews, we will identify organizations that have not removed such references and send those organizations a letter from the Department’s Office of General Counsel warning of potential enforcement action if the references are not removed. The Department will take follow-up action to ensure that the organizations either remove the inappropriate references or re-certify their adherence to the Principles. In addition, the Department will undertake efforts to identify false claims of Privacy Shield participation by organizations that have never participated in the Privacy Shield program, and will take similar corrective action with respect to such organizations.

Conduct Periodic *ex officio* Compliance Reviews and Assessments of the Program

- on an ongoing basis, monitor effective compliance, including through sending detailed questionnaires to participating organizations, to identify issues that may warrant further follow-up action. In particular, such compliance reviews shall take place when: (a) the Department has received specific non-frivolous complaints about an organization's compliance with the Principles, (b) an organization does not respond satisfactorily to inquiries by the Department for information relating to the Privacy Shield, or (c) there is credible evidence that an organization does not comply with its commitments under the Privacy Shield. The Department shall, when appropriate, consult with the competent data protection authorities about such compliance reviews; and
- assess periodically the administration and supervision of the Privacy Shield program to ensure that monitoring efforts are appropriate to address new issues as they arise.

The Department has increased the resources that will be devoted to the administration and supervision of the Privacy Shield program, including doubling the number of staff responsible for the administration and supervision of the program. We will continue to dedicate appropriate resources to such efforts to ensure effective monitoring and administration of the program.

Tailor the Privacy Shield Website to Targeted Audiences

The Department will tailor the Privacy Shield website to focus on three target audiences: EU individuals, EU businesses, and U.S. businesses. The inclusion of material targeted directly to EU individuals and EU businesses will facilitate transparency in a number of ways. With regard to EU individuals, it will clearly explain: (1) the rights the Privacy Shield provides to EU individuals; (2) the recourse mechanisms available to EU individuals when they believe an organization has breached its commitment to comply with the Principles; and (3) how to find information pertaining to an organization's Privacy Shield self-certification. With regard to EU businesses, it will facilitate verification of: (1) whether an organization is assured of the benefits of the Privacy Shield; (2) the type of information covered by an organization's Privacy Shield self-certification; (3) the privacy policy that applies to the covered information; and (4) the method the organization uses to verify its adherence to the Principles.

Increase Cooperation with DPAs

To increase opportunities for cooperation with DPAs, the Department will establish a dedicated contact at the Department to act as a liaison with DPAs. In instances where a DPA believes that an organization is not complying with the Principles, including following a complaint from an EU individual, the DPA can reach out to the dedicated contact at the Department to refer the organization for further review. The contact will also receive referrals regarding organizations that falsely claim to participate in the Privacy Shield, despite never having self-certified their adherence to the Principles. The contact will assist DPAs seeking information related to a specific organization's self-certification or previous participation in the program, and the contact will respond to DPA inquiries regarding the implementation of specific Privacy Shield requirements. Second, the Department will provide DPAs with material

regarding the Privacy Shield for inclusion on their own websites to increase transparency for EU individuals and EU businesses. Increased awareness regarding the Privacy Shield and the rights and responsibilities it creates should facilitate the identification of issues as they arise, so that these can be appropriately addressed.

Facilitate Resolution of Complaints about Non-Compliance

The Department, through the dedicated contact, will receive complaints referred to the Department by a DPA that a Privacy Shield organization is not complying with the Principles. The Department will make its best effort to facilitate resolution of the complaint with the Privacy Shield organization. Within 90 days after receipt of the complaint, the Department will provide an update to the DPA. To facilitate the submission of such complaints, the Department will create a standard form for DPAs to submit to the Department's dedicated contact. The dedicated contact will track all referrals from DPAs received by the Department, and the Department will provide in the annual review described below a report analyzing in aggregate the complaints it receives each year.

Adopt Arbitral Procedures and Select Arbitrators in Consultation with the Commission

The Department will fulfill its commitments under Annex I and publish the procedures after agreement has been reached.

Joint Review Mechanism of the Functioning of the Privacy Shield

The Department of Commerce, the FTC, and other agencies, as appropriate, will hold annual meetings with the Commission, interested DPAs, and appropriate representatives from the Article 29 Working Party, where the Department will provide updates on the Privacy Shield program. The annual meetings will include discussion of current issues related to the functioning, implementation, supervision, and enforcement of the Privacy Shield, including referrals received by the Department from DPAs, the results of *ex officio* compliance reviews, and may also include discussion of relevant changes of law.

National Security Exception

With respect to the limitations to the adherence to the Privacy Shield Principles for national security purposes, the General Counsel of the Office of the Director of National Intelligence, Robert Litt, has also sent a letter addressed to Justin Antonipillai and Ted Dean of the Department of Commerce, and this has been forwarded to you. This letter extensively discusses, among other things, the policies, safeguards, and limitations that apply to signals intelligence activities conducted by the U.S. In addition, this letter describes the transparency provided by the Intelligence Community about these matters. As the Commission is assessing the Privacy Shield Framework, the information in this letter provides assurance to conclude that the Privacy Shield will operate appropriately, in accordance with the Principles therein. We understand that you may raise information that has been released publicly by the Intelligence Community, along with other information, in the future to inform the annual review of the Privacy Shield Framework.

On the basis of the Privacy Shield Principles and the accompanying letters and materials, including the Department's commitments regarding the administration and supervision of the Privacy Shield Framework, our expectation is that the Commission will determine that the EU-U.S. Privacy Shield Framework provides adequate protection for the purposes of EU law and data transfers from the European Union will continue to organizations that participate in the Privacy Shield.

Sincerely,

A handwritten signature in black ink, appearing to read 'Stefan M. Selig', with a horizontal line drawn through it.

Stefan M. Selig

ANNEX II

EU-U.S. PRIVACY SHIELD FRAMEWORK PRINCIPLES ISSUED BY THE U.S. DEPARTMENT OF COMMERCE

I. OVERVIEW

1. While the United States and the European Union share the goal of enhancing privacy protection for their citizens, the United States takes a different approach to privacy from that taken by the European Union. The United States uses a sectoral approach that relies on a mix of legislation, regulation, and self-regulation. Given those differences and to provide organizations in the United States with a reliable mechanism for personal data transfers to the United States from the European Union while ensuring that EU data subjects continue to benefit from effective safeguards and protection as required by European legislation with respect to the processing of their personal data when they have been transferred to non-EU countries, the Department of Commerce is issuing these Privacy Shield Principles, including the Supplemental Principles (collectively “the Principles”) under its statutory authority to foster, promote, and develop international commerce (15 U.S.C. § 1512). The Principles were developed in consultation with the European Commission, and with industry and other stakeholders, to facilitate trade and commerce between the United States and European Union. They are intended for use solely by organizations in the United States receiving personal data from the European Union for the purpose of qualifying for the Privacy Shield and thus benefitting from the European Commission’s adequacy decision. The Principles do not affect the application of national provisions implementing Directive 95/46/EC (“the Directive”) that apply to the processing of personal data in the Member States. Nor do the Principles limit privacy obligations that otherwise apply under U.S. law.
2. In order to rely on the Privacy Shield to effectuate transfers of personal data from the EU, an organization must self-certify its adherence to the Principles to the Department of Commerce (or its designee) (“the Department”). While decisions by organizations to thus enter the Privacy Shield are entirely voluntary, effective compliance is compulsory: organizations that self-certify to the Department and publicly declare their commitment to adhere to the Principles must comply fully with the Principles. In order to enter the Privacy Shield, an organization must (a) be subject to the investigatory and enforcement powers of the Federal Trade Commission (the “FTC”), the Department of Transportation or another statutory body that will effectively ensure compliance with the Principles (other U.S. statutory bodies recognized by the EU may be included as an annex in the future); (b) publicly declare its commitment to comply with the Principles; (c) publicly disclose its privacy policies in line with these Principles; and (d) fully implement them. An organization’s failure to comply is enforceable under Section 5 of the Federal Trade Commission Act prohibiting unfair and deceptive acts in or affecting commerce (15 U.S.C. § 45(a)) or other laws or regulations prohibiting such acts.

3. The Department of Commerce will maintain and make available to the public an authoritative list of U.S. organizations that have self-certified to the Department and declared their commitment to adhere to the Principles (“the Privacy Shield List”). Privacy Shield benefits are assured from the date that the Department places the organization on the Privacy Shield List. The Department will remove an organization from the Privacy Shield List if it voluntarily withdraws from the Privacy Shield or if it fails to complete its annual re-certification to the Department. An organization’s removal from the Privacy Shield List means it may no longer benefit from the European Commission’s adequacy decision to receive personal information from the EU. The organization must continue to apply the Principles to the personal information it received while it participated in the Privacy Shield, and affirm to the Department on an annual basis its commitment to do so, for as long as it retains such information; otherwise, the organization must return or delete the information or provide “adequate” protection for the information by another authorized means. The Department will also remove from the Privacy Shield List those organizations that have persistently failed to comply with the Principles; these organizations do not qualify for Privacy Shield benefits and must return or delete the personal information they received under the Privacy Shield.
4. The Department will also maintain and make available to the public an authoritative record of U.S. organizations that had previously self-certified to the Department, but that have been removed from the Privacy Shield List. The Department will provide a clear warning that these organizations are not participants in the Privacy Shield; that removal from the Privacy Shield List means that such organizations cannot claim to be Privacy Shield compliant and must avoid any statements or misleading practices implying that they participate in the Privacy Shield; and that such organizations are no longer entitled to benefit from the European Commission’s adequacy decision that would enable those organizations to receive personal information from the EU. An organization that continues to claim participation in the Privacy Shield or makes other Privacy Shield-related misrepresentations after it has been removed from the Privacy Shield List may be subject to enforcement action by the FTC, the Department of Transportation, or other enforcement authorities.
5. Adherence to these Principles may be limited: (a) to the extent necessary to meet national security, public interest, or law enforcement requirements; (b) by statute, government regulation, or case law that creates conflicting obligations or explicit authorizations, provided that, in exercising any such authorization, an organization can demonstrate that its non-compliance with the Principles is limited to the extent necessary to meet the overriding legitimate interests furthered by such authorization; or (c) if the effect of the Directive or Member State law is to allow exceptions or derogations, provided such exceptions or derogations are applied in comparable contexts. Consistent with the goal of enhancing privacy protection, organizations should strive to implement these Principles fully and transparently, including indicating in their privacy policies where exceptions to the Principles permitted by (b) above will apply on a regular basis. For the same reason, where the option is

allowable under the Principles and/or U.S. law, organizations are expected to opt for the higher protection where possible.

6. Organizations are obligated to apply the Principles to all personal data transferred in reliance on the Privacy Shield after they enter the Privacy Shield. An organization that chooses to extend Privacy Shield benefits to human resources personal information transferred from the EU for use in the context of an employment relationship must indicate this when it self-certifies to the Department and conform to the requirements set forth in the Supplemental Principle on Self-Certification.
7. U.S. law will apply to questions of interpretation and compliance with the Principles and relevant privacy policies by Privacy Shield organizations, except where such organizations have committed to cooperate with European data protection authorities (“DPAs”). Unless otherwise stated, all provisions of the Principles apply where they are relevant.
8. Definitions:
 - a. “Personal data” and “personal information” are data about an identified or identifiable individual that are within the scope of the Directive, received by an organization in the United States from the European Union, and recorded in any form.
 - b. “Processing” of personal data means any operation or set of operations which is performed upon personal data, whether or not by automated means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure or dissemination, and erasure or destruction.
 - c. “Controller” means a person or organization which, alone or jointly with others, determines the purposes and means of the processing of personal data.
9. The effective date of the Principles is the date of final approval of the European Commission’s adequacy determination.

II. PRINCIPLES

1. NOTICE

- a. An organization must inform individuals about:
 - i. its participation in the Privacy Shield and provide a link to, or the web address for, the Privacy Shield List,
 - ii. the types of personal data collected and, where applicable, the entities or subsidiaries of the organization also adhering to the Principles,
 - iii. its commitment to subject to the Principles all personal data received from the EU in reliance on the Privacy Shield,
 - iv. the purposes for which it collects and uses personal information about them,
 - v. how to contact the organization with any inquiries or complaints, including any relevant establishment in the EU that can respond to such inquiries or complaints,
 - vi. the type or identity of third parties to which it discloses personal information, and the purposes for which it does so,
 - vii. the right of individuals to access their personal data,
 - viii. the choices and means the organization offers individuals for limiting the use and disclosure of their personal data,
 - ix. the independent dispute resolution body designated to address complaints and provide appropriate recourse free of charge to the individual, and whether it is: (1) the panel established by DPAs, (2) an alternative dispute resolution provider based in the EU, or (3) an alternative dispute resolution provider based in the United States,
 - x. being subject to the investigatory and enforcement powers of the FTC, the Department of Transportation or any other U.S. authorized statutory body,
 - xi. the possibility, under certain conditions, for the individual to invoke binding arbitration,
 - xii. the requirement to disclose personal information in response to lawful requests by public authorities, including to meet national security or law enforcement requirements, and

- xiii. its liability in cases of onward transfers to third parties.
- b. This notice must be provided in clear and conspicuous language when individuals are first asked to provide personal information to the organization or as soon thereafter as is practicable, but in any event before the organization uses such information for a purpose other than that for which it was originally collected or processed by the transferring organization or discloses it for the first time to a third party.

2. CHOICE

- a. An organization must offer individuals the opportunity to choose (opt out) whether their personal information is (i) to be disclosed to a third party or (ii) to be used for a purpose that is materially different from the purpose(s) for which it was originally collected or subsequently authorized by the individuals. Individuals must be provided with clear, conspicuous, and readily available mechanisms to exercise choice.
- b. By derogation to the previous paragraph, it is not necessary to provide choice when disclosure is made to a third party that is acting as an agent to perform task(s) on behalf of and under the instructions of the organization. However, an organization shall always enter into a contract with the agent.
- c. For sensitive information (*i.e.*, personal information specifying medical or health conditions, racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership or information specifying the sex life of the individual), organizations must obtain affirmative express consent (opt in) from individuals if such information is to be (i) disclosed to a third party or (ii) used for a purpose other than those for which it was originally collected or subsequently authorized by the individuals through the exercise of opt-in choice. In addition, an organization should treat as sensitive any personal information received from a third party where the third party identifies and treats it as sensitive.

3. ACCOUNTABILITY FOR ONWARD TRANSFER

- a. To transfer personal information to a third party acting as a controller, organizations must comply with the Notice and Choice Principles. Organizations must also enter into a contract with the third-party controller that provides that such data may only be processed for limited and specified purposes consistent with the consent provided by the individual and that the recipient will provide the same level of protection as the Principles.
- b. To transfer personal data to a third party acting as an agent, organizations must: (i) transfer such data only for limited and specified purposes; (ii) ascertain that the agent is obligated to provide at least the

same level of privacy protection as is required by the Principles; (iii) take reasonable and appropriate steps to ensure that the agent effectively processes the personal information transferred in a manner consistent with the organization's obligations under the Principles; (iv) upon notice, take reasonable and appropriate steps to stop and remediate unauthorized processing; and (v) provide a summary or a representative copy of the relevant privacy provisions of its contract with that agent to the Department upon request.

4. SECURITY

- a. Organizations creating, maintaining, using or disseminating personal information must take reasonable and appropriate measures to protect it from loss, misuse and unauthorized access, disclosure, alteration and destruction, taking into due account the risks involved in the processing and the nature of the personal data.

5. DATA INTEGRITY AND PURPOSE LIMITATION

- a. Consistent with the Principles, personal information must be limited to the information that is relevant for the purposes of processing. An organization may not process personal information in a way that is incompatible with the purposes for which it has been collected or subsequently authorized by the individual. To the extent necessary for those purposes, an organization must take reasonable steps to ensure that personal data is reliable for its intended use, accurate, complete, and current. An organization must adhere to the Principles for as long as it retains such information.

6. ACCESS

- a. Individuals must have access to personal information about them that an organization holds and be able to correct, amend, or delete that information where it is inaccurate, or has been processed in violation of the Principles, except where the burden or expense of providing access would be disproportionate to the risks to the individual's privacy in the case in question, or where the rights of persons other than the individual would be violated.

7. RECOURSE, ENFORCEMENT AND LIABILITY

- a. Effective privacy protection must include robust mechanisms for assuring compliance with the Principles, recourse for individuals who are affected by non-compliance with the Principles, and consequences for the organization when the Principles are not followed. At a minimum such mechanisms must include:
 - i. readily available independent recourse mechanisms by which each individual's complaints and disputes are investigated and expeditiously resolved at no cost to the individual and by

- reference to the Principles, and damages awarded where the applicable law or private-sector initiatives so provide;
- ii. follow-up procedures for verifying that the attestations and assertions organizations make about their privacy practices are true and that privacy practices have been implemented as presented and, in particular, with regard to cases of non-compliance; and
 - iii. obligations to remedy problems arising out of failure to comply with the Principles by organizations announcing their adherence to them and consequences for such organizations. Sanctions must be sufficiently rigorous to ensure compliance by organizations.
- b. Organizations and their selected independent recourse mechanisms will respond promptly to inquiries and requests by the Department for information relating to the Privacy Shield. All organizations must respond expeditiously to complaints regarding compliance with the Principles referred by EU Member State authorities through the Department. Organizations that have chosen to cooperate with DPAs, including organizations that process human resources data, must respond directly to such authorities with regard to the investigation and resolution of complaints.
 - c. Organizations are obligated to arbitrate claims and follow the terms as set forth in Annex I, provided that an individual has invoked binding arbitration by delivering notice to the organization at issue and following the procedures and subject to conditions set forth in Annex I.
 - d. In the context of an onward transfer, a Privacy Shield organization has responsibility for the processing of personal information it receives under the Privacy Shield and subsequently transfers to a third party acting as an agent on its behalf. The Privacy Shield organization shall remain liable under the Principles if its agent processes such personal information in a manner inconsistent with the Principles, unless the organization proves that it is not responsible for the event giving rise to the damage.
 - e. When an organization becomes subject to an FTC or court order based on non-compliance, the organization shall make public any relevant Privacy Shield-related sections of any compliance or assessment report submitted to the FTC, to the extent consistent with confidentiality requirements. The Department has established a dedicated point of contact for DPAs for any problems of compliance by Privacy Shield organizations. The FTC will give priority consideration to referrals of non-compliance with the Principles from the Department and EU Member State authorities, and will exchange information regarding referrals with the referring state authorities on a timely basis, subject to existing confidentiality restrictions.

III. SUPPLEMENTAL PRINCIPLES

1. Sensitive Data

- a. An organization is not required to obtain affirmative express consent (opt in) with respect to sensitive data where the processing is:
 - i. in the vital interests of the data subject or another person;
 - ii. necessary for the establishment of legal claims or defenses;
 - iii. required to provide medical care or diagnosis;
 - iv. carried out in the course of legitimate activities by a foundation, association or any other non-profit body with a political, philosophical, religious or trade-union aim and on condition that the processing relates solely to the members of the body or to the persons who have regular contact with it in connection with its purposes and that the data are not disclosed to a third party without the consent of the data subjects;
 - v. necessary to carry out the organization's obligations in the field of employment law; or
 - vi. related to data that are manifestly made public by the individual.

2. Journalistic Exceptions

- a. Given U.S. constitutional protections for freedom of the press and the Directive's exemption for journalistic material, where the rights of a free press embodied in the First Amendment of the U.S. Constitution intersect with privacy protection interests, the First Amendment must govern the balancing of these interests with regard to the activities of U.S. persons or organizations.
- b. Personal information that is gathered for publication, broadcast, or other forms of public communication of journalistic material, whether used or not, as well as information found in previously published material disseminated from media archives, is not subject to the requirements of the Privacy Shield Principles.

3. Secondary Liability

- a. Internet Service Providers ("ISPs"), telecommunications carriers, and other organizations are not liable under the Privacy Shield Principles when on behalf of another organization they merely transmit, route, switch, or cache information. As is the case with the Directive itself, the Privacy Shield does not create secondary liability. To the extent that an organization is acting as a mere conduit for data transmitted by third parties and does not determine the purposes and means of processing those personal data, it would not be liable.

4. Performing Due Diligence and Conducting Audits

- a. The activities of auditors and investment bankers may involve processing personal data without the consent or knowledge of the individual. This is permitted by the Notice, Choice, and Access Principles under the circumstances described below.
- b. Public stock corporations and closely held companies, including Privacy Shield organizations, are regularly subject to audits. Such audits, particularly those looking into potential wrongdoing, may be jeopardized if disclosed prematurely. Similarly, a Privacy Shield organization involved in a potential merger or takeover will need to perform, or be the subject of, a “due diligence” review. This will often entail the collection and processing of personal data, such as information on senior executives and other key personnel. Premature disclosure could impede the transaction or even violate applicable securities regulation. Investment bankers and attorneys engaged in due diligence, or auditors conducting an audit, may process information without knowledge of the individual only to the extent and for the period necessary to meet statutory or public interest requirements and in other circumstances in which the application of these Principles would prejudice the legitimate interests of the organization. These legitimate interests include the monitoring of organizations’ compliance with their legal obligations and legitimate accounting activities, and the need for confidentiality connected with possible acquisitions, mergers, joint ventures, or other similar transactions carried out by investment bankers or auditors.

5. The Role of the Data Protection Authorities

- a. Organizations will implement their commitment to cooperate with European Union data protection authorities (“DPAs”) as described below. Under the Privacy Shield, U.S. organizations receiving personal data from the EU must commit to employ effective mechanisms for assuring compliance with the Privacy Shield Principles. More specifically as set out in the Recourse, Enforcement and Liability Principle, participating organizations must provide: (a)(i) recourse for individuals to whom the data relate; (a)(ii) follow up procedures for verifying that the attestations and assertions they have made about their privacy practices are true; and (a)(iii) obligations to remedy problems arising out of failure to comply with the Principles and consequences for such organizations. An organization may satisfy points (a)(i) and (a)(iii) of the Recourse, Enforcement and Liability Principle if it adheres to the requirements set forth here for cooperating with the DPAs.
- b. An organization commits to cooperate with the DPAs by declaring in its Privacy Shield self-certification submission to the Department of Commerce (*see* Supplemental Principle on Self-Certification) that the organization:

- i. elects to satisfy the requirement in points (a)(i) and (a)(iii) of the Privacy Shield Recourse, Enforcement and Liability Principle by committing to cooperate with the DPAs;
- ii. will cooperate with the DPAs in the investigation and resolution of complaints brought under the Privacy Shield; and
- iii. will comply with any advice given by the DPAs where the DPAs take the view that the organization needs to take specific action to comply with the Privacy Shield Principles, including remedial or compensatory measures for the benefit of individuals affected by any non-compliance with the Principles, and will provide the DPAs with written confirmation that such action has been taken.

c. Operation of DPA Panels

- i. The cooperation of the DPAs will be provided in the form of information and advice in the following way:
 - 1. The advice of the DPAs will be delivered through an informal panel of DPAs established at the European Union level, which will *inter alia* help ensure a harmonized and coherent approach.
 - 2. The panel will provide advice to the U.S. organizations concerned on unresolved complaints from individuals about the handling of personal information that has been transferred from the EU under the Privacy Shield. This advice will be designed to ensure that the Privacy Shield Principles are being correctly applied and will include any remedies for the individual(s) concerned that the DPAs consider appropriate.
 - 3. The panel will provide such advice in response to referrals from the organizations concerned and/or to complaints received directly from individuals against organizations which have committed to cooperate with DPAs for Privacy Shield purposes, while encouraging and if necessary helping such individuals in the first instance to use the in-house complaint handling arrangements that the organization may offer.
 - 4. Advice will be issued only after both sides in a dispute have had a reasonable opportunity to comment and to provide any evidence they wish. The panel will seek to deliver advice as quickly as this requirement for due process allows. As a general rule, the panel will aim to provide advice within 60 days after receiving a complaint or referral and more quickly where possible.
 - 5. The panel will make public the results of its consideration of complaints submitted to it, if it sees fit.

6. The delivery of advice through the panel will not give rise to any liability for the panel or for individual DPAs.
 - ii. As noted above, organizations choosing this option for dispute resolution must undertake to comply with the advice of the DPAs. If an organization fails to comply within 25 days of the delivery of the advice and has offered no satisfactory explanation for the delay, the panel will give notice of its intention either to refer the matter to the Federal Trade Commission, the Department of Transportation, or other U.S. federal or state body with statutory powers to take enforcement action in cases of deception or misrepresentation, or to conclude that the agreement to cooperate has been seriously breached and must therefore be considered null and void. In the latter case, the panel will inform the Department of Commerce so that the Privacy Shield List can be duly amended. Any failure to fulfill the undertaking to cooperate with the DPAs, as well as failures to comply with the Privacy Shield Principles, will be actionable as a deceptive practice under Section 5 of the FTC Act or other similar statute.
 - d. An organization that wishes its Privacy Shield benefits to cover human resources data transferred from the EU in the context of the employment relationship must commit to cooperate with the DPAs with regard to such data (*see* Supplemental Principle on Human Resources Data).
 - e. Organizations choosing this option will be required to pay an annual fee which will be designed to cover the operating costs of the panel, and they may additionally be asked to meet any necessary translation expenses arising out of the panel's consideration of referrals or complaints against them. The annual fee will not exceed USD 500 and will be less for smaller companies.

6. Self-Certification

- a. Privacy Shield benefits are assured from the date on which the Department has placed the organization's self-certification submission on the Privacy Shield List after having determined that the submission is complete.
- b. To self-certify for the Privacy Shield, an organization must provide to the Department a self-certification submission, signed by a corporate officer on behalf of the organization that is joining the Privacy Shield, that contains at least the following information:
 - i. name of organization, mailing address, e-mail address, telephone, and fax numbers;
 - ii. description of the activities of the organization with respect to personal information received from the EU; and

- iii. description of the organization's privacy policy for such personal information, including:
 - 1. if the organization has a public website, the relevant web address where the privacy policy is available, or if the organization does not have a public website, where the privacy policy is available for viewing by the public;
 - 2. its effective date of implementation;
 - 3. a contact office for the handling of complaints, access requests, and any other issues arising under the Privacy Shield;
 - 4. the specific statutory body that has jurisdiction to hear any claims against the organization regarding possible unfair or deceptive practices and violations of laws or regulations governing privacy (and that is listed in the Principles or a future annex to the Principles);
 - 5. name of any privacy program in which the organization is a member;
 - 6. method of verification (*e.g.*, in-house, third party) (*see* Supplemental Principle on Verification); and
 - 7. the independent recourse mechanism that is available to investigate unresolved complaints.

- c. Where the organization wishes its Privacy Shield benefits to cover human resources information transferred from the EU for use in the context of the employment relationship, it may do so where a statutory body listed in the Principles or a future annex to the Principles has jurisdiction to hear claims against the organization arising out of the processing of human resources information. In addition, the organization must indicate this in its self-certification submission and declare its commitment to cooperate with the EU authority or authorities concerned in conformity with the Supplemental Principles on Human Resources Data and the Role of the Data Protection Authorities as applicable and that it will comply with the advice given by such authorities. The organization must also provide the Department with a copy of its human resources privacy policy and provide information where the privacy policy is available for viewing by its affected employees.

- d. The Department will maintain the Privacy Shield List of organizations that file completed self-certification submissions, thereby assuring the availability of Privacy Shield benefits, and will update such list on the basis of annual self-recertification submissions and notifications received pursuant to the Supplemental Principle on Dispute Resolution and Enforcement. Such self-certification submissions must be provided not less than annually; otherwise the organization will be removed from the Privacy Shield List and Privacy Shield benefits will

no longer be assured. Both the Privacy Shield List and the self-certification submissions by the organizations will be made publicly available. All organizations that are placed on the Privacy Shield List by the Department must also state in their relevant published privacy policy statements that they adhere to the Privacy Shield Principles. If available online, an organization's privacy policy must include a hyperlink to the Department's Privacy Shield website and a hyperlink to the website or complaint submission form of the independent recourse mechanism that is available to investigate unresolved complaints.

- e. The Privacy Principles apply immediately upon certification. Recognizing that the Principles will impact commercial relationships with third parties, organizations that certify to the Privacy Shield Framework in the first two months following the Framework's effective date shall bring existing commercial relationships with third parties into conformity with the Accountability for Onward Transfer Principle as soon as possible, and in any event no later than nine months from the date upon which they certify to the Privacy Shield. During that interim period, where organizations transfer data to a third party, they shall (i) apply the Notice and Choice Principles, and (ii) where personal data is transferred to a third party acting as an agent, ascertain that the agent is obligated to provide at least the same level of protection as is required by the Principles.
- f. An organization must subject to the Privacy Shield Principles all personal data received from the EU in reliance upon the Privacy Shield. The undertaking to adhere to the Privacy Shield Principles is not time-limited in respect of personal data received during the period in which the organization enjoys the benefits of the Privacy Shield. Its undertaking means that it will continue to apply the Principles to such data for as long as the organization stores, uses or discloses them, even if it subsequently leaves the Privacy Shield for any reason. An organization that withdraws from the Privacy Shield but wants to retain such data must affirm to the Department on an annual basis its commitment to continue to apply the Principles or provide "adequate" protection for the information by another authorized means (for example, using a contract that fully reflects the requirements of the relevant standard contractual clauses adopted by the European Commission); otherwise, the organization must return or delete the information. An organization that withdraws from the Privacy Shield must remove from any relevant privacy policy any references to the Privacy Shield that imply that the organization continues to actively participate in the Privacy Shield and is entitled to its benefits.
- g. An organization that will cease to exist as a separate legal entity as a result of a merger or a takeover must notify the Department of this in advance. The notification should also indicate whether the acquiring entity or the entity resulting from the merger will (i) continue to be bound by the Privacy Shield Principles by the operation of law governing the takeover or merger or (ii) elect to self-certify its

adherence to the Privacy Shield Principles or put in place other safeguards, such as a written agreement that will ensure adherence to the Privacy Shield Principles. Where neither (i) nor (ii) applies, any personal data that has been acquired under the Privacy Shield must be promptly deleted.

- h. When an organization leaves the Privacy Shield for any reason, it must remove all statements implying that the organization continues to participate in the Privacy Shield or is entitled to the benefits of the Privacy Shield. The EU-U.S. Privacy Shield certification mark, if used, must also be removed. Any misrepresentation to the general public concerning an organization's adherence to the Privacy Shield Principles may be actionable by the FTC or other relevant government body. Misrepresentations to the Department may be actionable under the False Statements Act (18 U.S.C. § 1001).

7. Verification

- a. Organizations must provide follow up procedures for verifying that the attestations and assertions they make about their Privacy Shield privacy practices are true and those privacy practices have been implemented as represented and in accordance with the Privacy Shield Principles.
- b. To meet the verification requirements of the Recourse, Enforcement and Liability Principle, an organization must verify such attestations and assertions either through self-assessment or outside compliance reviews.
- c. Under the self-assessment approach, such verification must indicate that an organization's published privacy policy regarding personal information received from the EU is accurate, comprehensive, prominently displayed, completely implemented and accessible. It must also indicate that its privacy policy conforms to the Privacy Shield Principles; that individuals are informed of any in-house arrangements for handling complaints and of the independent mechanisms through which they may pursue complaints; that it has in place procedures for training employees in its implementation, and disciplining them for failure to follow it; and that it has in place internal procedures for periodically conducting objective reviews of compliance with the above. A statement verifying the self-assessment must be signed by a corporate officer or other authorized representative of the organization at least once a year and made available upon request by individuals or in the context of an investigation or a complaint about non-compliance.
- d. Where the organization has chosen outside compliance review, such a review must demonstrate that its privacy policy regarding personal information received from the EU conforms to the Privacy Shield Principles, that it is being complied with, and that individuals are informed of the mechanisms through which they may pursue complaints. The methods of review may include, without limitation,

auditing, random reviews, use of “decoys”, or use of technology tools as appropriate. A statement verifying that an outside compliance review has been successfully completed must be signed either by the reviewer or by the corporate officer or other authorized representative of the organization at least once a year and made available upon request by individuals or in the context of an investigation or a complaint about compliance.

- e. Organizations must retain their records on the implementation of their Privacy Shield privacy practices and make them available upon request in the context of an investigation or a complaint about non-compliance to the independent body responsible for investigating complaints or to the agency with unfair and deceptive practices jurisdiction. Organizations must also respond promptly to inquiries and other requests for information from the Department relating to the organization’s adherence to the Principles.

8. Access

a. The Access Principle in Practice

- i. Under the Privacy Shield Principles, the right of access is fundamental to privacy protection. In particular, it allows individuals to verify the accuracy of information held about them. The Access Principle means that individuals have the right to:
 - 1. obtain from an organization confirmation of whether or not the organization is processing personal data relating to them;¹
 - 2. have communicated to them such data so that they could verify its accuracy and the lawfulness of the processing; and
 - 3. have the data corrected, amended or deleted where it is inaccurate or processed in violation of the Principles.
- ii. Individuals do not have to justify requests for access to their personal data. In responding to individuals’ access requests, organizations should first be guided by the concern(s) that led to the requests in the first place. For example, if an access request is vague or broad in scope, an organization may engage the individual in a dialogue so as to better understand the motivation for the request and to locate responsive information. The organization might inquire about which part(s) of the organization the individual interacted with or about the nature

¹ The organization should answer requests from an individual concerning the purposes of the processing, the categories of personal data concerned, and the recipients or categories of recipients to whom the personal data is disclosed.

of the information or its use that is the subject of the access request.

- iii. Consistent with the fundamental nature of access, organizations should always make good faith efforts to provide access. For example, where certain information needs to be protected and can be readily separated from other personal information subject to an access request, the organization should redact the protected information and make available the other information. If an organization determines that access should be restricted in any particular instance, it should provide the individual requesting access with an explanation of why it has made that determination and a contact point for any further inquiries.

b. Burden or Expense of Providing Access

- i. The right of access to personal data may be restricted in exceptional circumstances where the legitimate rights of persons other than the individual would be violated or where the burden or expense of providing access would be disproportionate to the risks to the individual's privacy in the case in question. Expense and burden are important factors and should be taken into account but they are not controlling factors in determining whether providing access is reasonable.
- ii. For example, if the personal information is used for decisions that will significantly affect the individual (*e.g.*, the denial or grant of important benefits, such as insurance, a mortgage, or a job), then consistent with the other provisions of these Supplemental Principles, the organization would have to disclose that information even if it is relatively difficult or expensive to provide. If the personal information requested is not sensitive or not used for decisions that will significantly affect the individual, but is readily available and inexpensive to provide, an organization would have to provide access to such information.

c. Confidential Commercial Information

- i. Confidential commercial information is information that an organization has taken steps to protect from disclosure, where disclosure would help a competitor in the market. Organizations may deny or limit access to the extent that granting full access would reveal its own confidential commercial information, such as marketing inferences or classifications generated by the organization, or the confidential commercial information of another that is subject to a contractual obligation of confidentiality.
- ii. Where confidential commercial information can be readily separated from other personal information subject to an access

request, the organization should redact the confidential commercial information and make available the non-confidential information.

d. Organization of Data Bases

- i. Access can be provided in the form of disclosure of the relevant personal information by an organization to the individual and does not require access by the individual to an organization's data base.
- ii. Access needs to be provided only to the extent that an organization stores the personal information. The Access Principle does not itself create any obligation to retain, maintain, reorganize, or restructure personal information files.

e. When Access May be Restricted

- i. As organizations must always make good faith efforts to provide individuals with access to their personal data, the circumstances in which organizations may restrict such access are limited, and any reasons for restricting access must be specific. As under the Directive, an organization can restrict access to information to the extent that disclosure is likely to interfere with the safeguarding of important countervailing public interests, such as national security; defense; or public security. In addition, where personal information is processed solely for research or statistical purposes, access may be denied. Other reasons for denying or limiting access are:
 1. interference with the execution or enforcement of the law or with private causes of action, including the prevention, investigation or detection of offenses or the right to a fair trial;
 2. disclosure where the legitimate rights or important interests of others would be violated;
 3. breaching a legal or other professional privilege or obligation;
 4. prejudicing employee security investigations or grievance proceedings or in connection with employee succession planning and corporate re-organizations; or
 5. prejudicing the confidentiality necessary in monitoring, inspection or regulatory functions connected with sound management, or in future or ongoing negotiations involving the organization.
- ii. An organization which claims an exception has the burden of demonstrating its necessity, and the reasons for restricting access and a contact point for further inquiries should be given to individuals.

- f. Right to Obtain Confirmation and Charging a Fee to Cover the Costs for Providing Access
 - i. An individual has the right to obtain confirmation of whether or not this organization has personal data relating to him or her. An individual also has the right to have communicated to him or her personal data relating to him or her. An organization may charge a fee that is not excessive.
 - ii. Charging a fee may be justified, for example, where requests for access are manifestly excessive, in particular because of their repetitive character.
 - iii. Access may not be refused on cost grounds if the individual offers to pay the costs.
- g. Repetitious or Vexatious Requests for Access
 - i. An organization may set reasonable limits on the number of times within a given period that access requests from a particular individual will be met. In setting such limitations, an organization should consider such factors as the frequency with which information is updated, the purpose for which the data are used, and the nature of the information.
- h. Fraudulent Requests for Access
 - i. An organization is not required to provide access unless it is supplied with sufficient information to allow it to confirm the identity of the person making the request.
- i. Timeframe for Responses
 - i. Organizations should respond to access requests within a reasonable time period, in a reasonable manner, and in a form that is readily intelligible to the individual. An organization that provides information to data subjects at regular intervals may satisfy an individual access request with its regular disclosure if it would not constitute an excessive delay.

9. **Human Resources Data**

- a. Coverage by the Privacy Shield
 - i. Where an organization in the EU transfers personal information about its employees (past or present) collected in the context of the employment relationship, to a parent, affiliate, or unaffiliated service provider in the United States participating in the Privacy Shield, the transfer enjoys the benefits of the Privacy Shield. In such cases, the collection of the information and its processing prior to transfer will have been subject to the national laws of the EU country where it was collected, and any conditions for or restrictions on its transfer according to those laws will have to be respected.

- ii. The Privacy Shield Principles are relevant only when individually identified records are transferred or accessed. Statistical reporting relying on aggregate employment data and containing no personal data or the use of anonymized data does not raise privacy concerns.
- b. Application of the Notice and Choice Principles
- i. A U.S. organization that has received employee information from the EU under the Privacy Shield may disclose it to third parties or use it for different purposes only in accordance with the Notice and Choice Principles. For example, where an organization intends to use personal information collected through the employment relationship for non-employment-related purposes, such as marketing communications, the U.S. organization must provide the affected individuals with the requisite choice before doing so, unless they have already authorized the use of the information for such purposes. Moreover, such choices must not be used to restrict employment opportunities or take any punitive action against such employees.
 - ii. It should be noted that certain generally applicable conditions for transfer from some EU Member States may preclude other uses of such information even after transfer outside the EU and such conditions will have to be respected.
 - iii. In addition, employers should make reasonable efforts to accommodate employee privacy preferences. This could include, for example, restricting access to the personal data, anonymizing certain data, or assigning codes or pseudonyms when the actual names are not required for the management purpose at hand.
 - iv. To the extent and for the period necessary to avoid prejudicing the ability of the organization in making promotions, appointments, or other similar employment decisions, an organization does not need to offer notice and choice.
- c. Application of the Access Principle
- i. The Supplemental Principle on Access provides guidance on reasons which may justify denying or limiting access on request in the human resources context. Of course, employers in the European Union must comply with local regulations and ensure that European Union employees have access to such information as is required by law in their home countries, regardless of the location of data processing and storage. The Privacy Shield requires that an organization processing such data in the United States will cooperate in providing such access either directly or through the EU employer.
- d. Enforcement

- i. In so far as personal information is used only in the context of the employment relationship, primary responsibility for the data vis-à-vis the employee remains with the organization in the EU. It follows that, where European employees make complaints about violations of their data protection rights and are not satisfied with the results of internal review, complaint, and appeal procedures (or any applicable grievance procedures under a contract with a trade union), they should be directed to the state or national data protection or labor authority in the jurisdiction where the employees work. This includes cases where the alleged mishandling of their personal information is the responsibility of the U.S. organization that has received the information from the employer and thus involves an alleged breach of the Privacy Shield Principles. This will be the most efficient way to address the often overlapping rights and obligations imposed by local labor law and labor agreements as well as data protection law.
 - ii. A U.S. organization participating in the Privacy Shield that uses EU human resources data transferred from the European Union in the context of the employment relationship and that wishes such transfers to be covered by the Privacy Shield must therefore commit to cooperate in investigations by and to comply with the advice of competent EU authorities in such cases.
 - e. Application of the Accountability for Onward Transfer Principle
 - i. For occasional employment-related operational needs of the Privacy Shield organization with respect to personal data transferred under the Privacy Shield, such as the booking of a flight, hotel room, or insurance coverage, transfers of personal data of a small number of employees can take place to controllers without application of the Access Principle or entering into a contract with the third-party controller, as otherwise required under the Accountability for Onward Transfer Principle, provided that the Privacy Shield organization has complied with the Notice and Choice Principles.

10. Obligatory Contracts for Onward Transfers

- a. Data Processing Contracts
 - i. When personal data is transferred from the EU to the United States only for processing purposes, a contract will be required, regardless of participation by the processor in the Privacy Shield.
 - ii. Data controllers in the European Union are always required to enter into a contract when a transfer for mere processing is made, whether the processing operation is carried out inside or outside the EU, and whether or not the processor participates in

the Privacy Shield. The purpose of the contract is to make sure that the processor:

1. acts only on instructions from the controller;
 2. provides appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, and understands whether onward transfer is allowed; and
 3. taking into account the nature of the processing, assists the controller in responding to individuals exercising their rights under the Principles.
- iii. Because adequate protection is provided by Privacy Shield participants, contracts with Privacy Shield participants for mere processing do not require prior authorization (or such authorization will be granted automatically by the EU Member States), as would be required for contracts with recipients not participating in the Privacy Shield or otherwise not providing adequate protection.
- b. Transfers within a Controlled Group of Corporations or Entities
- i. When personal information is transferred between two controllers within a controlled group of corporations or entities, a contract is not always required under the Accountability for Onward Transfer Principle. Data controllers within a controlled group of corporations or entities may base such transfers on other instruments, such as EU Binding Corporate Rules or other intra-group instruments (e.g., compliance and control programs), ensuring the continuity of protection of personal information under the Privacy Shield Principles. In case of such transfers, the Privacy Shield organization remains responsible for compliance with Privacy Shield Principles.
- c. Transfers between Controllers
- i. For transfers between controllers, the recipient controller need not be a Privacy Shield organization or have an independent recourse mechanism. The Privacy Shield organization must enter into a contract with the recipient third-party controller that provides for the same level of protection as is available under the Privacy Shield, not including the requirement that the third party controller be a Privacy Shield organization or have an independent recourse mechanism, provided it makes available an equivalent mechanism.

11. Dispute Resolution and Enforcement

- a. The Recourse, Enforcement and Liability Principle sets out the requirements for Privacy Shield enforcement. How to meet the requirements of point (a)(ii) of the Principle is set out in the

Supplemental Principle on Verification. This Supplemental Principle addresses points (a)(i) and (a)(iii), both of which require independent recourse mechanisms. These mechanisms may take different forms, but they must meet the Recourse, Enforcement and Liability Principle's requirements. Organizations satisfy the requirements through the following: (i) compliance with private sector developed privacy programs that incorporate the Privacy Shield Principles into their rules and that include effective enforcement mechanisms of the type described in the Recourse, Enforcement and Liability Principle; (ii) compliance with legal or regulatory supervisory authorities that provide for handling of individual complaints and dispute resolution; or (iii) commitment to cooperate with data protection authorities located in the European Union or their authorized representatives.

- b. This list is intended to be illustrative and not limiting. The private sector may design additional mechanisms to provide enforcement, so long as they meet the requirements of the Recourse, Enforcement and Liability Principle and the Supplemental Principles. Please note that the Recourse, Enforcement and Liability Principle's requirements are additional to the requirement that self-regulatory efforts must be enforceable under Section 5 of the Federal Trade Commission Act, which prohibits unfair and deceptive acts, or another law or regulation prohibiting such acts.
- c. In order to help ensure compliance with their Privacy Shield commitments and to support the administration of the program, organizations, as well as their independent recourse mechanisms, must provide information relating to the Privacy Shield when requested by the Department. In addition, organizations must respond expeditiously to complaints regarding their compliance with the Principles referred through the Department by DPAs. The response should address whether the complaint has merit and, if so, how the organization will rectify the problem. The Department will protect the confidentiality of information it receives in accordance with U.S. law.
- d. Recourse Mechanisms
 - i. Consumers should be encouraged to raise any complaints they may have with the relevant organization before proceeding to independent recourse mechanisms. Organizations must respond to a consumer within 45 days of receiving a complaint. Whether a recourse mechanism is independent is a factual question that can be demonstrated notably by impartiality, transparent composition and financing, and a proven track record. As required by the Recourse, Enforcement and Liability Principle, the recourse available to individuals must be readily available and free of charge to individuals. Dispute resolution bodies should look into each complaint received from individuals unless they are obviously unfounded or frivolous. This does not preclude the establishment of eligibility requirements by the organization operating the recourse mechanism, but such requirements should be

transparent and justified (for example, to exclude complaints that fall outside the scope of the program or are for consideration in another forum), and should not have the effect of undermining the commitment to look into legitimate complaints. In addition, recourse mechanisms should provide individuals with full and readily available information about how the dispute resolution procedure works when they file a complaint. Such information should include notice about the mechanism's privacy practices, in conformity with the Privacy Shield Principles. They should also cooperate in the development of tools such as standard complaint forms to facilitate the complaint resolution process.

- ii. Independent recourse mechanisms must include on their public websites information regarding the Privacy Shield Principles and the services that they provide under the Privacy Shield. This information must include: (1) information on or a link to the Privacy Shield Principles' requirements for independent recourse mechanisms; (2) a link to the Department's Privacy Shield website; (3) an explanation that their dispute resolution services under the Privacy Shield are free of charge to individuals; (4) a description of how a Privacy Shield-related complaint can be filed; (5) the timeframe in which Privacy Shield-related complaints are processed; and (6) a description of the range of potential remedies.
- iii. Independent recourse mechanisms must publish an annual report providing aggregate statistics regarding their dispute resolution services. The annual report must include: (1) the total number of Privacy Shield-related complaints received during the reporting year; (2) the types of complaints received; (3) dispute resolution quality measures, such as the length of time taken to process complaints; and (4) the outcomes of the complaints received, notably the number and types of remedies or sanctions imposed.
- iv. As set forth in Annex I, an arbitration option is available to an individual to determine, for residual claims, whether a Privacy Shield organization has violated its obligations under the Principles as to that individual, and whether any such violation remains fully or partially unremedied. This option is available only for these purposes. This option is not available, for example, with respect to the exceptions to the Principles² or with respect to an allegation about the adequacy of the Privacy Shield. Under this arbitration option, the Privacy Shield Panel (consisting of one or three arbitrators, as agreed by the parties) has the authority to impose individual-specific, non-monetary equitable relief (such as access, correction, deletion, or return

² Section I.5 of the Principles.

of the individual's data in question) necessary to remedy the violation of the Principles only with respect to the individual. Individuals and Privacy Shield organizations will be able to seek judicial review and enforcement of the arbitral decisions pursuant to U.S. law under the Federal Arbitration Act.

e. Remedies and Sanctions

- i. The result of any remedies provided by the dispute resolution body should be that the effects of non-compliance are reversed or corrected by the organization, insofar as feasible, and that future processing by the organization will be in conformity with the Principles and, where appropriate, that processing of the personal data of the individual who brought the complaint will cease. Sanctions need to be rigorous enough to ensure compliance by the organization with the Principles. A range of sanctions of varying degrees of severity will allow dispute resolution bodies to respond appropriately to varying degrees of non-compliance. Sanctions should include both publicity for findings of non-compliance and the requirement to delete data in certain circumstances.³ Other sanctions could include suspension and removal of a seal, compensation for individuals for losses incurred as a result of non-compliance and injunctive awards. Private sector dispute resolution bodies and self-regulatory bodies must notify failures of Privacy Shield organizations to comply with their rulings to the governmental body with applicable jurisdiction or to the courts, as appropriate, and to notify the Department.

f. FTC Action

- ii. The FTC has committed to reviewing on a priority basis referrals alleging non-compliance with the Principles received from: (i) privacy self-regulatory organizations and other independent dispute resolution bodies; (ii) EU Member States; and (iii) the Department, to determine whether Section 5 of the FTC Act prohibiting unfair or deceptive acts or practices in commerce has been violated. If the FTC concludes that it has reason to believe Section 5 has been violated, it may resolve the matter by seeking an administrative cease and desist order prohibiting the challenged practices or by filing a complaint in a federal district court, which if successful could result in a federal court order to same effect. This includes false claims of adherence to the Privacy Shield Principles or participation in the Privacy Shield by organizations, which either are no longer

³ Dispute resolution bodies have discretion about the circumstances in which they use these sanctions. The sensitivity of the data concerned is one factor to be taken into consideration in deciding whether deletion of data should be required, as is whether an organization has collected, used, or disclosed information in blatant contravention of the Privacy Shield Principles.

on the Privacy Shield List or have never self-certified to the Department. The FTC may obtain civil penalties for violations of an administrative cease and desist order and may pursue civil or criminal contempt for violation of a federal court order. The FTC will notify the Department of any such actions it takes. The Department encourages other government bodies to notify it of the final disposition of any such referrals or other rulings determining adherence to the Privacy Shield Principles.

g. Persistent Failure to Comply

- i. If an organization persistently fails to comply with the Principles, it is no longer entitled to benefit from the Privacy Shield. Organizations that have persistently failed to comply with the Principles will be removed from the Privacy Shield List by the Department and must return or delete the personal information they received under the Privacy Shield.
- ii. Persistent failure to comply arises where an organization that has self-certified to the Department refuses to comply with a final determination by any privacy self-regulatory, independent dispute resolution, or government body, or where such a body determines that an organization frequently fails to comply with the Principles to the point where its claim to comply is no longer credible. In these cases, the organization must promptly notify the Department of such facts. Failure to do so may be actionable under the False Statements Act (18 U.S.C. § 1001). An organization's withdrawal from a private-sector privacy self-regulatory program or independent dispute resolution mechanism does not relieve it of its obligation to comply with the Principles and would constitute a persistent failure to comply.
- iii. The Department will remove an organization from the Privacy Shield List in response to any notification it receives of persistent failure to comply, whether it is received from the organization itself, from a privacy self-regulatory body or another independent dispute resolution body, or from a government body, but only after first providing 30 days' notice and an opportunity to respond to the organization that has failed to comply. Accordingly, the Privacy Shield List maintained by the Department will make clear which organizations are assured and which organizations are no longer assured of Privacy Shield benefits.
- iv. An organization applying to participate in a self-regulatory body for the purposes of requalifying for the Privacy Shield must provide that body with full information about its prior participation in the Privacy Shield.

12. Choice – Timing of Opt Out

- a. Generally, the purpose of the Choice Principle is to ensure that personal information is used and disclosed in ways that are consistent with the individual's expectations and choices. Accordingly, an individual should be able to exercise "opt out" choice of having personal information used for direct marketing at any time subject to reasonable limits established by the organization, such as giving the organization time to make the opt out effective. An organization may also require sufficient information to confirm the identity of the individual requesting the "opt out." In the United States, individuals may be able to exercise this option through the use of a central "opt out" program such as the Direct Marketing Association's Mail Preference Service. Organizations that participate in the Direct Marketing Association's Mail Preference Service should promote its availability to consumers who do not wish to receive commercial information. In any event, an individual should be given a readily available and affordable mechanism to exercise this option.
- b. Similarly, an organization may use information for certain direct marketing purposes when it is impracticable to provide the individual with an opportunity to opt out before using the information, if the organization promptly gives the individual such opportunity at the same time (and upon request at any time) to decline (at no cost to the individual) to receive any further direct marketing communications and the organization complies with the individual's wishes.

13. Travel Information

- a. Airline passenger reservation and other travel information, such as frequent flyer or hotel reservation information and special handling needs, such as meals to meet religious requirements or physical assistance, may be transferred to organizations located outside the EU in several different circumstances. Under Article 26 of the Directive, personal data may be transferred "to a third country which does not ensure an adequate level of protection within the meaning of Article 25(2)" on the condition that it (i) is necessary to provide the services requested by the consumer or to fulfill the terms of an agreement, such as a "frequent flyer" agreement; or (ii) has been unambiguously consented to by the consumer. U.S. organizations subscribing to the Privacy Shield provide adequate protection for personal data and may therefore receive data transfers from the EU without meeting these conditions or other conditions set out in Article 26 of the Directive. Since the Privacy Shield includes specific rules for sensitive information, such information (which may need to be collected, for example, in connection with customers' needs for physical assistance) may be included in transfers to Privacy Shield participants. In all cases, however, the organization transferring the information has to respect the law in the EU Member State in which it is operating, which may inter alia impose special conditions for the handling of sensitive data.

14. **Pharmaceutical and Medical Products**

- a. Application of EU Member State Laws or the Privacy Shield Principles
 - i. EU Member State law applies to the collection of the personal data and to any processing that takes place prior to the transfer to the United States. The Privacy Shield Principles apply to the data once they have been transferred to the United States. Data used for pharmaceutical research and other purposes should be anonymized when appropriate.
- b. Future Scientific Research
 - i. Personal data developed in specific medical or pharmaceutical research studies often play a valuable role in future scientific research. Where personal data collected for one research study are transferred to a U.S. organization in the Privacy Shield, the organization may use the data for a new scientific research activity if appropriate notice and choice have been provided in the first instance. Such notice should provide information about any future specific uses of the data, such as periodic follow-up, related studies, or marketing.
 - ii. It is understood that not all future uses of the data can be specified, since a new research use could arise from new insights on the original data, new medical discoveries and advances, and public health and regulatory developments. Where appropriate, the notice should therefore include an explanation that personal data may be used in future medical and pharmaceutical research activities that are unanticipated. If the use is not consistent with the general research purpose(s) for which the personal data were originally collected, or to which the individual has consented subsequently, new consent must be obtained.
- c. Withdrawal from a Clinical Trial
 - i. Participants may decide or be asked to withdraw from a clinical trial at any time. Any personal data collected previous to withdrawal may still be processed along with other data collected as part of the clinical trial, however, if this was made clear to the participant in the notice at the time he or she agreed to participate.
- d. Transfers for Regulatory and Supervision Purposes
 - i. Pharmaceutical and medical device companies are allowed to provide personal data from clinical trials conducted in the EU to regulators in the United States for regulatory and supervision purposes. Similar transfers are allowed to parties other than regulators, such as company locations and other researchers, consistent with the Principles of Notice and Choice.

- e. “Blinded” Studies
 - i. To ensure objectivity in many clinical trials, participants, and often investigators as well, cannot be given access to information about which treatment each participant may be receiving. Doing so would jeopardize the validity of the research study and results. Participants in such clinical trials (referred to as “blinded” studies) do not have to be provided access to the data on their treatment during the trial if this restriction has been explained when the participant entered the trial and the disclosure of such information would jeopardize the integrity of the research effort.
 - ii. Agreement to participate in the trial under these conditions is a reasonable forgoing of the right of access. Following the conclusion of the trial and analysis of the results, participants should have access to their data if they request it. They should seek it primarily from the physician or other health care provider from whom they received treatment within the clinical trial, or secondarily from the sponsoring organization.
- f. Product Safety and Efficacy Monitoring
 - i. A pharmaceutical or medical device company does not have to apply the Privacy Shield Principles with respect to the Notice, Choice, Accountability for Onward Transfer, and Access Principles in its product safety and efficacy monitoring activities, including the reporting of adverse events and the tracking of patients/subjects using certain medicines or medical devices, to the extent that adherence to the Principles interferes with compliance with regulatory requirements. This is true both with respect to reports by, for example, health care providers to pharmaceutical and medical device companies, and with respect to reports by pharmaceutical and medical device companies to government agencies like the Food and Drug Administration.
- g. Key-coded Data
 - i. Invariably, research data are uniquely key-coded at their origin by the principal investigator so as not to reveal the identity of individual data subjects. Pharmaceutical companies sponsoring such research do not receive the key. The unique key code is held only by the researcher, so that he or she can identify the research subject under special circumstances (*e.g.*, if follow-up medical attention is required). A transfer from the EU to the United States of data coded in this way would not constitute a transfer of personal data that would be subject to the Privacy Shield Principles.

15. Public Record and Publicly Available Information

- a. An organization must apply the Privacy Shield Principles of Security, Data Integrity and Purpose Limitation, and Recourse, Enforcement and Liability to personal data from publicly available sources. These Principles shall apply also to personal data collected from public records, *i.e.*, those records kept by government agencies or entities at any level that are open to consultation by the public in general.
- b. It is not necessary to apply the Notice, Choice, or Accountability for Onward Transfer Principles to public record information, as long as it is not combined with non-public record information, and any conditions for consultation established by the relevant jurisdiction are respected. Also, it is generally not necessary to apply the Notice, Choice, or Accountability for Onward Transfer Principles to publicly available information unless the European transferor indicates that such information is subject to restrictions that require application of those Principles by the organization for the uses it intends. Organizations will have no liability for how such information is used by those obtaining such information from published materials.
- c. Where an organization is found to have intentionally made personal information public in contravention of the Principles so that it or others may benefit from these exceptions, it will cease to qualify for the benefits of the Privacy Shield.
- d. It is not necessary to apply the Access Principle to public record information as long as it is not combined with other personal information (apart from small amounts used to index or organize the public record information); however, any conditions for consultation established by the relevant jurisdiction are to be respected. In contrast, where public record information is combined with other non-public record information (other than as specifically noted above), an organization must provide access to all such information, assuming it is not subject to other permitted exceptions.
- e. As with public record information, it is not necessary to provide access to information that is already publicly available to the public at large, as long as it is not combined with non-publicly available information. Organizations that are in the business of selling publicly available information may charge the organization's customary fee in responding to requests for access. Alternatively, individuals may seek access to their information from the organization that originally compiled the data.

16. Access Requests by Public Authorities

- a. In order to provide transparency in respect of lawful requests by public authorities to access personal information, Privacy Shield organizations may voluntarily issue periodic transparency reports on the number of requests for personal information they receive by public

authorities for law enforcement or national security reasons, to the extent such disclosures are permissible under applicable law.

- b. The information provided by the Privacy Shield organizations in these reports together with information that has been released by the intelligence community, along with other information, can be used to inform the annual joint review of the functioning of the Privacy Shield in accordance with the Principles.
- c. Absence of notice in accordance with point (a)(xii) of the Notice Principle shall not prevent or impair an organization's ability to respond to any lawful request.

ANNEX I

This Annex I provides the terms under which Privacy Shield organizations are obligated to arbitrate claims, pursuant to the Recourse, Enforcement and Liability Principle. The binding arbitration option described below applies to certain “residual” claims as to data covered by the EU-U.S. Privacy Shield. The purpose of this option is to provide a prompt, independent, and fair mechanism, at the option of individuals, for resolution of claimed violations of the Principles not resolved by any of the other Privacy Shield mechanisms, if any.

A. Scope

This arbitration option is available to an individual to determine, for residual claims, whether a Privacy Shield organization has violated its obligations under the Principles as to that individual, and whether any such violation remains fully or partially unremedied. This option is available only for these purposes. This option is not available, for example, with respect to the exceptions to the Principles¹ or with respect to an allegation about the adequacy of the Privacy Shield.

B. Available Remedies

Under this arbitration option, the Privacy Shield Panel (consisting of one or three arbitrators, as agreed by the parties) has the authority to impose individual-specific, non-monetary equitable relief (such as access, correction, deletion, or return of the individual’s data in question) necessary to remedy the violation of the Principles only with respect to the individual. These are the only powers of the arbitration panel with respect to remedies. In considering remedies, the arbitration panel is required to consider other remedies that already have been imposed by other mechanisms under the Privacy Shield. No damages, costs, fees, or other remedies are available. Each party bears its own attorney’s fees.

C. Pre-Arbitration Requirements

An individual who decides to invoke this arbitration option must take the following steps prior to initiating an arbitration claim: (1) raise the claimed violation directly with the organization and afford the organization an opportunity to resolve the issue within the timeframe set forth in Section III.11(d)(i) of the Principles; (2) make use of the independent recourse mechanism under the Principles, which is at no cost to the individual; and (3) raise the issue through their Data Protection Authority to the Department of Commerce and afford the Department of Commerce an opportunity to use best efforts to resolve the issue within the timeframes set forth in the Letter from the International Trade Administration of the Department of Commerce, at no cost to the individual.

This arbitration option may not be invoked if the individual’s same claimed violation of the Principles (1) has previously been subject to binding arbitration; (2) was the subject of a final judgment entered in a court action to which the individual was a party; or (3) was previously settled by the parties. In addition, this option may not be invoked if an EU Data Protection

¹ Section I.5 of the Principles.

Authority (1) has authority under Sections III.5 or III.9 of the Principles; or (2) has the authority to resolve the claimed violation directly with the organization. A DPA's authority to resolve the same claim against an EU data controller does not alone preclude invocation of this arbitration option against a different legal entity not bound by the DPA authority.

D. Binding Nature of Decisions

An individual's decision to invoke this binding arbitration option is entirely voluntary. Arbitral decisions will be binding on all parties to the arbitration. Once invoked, the individual forgoes the option to seek relief for the same claimed violation in another forum, except that if non-monetary equitable relief does not fully remedy the claimed violation, the individual's invocation of arbitration will not preclude a claim for damages that is otherwise available in the courts.

E. Review and Enforcement

Individuals and Privacy Shield organizations will be able to seek judicial review and enforcement of the arbitral decisions pursuant to U.S. law under the Federal Arbitration Act.² Any such cases must be brought in the federal district court whose territorial coverage includes the primary place of business of the Privacy Shield organization.

² Chapter 2 of the Federal Arbitration Act ("FAA") provides that "[a]n arbitration agreement or arbitral award arising out of a legal relationship, whether contractual or not, which is considered as commercial, including a transaction, contract, or agreement described in [section 2 of the FAA], falls under the Convention [on the Recognition and Enforcement of Foreign Arbitral Awards of June 10, 1958, 21 U.S.T. 2519, T.I.A.S. No. 6997 ("New York Convention")." 9 U.S.C. § 202. The FAA further provides that "[a]n agreement or award arising out of such a relationship which is entirely between citizens of the United States shall be deemed not to fall under the [New York] Convention unless that relationship involves property located abroad, envisages performance or enforcement abroad, or has some other reasonable relation with one or more foreign states." *Id.* Under Chapter 2, "any party to the arbitration may apply to any court having jurisdiction under this chapter for an order confirming the award as against any other party to the arbitration. The court shall confirm the award unless it finds one of the grounds for refusal or deferral of recognition or enforcement of the award specified in the said [New York] Convention." *Id.* § 207. Chapter 2 further provides that "[t]he district courts of the United States . . . shall have original jurisdiction over . . . an action or proceeding [under the New York Convention], regardless of the amount in controversy." *Id.* § 203.

Chapter 2 also provides that "Chapter 1 applies to actions and proceedings brought under this chapter to the extent that chapter is not in conflict with this chapter or the [New York] Convention as ratified by the United States." *Id.* § 208. Chapter 1, in turn, provides that "[a] written provision in . . . a contract evidencing a transaction involving commerce to settle by arbitration a controversy thereafter arising out of such contract or transaction, or the refusal to perform the whole or any part thereof, or an agreement in writing to submit to arbitration an existing controversy arising out of such a contract, transaction, or refusal, shall be valid, irrevocable, and enforceable, save upon such grounds as exist at law or in equity for the revocation of any contract." *Id.* § 2. Chapter 1 further provides that "any party to the arbitration may apply to the court so specified for an order confirming the award, and thereupon the court must grant such an order unless the award is vacated, modified, or corrected as prescribed in sections 10 and 11 of [the FAA]." *Id.* § 9.

This arbitration option is intended to resolve individual disputes, and arbitral decisions are not intended to function as persuasive or binding precedent in matters involving other parties, including in future arbitrations or in EU or U.S. courts, or FTC proceedings.

F. The Arbitration Panel

The parties will select the arbitrators from the list of arbitrators discussed below.

Consistent with applicable law, the U.S. Department of Commerce and the European Commission will develop a list of at least 20 arbitrators, chosen on the basis of independence, integrity, and expertise. The following shall apply in connection with this process:

Arbitrators:

- (1) will remain on the list for a period of 3 years, absent exceptional circumstances or for cause, renewable for one additional period of 3 years;
- (2) shall not be subject to any instructions from, or be affiliated with, either party, or any Privacy Shield organization, or the U.S., EU, or any EU Member State or any other governmental authority, public authority, or enforcement authority; and
- (3) must be admitted to practice law in the U.S. and be experts in U.S. privacy law, with expertise in EU data protection law.

G. Arbitration Procedures

Consistent with applicable law, within 6 months from the adoption of the adequacy decision, the Department of Commerce and the European Commission will agree to adopt an existing, well-established set of U.S. arbitral procedures (such as AAA or JAMS) to govern proceedings before the Privacy Shield Panel, subject to each of the following considerations:

1. An individual may initiate binding arbitration, subject to the pre-arbitration requirements provision above, by delivering a "Notice" to the organization. The Notice shall contain a summary of steps taken under Paragraph C to resolve the claim, a description of the alleged violation, and, at the choice of the individual, any supporting documents and materials and/or a discussion of law relating to the alleged claim.
2. Procedures will be developed to ensure that an individual's same claimed violation does not receive duplicative remedies or procedures.
3. FTC action may proceed in parallel with arbitration.
4. No representative of the U.S., EU, or any EU Member State or any other governmental authority, public authority, or enforcement authority may participate in these arbitrations, provided, that at the request of an EU individual, EU DPAs may provide assistance in the preparation only of the Notice but EU DPAs may not have access to discovery or any other materials related to these arbitrations.
5. The location of the arbitration will be the United States, and the individual may choose video or telephone participation, which will be provided at no cost to the individual. In-person participation will not be required.

6. The language of the arbitration will be English unless otherwise agreed by the parties. Upon a reasoned request, and taking into account whether the individual is represented by an attorney, interpretation at the arbitral hearing as well as translation of arbitral materials will be provided at no cost to the individual, unless the panel finds that, under the circumstances of the specific arbitration, this would lead to unjustified or disproportionate costs.
7. Materials submitted to arbitrators will be treated confidentially and will only be used in connection with the arbitration.
8. Individual-specific discovery may be permitted if necessary, and such discovery will be treated confidentially by the parties and will only be used in connection with the arbitration.
9. Arbitrations should be completed within 90 days of the delivery of the Notice to the organization at issue, unless otherwise agreed to by the parties.

H. Costs

Arbitrators should take reasonable steps to minimize the costs or fees of the arbitrations.

Subject to applicable law, the Department of Commerce will facilitate the establishment of a fund, into which Privacy Shield organizations will be required to pay an annual contribution, based in part on the size of the organization, which will cover the arbitral cost, including arbitrator fees, up to maximum amounts (“caps”), in consultation with the European Commission. The fund will be managed by a third party, which will report regularly on the operations of the fund. At the annual review, the Department of Commerce and European Commission will review the operation of the fund, including the need to adjust the amount of the contributions or of the caps, and will consider, among other things, the number of arbitrations and the costs and timing of the arbitrations, with the mutual understanding that there will be no excessive financial burden imposed on Privacy Shield organizations. Attorney’s fees are not covered by this provision or any fund under this provision.

ANNEX III

THE SECRETARY OF STATE
WASHINGTON

February 22, 2016

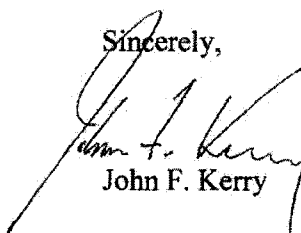
Dear Commissioner Jourová,

I am pleased we have reached an understanding on the European Union-United States Privacy Shield that will include an Ombudsperson mechanism through which authorities in the EU will be able to submit requests on behalf of EU individuals regarding U.S. signals intelligence practices.

On January 17, 2014, President Barack Obama announced important intelligence reforms included in Presidential Policy Directive 28 (PPD-28). Under PPD-28, I designated Under Secretary of State Catherine A. Novelli, who also serves as Senior Coordinator for International Information Technology Diplomacy, as our point of contact for foreign governments that wish to raise concerns regarding U.S. signals intelligence activities. Building on this role, I have established a Privacy Shield Ombudsperson mechanism in accordance with the terms set out in Annex A. I have directed Under Secretary Novelli to perform this function. Under Secretary Novelli is independent from the U.S. intelligence community, and reports directly to me.

I have directed my staff to devote the necessary resources to implement this new Ombudsperson mechanism, and am confident it will be an effective means to address EU individuals' concerns.

Sincerely,



John F. Kerry

EU-U.S. PRIVACY SHIELD OMBUDSPERSON MECHANISM REGARDING SIGNALS INTELLIGENCE

In recognition of the importance of the EU-U.S. Privacy Shield Framework, this Memorandum sets forth the process for implementing a new mechanism, consistent with Presidential Policy Directive 28 (PPD-28), regarding signals intelligence.

On January 17, 2014, President Obama gave a speech announcing important intelligence reforms. In that speech, he pointed out that “[o]ur efforts help protect not only our nation, but our friends and allies as well. Our efforts will only be effective if ordinary citizens in other countries have confidence that the United States respects their privacy too.” President Obama announced the issuance of a new presidential directive—PPD-28—to “clearly prescribe what we do, and do not do, when it comes to our overseas surveillance.”

Section 4(d) of PPD-28 directs the Secretary of State to designate a “Senior Coordinator for International Information Technology Diplomacy” (Senior Coordinator) “to ... serve as a point of contact for foreign governments who wish to raise concerns regarding signals intelligence activities conducted by the United States.” As of January 2015, Under Secretary C. Novelli has served as the Senior Coordinator.

This Memorandum describes a new mechanism that the Senior Coordinator will follow to facilitate the processing of requests relating to national security access to data transmitted from the EU to the United States pursuant to the Privacy Shield, standard contractual clauses (SCCs), binding corporate rules (BCRs), “Derogations,”¹ or “Possible Future Derogations,”² through

¹ “Derogations” in this context mean a commercial transfer or transfers that take place on the condition that: (a) the data subject has given his consent unambiguously to the proposed transfer; or (b) the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of precontractual measures taken in response to the data subject’s request; or (c) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and a third party; or (d) the transfer is necessary or legally required on important public interest grounds, or for the establishment, exercise or defense of legal claims; or (e) the transfer is necessary in order to protect the vital interests of the data subject; or (f) the transfer is made from a register which according to laws or regulations is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate legitimate interest, to the extent that the conditions laid down in law for consultation are fulfilled in the particular case.

² “Possible Future Derogations” in this context mean a commercial transfer or transfers that take place on one of the following conditions, to the extent the condition constitutes lawful grounds for transfers of personal data from the EU to the U.S.: (a) the data subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate

established avenues under applicable United States laws and policy, and the response to those requests.

1. **The Privacy Shield Ombudsperson.** The Senior Coordinator will serve as the Privacy Shield Ombudsperson and designate additional State Department officials, as appropriate to assist in her performance of the responsibilities detailed in this memorandum. (Hereinafter, the Coordinator and any officials performing such duties will be referred to as “Privacy Shield Ombudsperson.”) The Privacy Shield Ombudsperson will work closely with appropriate officials from other departments and agencies who are responsible for processing requests in accordance with applicable United States law and policy. The Under Secretary reports directly to the Secretary of State, and is independent from the Intelligence Community.
2. **Effective Coordination.** The Privacy Shield Ombudsperson will be able to effectively use and coordinate with the mechanisms and officials described below, in order to ensure appropriate response to communications from submitting EU individual complaint handling body.
 - a. The Privacy Shield Ombudsperson will work closely with other United States Government officials, including appropriate independent oversight bodies, to ensure that completed requests are processed and resolved in accordance with applicable laws and policies. In particular, the Privacy Shield Ombudsperson will be able to coordinate closely with the Office of the Director of National Intelligence, the Department of Justice, and other departments and agencies involved in United States national security as appropriate, and Inspectors General, Freedom of Information Act Officers, and Civil Liberties and Privacy Officers.
 - b. The United States Government will rely on mechanisms for coordinating and overseeing national security matters across departments and agencies to help ensure that the Privacy Shield Ombudsperson is able to respond within the meaning of Section 4(e) to completed requests under Section 3(b).
 - c. The Privacy Shield Ombudsperson may refer matters related to requests to the Privacy and Civil Liberties Oversight Board for its consideration.

safeguards; or (b) the transfer is necessary in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent; or (c) where a transfer to a third country or an international organization may take place only if the transfer is not repetitive, concerns only a limited number of data subjects, is necessary for the purposes of compelling legitimate interests pursued by the controller which are not overridden by the interests or rights and freedoms of the data subject, where the controller has assessed all the circumstances surrounding the data transfer and based on this assessment adduced suitable safeguards with respect to the protection of personal data.

3. Submitting Requests.

- a. A request will initially be submitted to the Member States bodies competent for the oversight of national security services. The EU reserves the possibility to designate a centralized EU individual complaint handling body to which a request can also be submitted (hereafter together or alternatively: the “EU individual complaint handling body”).
- b. The EU individual complaint handling body will ensure, in compliance with the following actions, that the request is complete:
 - (i) Verifying the identity of the individual, and that the individual is acting on his/her own behalf, and not as a representative of a governmental or intergovernmental organization.
 - (ii) Ensuring the request is made in writing, and that it contains the following basic information:
 - any information that forms the basis for the request,
 - the nature of information or relief sought,
 - the United States Government entities believed to be involved, if any, and
 - the other measures pursued to obtain the information or relief requested and the response received through those other measures.
 - (iii) Verifying that the request pertains to data reasonably believed to have been transferred from the EU to the United States pursuant to the Privacy Shield, SCCs, BCRs, Derogations, or Possible Future Derogations.
 - (iv) Making an initial determination that the request is not frivolous, vexatious, or made in bad faith.
- c. To be completed for purposes of further handling by the Privacy Shield Ombudsperson under this memorandum, the request need not demonstrate that the requester’s data has in fact been accessed by the United States Government through signal intelligence activities.

4. Commitments to Communicate with Submitting EU Individual Complaint Handling Body.

- a. The Privacy Shield Ombudsperson will acknowledge receipt of the request to the submitting EU individual complaint handling body.
- b. The Privacy Shield Ombudsperson will conduct an initial review to verify that the request has been completed in conformance with Section 3(b). If the Privacy Shield Ombudsperson notes any deficiencies or has any questions regarding the completion of the request, the Privacy Shield Ombudsperson will seek to address and resolve those concerns with the submitting EU individual complaint handling body.

- c. If, to facilitate appropriate processing of the request, the Privacy Shield Ombudsperson needs more information about the request, or if specific action is needed to be taken by the individual who originally submitted the request, the Privacy Shield Ombudsperson will so inform the submitting EU individual complaint handling body.
 - d. The Privacy Shield Ombudsperson will track the status of requests and provide updates as appropriate to the submitting EU individual complaint handling body.
 - e. Once a request has been completed as described in Section 3 of this Memorandum, the Privacy Shield Ombudsperson will provide in a timely manner an appropriate response to the submitting EU individual complaint handling body, subject to the continuing obligation to protect information under applicable laws and policies. The Privacy Shield Ombudsperson will provide a response to the submitting EU individual complaint handling body confirming (i) that the complaint has been properly investigated, and (ii) that the U.S. law, statutes, executive orders, presidential directives, and agency policies, providing the limitations and safeguards described in the ODNI letter, have been complied with, or, in the event of non-compliance, such non-compliance has been remedied. The Privacy Shield Ombudsperson will neither confirm nor deny whether the individual has been the target of surveillance nor will the Privacy Shield Ombudsperson confirm the specific remedy that was applied. As further explained in Section 5, FOIA requests will be processed as provided under that statute and applicable regulations.
 - f. The Privacy Shield Ombudsperson will communicate directly with the EU individual complaint handling body, who will in turn be responsible for communicating with the individual submitting the request. If direct communications are part of one of the underlying processes described below, then those communications will take place in accordance with existing procedures.
 - g. Commitments in this Memorandum will not apply to general claims that the EU-U.S. Privacy Shield is inconsistent with European Union data protection requirements. The commitments in this Memorandum are made based on the common understanding by the European Commission and the U.S. government that given the scope of commitments under this mechanism, there may be resource constraints that arise, including with respect to Freedom of Information Act (FOIA) requests. Should the carrying-out of the Privacy Shield Ombudsperson's functions exceed reasonable resource constraints and impede the fulfillment of these commitments, the U.S. government will discuss with the European Commission any adjustments that may be appropriate to address the situation.
5. **Requests for Information.** Requests for access to United States Government records may be made and processed under the Freedom of Information Act (FOIA).

- a. FOIA provides a means for any person to seek access to existing federal agency records, regardless of the nationality of the requester. This statute is codified in the United States Code at 5 U.S.C. § 552. The statute, together with additional information about FOIA, is available at www.FOIA.gov and <http://www.justice.gov/oip/foia-resources>. Each agency has a Chief FOIA Officer, and has provided information on its public website about how to submit a FOIA request to the agency. Agencies have processes for consulting with one another on FOIA requests that involve records held by another agency.
 - b. By way of example:
 - (i) The Office of the Director of National Intelligence (ODNI) has established the ODNI FOIA Portal for the ODNI: <http://www.dni.gov/index.php/about-this-site/foia>. This portal provides information on submitting a request, checking on the status of an existing request, and accessing information that has been released and published by the ODNI under FOIA. The ODNI FOIA Portal includes links to other FOIA websites for IC elements: <http://www.dni.gov/index.php/about-this-site/foia/other-ic-foia-sites>.
 - (ii) The Department of Justice's Office of Information Policy provides comprehensive information about FOIA: <http://www.justice.gov/oip>. This includes not only information about submitting a FOIA request to the Department of Justice, but also provides guidance to the United States government on interpreting and applying FOIA requirements.
 - c. Under FOIA, access to government records is subject to certain enumerated exemptions. These include limits on access to classified national security information, personal information of third parties, and information concerning law enforcement investigations, and are comparable to the limitations imposed by each EU Member State with its own information access law. These limitations apply equally to Americans and non-Americans.
 - d. Disputes over the release of records requested pursuant to FOIA can be appealed administratively and then in federal court. The court is required to make a *de novo* determination of whether records are properly withheld, 5 U.S.C. § 552(a)(4)(B), and can compel the government to provide access to records. In some cases courts have overturned government assertions that information should be withheld as classified. Although no monetary damages are available, courts can award attorney's fees.
6. **Requests for Further Action.** A request alleging violation of law or other misconduct will be referred to the appropriate United States Government body, including independent oversight bodies, with the power to investigate the respective request and address non-compliance as described below.

- a. Inspectors General are statutorily independent; have broad power to conduct investigations, audits and reviews of programs, including of fraud and abuse or violation of law; and can recommend corrective actions.
- (i) The Inspector General Act of 1978, as amended, statutorily established the Federal Inspectors General (IG) as independent and objective units within most agencies whose duties are to combat waste, fraud, and abuse in the programs and operations of their respective agencies. To this end, each IG is responsible for conducting audits and investigations relating to the programs and operations of its agency. Additionally, IGs provide leadership and coordination and recommend policies for activities designed to promote economy, efficiency, and effectiveness, and prevent and detect fraud and abuse, in agency programs and operations.
- (ii) Each element of the Intelligence Community has its own Office of the Inspector General with responsibility for oversight of foreign intelligence activities, among other matters. A number of Inspector General reports about intelligence programs have been publicly released.
- (iii) By way of example:
- The Office of the Inspector General of the Intelligence Community (IC IG) was established pursuant to Section 405 of the Intelligence Authorization Act of Fiscal Year 2010. The IC IG is responsible for conducting IC-wide audits, investigations, inspections, and reviews that identify and address systemic risks, vulnerabilities, and deficiencies that cut across IC agency missions, in order to positively impact IC-wide economies and efficiencies. The IC IG is authorized to investigate complaints or information concerning allegations of a violation of law, rule, regulation, waste, fraud, abuse of authority, or a substantial or specific danger to public health and safety in connection with ODNI and/or IC intelligence programs and activities. The IC IG provides information on how to contact the IC IG directly to submit a report: <http://www.dni.gov/index.php/about-this-site/contact-the-ig>.
 - The Office of the Inspector General (OIG) in the U.S. Department of Justice (DOJ) is a statutorily created independent entity whose mission is to detect and deter waste, fraud, abuse, and misconduct in DOJ programs and personnel, and to promote economy and efficiency in those programs. The OIG investigates alleged violations of criminal and civil laws by DOJ employees and also audits and inspects DOJ programs. The OIG has jurisdiction over all complaints of misconduct against Department of Justice employees, including the Federal Bureau of Investigation; Drug Enforcement Administration; Federal Bureau of Prisons; U.S. Marshals Service; Bureau of Alcohol, Tobacco, Firearms, and Explosives; United States Attorneys Offices; and employees who work in other

Divisions or Offices in the Department of Justice. (The one exception is that allegations of misconduct by a Department attorney or law enforcement personnel that relate to the exercise of the Department attorney's authority to investigate, litigate, or provide legal advice are the responsibility of the Department's Office of Professional Responsibility.) In addition, section 1001 of the USA Patriot Act, signed into law on October 26, 2001, directs the Inspector General to review information and receive complaints alleging abuses of civil rights and civil liberties by Department of Justice employees. The OIG maintains a public website – <https://www.oig.justice.gov> – which includes a “Hotline” for submitting complaints – <https://www.oig.justice.gov/hotline/index.htm>.

- b. Privacy and Civil Liberties offices and entities in the United States Government also have relevant responsibilities. By way of example:
- (i) Section 803 of the Implementing Recommendations of the 9/11 Commission Act of 2007, codified in the United States Code at 42 U.S.C. § 2000-ee1, establishes privacy and civil liberties officers at certain departments and agencies (including the Department of State, Department of Justice, and ODNI). Section 803 specifies that these privacy and civil liberties officers will serve as the principal advisor to, among other things, ensure that such department, agency, or element has adequate procedures to address complaints from individuals who allege such department, agency, or element has violated their privacy or civil liberties.
 - (ii) The ODNI's Civil Liberties and Privacy Office (ODNI CLPO) is led by the ODNI Civil Liberties Protection Officer, a position established by the National Security Act of 1948, as amended. The duties of the ODNI CLPO include ensuring that the policies and procedures of the elements of the Intelligence Community include adequate protections for privacy and civil liberties, and reviewing and investigating complaints alleging abuse or violation of civil liberties and privacy in ODNI programs and activities. The ODNI CLPO provides information to the public on its website, including instructions for how to submit a complaint: www.dni.gov/clpo. If the ODNI CLPO receives a privacy or civil liberties complaint involving IC programs and activities, it will coordinate with other IC elements on how that complaint should be further processed within the IC. Note that the National Security Agency (NSA) also has a Civil Liberties and Privacy Office, which provides information about its responsibilities on its website – https://www.nsa.gov/civil_liberties/. If information indicates that an agency is out of compliance with privacy requirements (*e.g.*, a requirement under Section 4 of PPD-28), then agencies have compliance mechanisms to review and remedy the incident. Agencies are required to report compliance incidents under PPD-28 to the ODNI.

- (iii) The Office of Privacy and Civil Liberties (OPCL) at the Department of Justice supports the duties and responsibilities of the Department's Chief Privacy and Civil Liberties Officer (CPCLO). The principal mission of OPCL is to protect the privacy and civil liberties of the American people through review, oversight, and coordination of the Department's privacy operations. OPCL provides legal advice and guidance to Departmental components; ensures the Department's privacy compliance, including compliance with the Privacy Act of 1974, the privacy provisions of both the E-Government Act of 2002 and the Federal Information Security Management Act, as well as administration policy directives issued in furtherance of those Acts; develops and provides Departmental privacy training; assists the CPCLO in developing Departmental privacy policy; prepares privacy-related reporting to the President and Congress; and reviews the information handling practices of the Department to ensure that such practices are consistent with the protection of privacy and civil liberties. OPCL provides information to the public about its responsibilities at <http://www.justice.gov/opcl>.
- (iv) According to 42 U.S.C. § 2000ee *et seq.*, the Privacy and Civil Liberties Oversight Board shall continually review (i) the policies and procedures, as well as their implementation, of the departments, agencies and elements of the executive branch relating to efforts to protect the Nation from terrorism to ensure that privacy and civil liberties are protected, and (ii) other actions by the executive branch relating to such efforts to determine whether such actions appropriately protect privacy and civil liberties and are consistent with governing laws, regulations, and policies regarding privacy and civil liberties. It shall receive and review reports and other information from privacy officers and civil liberties officers and, when appropriate, make recommendations to them regarding their activities. Section 803 of the Implementing Recommendations of the 9/11 Commission Act of 2007, codified at 42 U.S.C. § 2000ee-1, directs the privacy and civil liberties officers of eight federal agencies (including the Secretary of Defense, Secretary of Homeland Security, Director of National Intelligence, and Director of the Central Intelligence Agency), and any additional agency designated by the Board, to submit periodic reports to the PCLOB, including the number, nature, and disposition of the complaints received by the respective agency for alleged violations. The PCLOB's enabling statute directs the Board to receive these reports and, when appropriate, make recommendations to the privacy and civil liberties officers regarding their activities.

ANNEX IV



OFFICE OF CHAIRWOMAN
EDITH RAMIREZ

United States of America
FEDERAL TRADE COMMISSION
WASHINGTON, DC 20580

February 23, 2016

VIA EMAIL

Věra Jourová
Commissioner for Justice, Consumers and Gender Equality
European Commission
Rue de la Loi / Wetstraat 200
1049 Brussels
Belgium

Dear Commissioner Jourová:

The United States Federal Trade Commission (“FTC”) appreciates the opportunity to describe its enforcement of the new EU-U.S. Privacy Shield Framework (the “Privacy Shield Framework” or “Framework”). We believe the Framework will play a critical role in facilitating privacy-protective commercial transactions in an increasingly interconnected world. It will enable businesses to conduct important operations in the global economy, while at the same time ensuring that EU consumers retain important privacy protections. The FTC has long committed to protecting privacy across borders and will make enforcement of the new Framework a high priority. Below, we explain the FTC’s history of strong privacy enforcement generally, including our enforcement of the original Safe Harbor program, as well as the FTC’s approach to enforcement of the new Framework.

The FTC first publicly expressed its commitment to enforce the Safe Harbor program in 2000. At that time, then-FTC Chairman Robert Pitofsky sent the European Commission a letter outlining the FTC’s pledge to vigorously enforce the Safe Harbor Privacy Principles. The FTC has continued to uphold this commitment through nearly 40 enforcement actions, numerous additional investigations, and cooperation with individual European data protection authorities (“EU DPAs”) on matters of mutual interest.

After the European Commission raised concerns in November 2013 about the administration and enforcement of the Safe Harbor program, we and the U.S. Department of Commerce began consultations with officials from the European Commission to explore ways to strengthen it. While those consultations were proceeding, on October 6, 2015, the European Court of Justice issued a decision in the *Schrems* case that, among other things, invalidated the European Commission’s decision on the adequacy of the Safe Harbor program. Following the decision, we continued to work closely with the Department of Commerce and the European

Commission in an effort to strengthen the privacy protections provided to EU citizens. The Privacy Shield Framework is a result of these ongoing consultations. As was the case with the Safe Harbor program, the FTC hereby commits to vigorous enforcement of the new Framework. This letter memorializes that commitment.

Notably, we affirm our commitment in four key areas: (1) referral prioritization and investigations; (2) addressing false or deceptive Privacy Shield membership claims; (3) continued order monitoring; and (4) enhanced engagement and enforcement cooperation with EU DPAs. We provide below detailed information about each of these commitments and relevant background about the FTC's role in protecting consumer privacy and enforcing Safe Harbor, as well as the broader privacy landscape in the United States.¹

I. Background

A. FTC Privacy Enforcement and Policy Work

The FTC has broad civil enforcement authority to promote consumer protection and competition in the commercial sphere. As part of its consumer protection mandate, the FTC enforces a wide range of laws to protect the privacy and security of consumer data. The primary law enforced by the FTC, the FTC Act, prohibits “unfair” and “deceptive” acts or practices in or affecting commerce.² A representation, omission, or practice is deceptive if it is material and likely to mislead consumers acting reasonably under the circumstances.³ An act or practice is unfair if it causes, or is likely to cause, substantial injury that is not reasonably avoidable by consumers or outweighed by countervailing benefits to consumers or competition.⁴ The FTC also enforces targeted statutes that protect information relating to health, credit and other financial matters, as well as children’s online information, and has issued regulations implementing each of these statutes.

The FTC’s jurisdiction under the FTC Act applies to matters “in or affecting commerce.” The FTC does not have jurisdiction over criminal law enforcement or national security matters. Nor can the FTC reach most other governmental actions. In addition, there are exceptions to the FTC’s jurisdiction over commercial activities, including with respect to banks, airlines, the business of insurance, and the common carrier activities of telecommunications service providers. The FTC also does not have jurisdiction over most non-profit organizations, but it does have jurisdiction over sham charities or other non-profits that in actuality operate for profit. The FTC also has jurisdiction over non-profit organizations that operate for the profit of their for-profit members, including by providing substantial economic benefits to those members.⁵ In some instances, the FTC’s jurisdiction is concurrent with that of other law enforcement agencies.

¹ We provide additional information about U.S. federal and state privacy laws in Attachment A, and a summary of our recent privacy and security enforcement actions in Attachment B. This summary is also available on the FTC’s website at <https://www.ftc.gov/reports/privacy-data-security-update-2015>.

² 15 U.S.C. § 45(a).

³ See FTC Policy Statement on Deception, *appended to Cliffdale Assocs., Inc.*, 103 F.T.C. 110, 174 (1984), available at <https://www.ftc.gov/public-statements/1983/10/ftc-policy-statement-deception>.

⁴ See 15 U.S.C § 45(n); FTC Policy Statement on Unfairness, *appended to Int’l Harvester Co.*, 104 F.T.C. 949, 1070 (1984), available at <https://www.ftc.gov/public-statements/1980/12/ftc-policy-statement-unfairness>.

⁵ See *California Dental Ass’n v. FTC*, 526 U.S. 756 (1999).

We have developed strong working relationships with federal and state authorities and work closely with them to coordinate investigations or make referrals where appropriate.

Enforcement is the lynchpin of the FTC's approach to privacy protection. To date, the FTC has brought over 500 cases protecting the privacy and security of consumer information. This body of cases covers both offline and online information and includes enforcement actions against companies large and small, alleging that they failed to properly dispose of sensitive consumer data, failed to secure consumers' personal information, deceptively tracked consumers online, spammed consumers, installed spyware or other malware on consumers' computers, violated Do Not Call and other telemarketing rules, and improperly collected and shared consumer information on mobile devices. The FTC's enforcement actions—in both the physical and digital worlds—send an important message to companies about the need to protect consumer privacy.

The FTC has also pursued numerous policy initiatives aimed at enhancing consumer privacy that inform its enforcement work. The FTC has hosted workshops and issued reports recommending best practices aimed at improving privacy in the mobile ecosystem; increasing transparency of the data broker industry; maximizing the benefits of big data while mitigating its risks, particularly for low-income and underserved consumers; and highlighting the privacy and security implications of facial recognition and the Internet of Things, among other areas.

The FTC also engages in consumer and business education to enhance the impact of its enforcement and policy development initiatives. The FTC has used a variety of tools—publications, online resources, workshops, and social media—to provide educational materials on a wide range of topics, including mobile apps, children's privacy, and data security. Most recently, the Commission launched its "Start With Security" initiative, which includes new guidance for businesses drawing on lessons learned from the agency's data security cases, as well as a series of workshops across the country. In addition, the FTC has long been a leader in educating consumers about basic computer security. Last year, our OnGuard Online site and its Spanish language counterpart, Alerta en Línea, had more than 5 million page views.

B. U.S. Legal Protections Benefiting EU Consumers

The Framework will operate in the context of the larger U.S. privacy landscape, which protects EU consumers in a number of ways.

The FTC Act's prohibition on unfair or deceptive acts or practices is not limited to protecting U.S. consumers from U.S. companies, as it includes those practices that (1) cause or are likely to cause reasonably foreseeable injury in the United States, or (2) involve material conduct in the United States. Further, the FTC can use all remedies, including restitution, that are available to protect domestic consumers when protecting foreign consumers.

Indeed, the FTC's enforcement work significantly benefits both U.S. and foreign consumers. For example, our cases enforcing Section 5 of the FTC Act have protected the privacy of U.S. and foreign consumers alike. In a case against an information broker, Accusearch, the FTC alleged that the company's sale of confidential telephone records to third

parties without consumers' knowledge or consent was an unfair practice in violation of Section 5 of the FTC Act. Accusearch sold information relating to both U.S. and foreign consumers.⁶ The court granted injunctive relief against Accusearch prohibiting, among other things, the marketing or sale of consumers' personal information without written consent, unless it was lawfully obtained from publicly available information, and ordered disgorgement of almost \$200,000.⁷

The FTC's settlement with TRUSTe is another example. It ensures that consumers, including those in the European Union, can rely on representations that a global self-regulatory organization makes about its review and certification of domestic and foreign online services.⁸ Importantly, our action against TRUSTe also strengthens the privacy self-regulatory system more broadly by ensuring the accountability of entities that play an important role in self-regulatory schemes, including cross-border privacy frameworks.

The FTC also enforces other targeted laws whose protections extend to non-U.S. consumers, such as the Children's Online Privacy Protection Act ("COPPA"). Among other things, COPPA requires that operators of child-directed websites and online services, or general audience sites that knowingly collect personal information from children under the age of 13, provide parental notice and obtain verifiable parental consent. U.S.-based websites and services that are subject to COPPA and collect personal information from foreign children are required to comply with COPPA. Foreign-based websites and online services must also comply with COPPA if they are directed to children in the United States, or if they knowingly collect personal information from children in the United States. In addition to the U.S. federal laws enforced by the FTC, certain other federal and state consumer protection and privacy laws may provide additional benefits to EU consumers.

C. Safe Harbor Enforcement

As part of its privacy and security enforcement program, the FTC has also sought to protect EU consumers by bringing enforcement actions that involved Safe Harbor violations. The FTC has brought 39 Safe Harbor enforcement actions: 36 alleging false certification claims, and three cases—against Google, Facebook, and Myspace—involving alleged violations of Safe Harbor Privacy Principles.⁹ These cases demonstrate the enforceability of certifications and the repercussions for non-compliance. Twenty-year consent orders require Google, Facebook, and Myspace to implement comprehensive privacy programs that must be reasonably designed to address privacy risks related to the development and management of new and existing products

⁶ See Office of the Privacy Commissioner of Canada, Complaint under PIPEDA against Accusearch, Inc., doing business as Abika.com, https://www.priv.gc.ca/cf-dc/2009/2009_009_0731_e.asp. The Office of the Privacy Commissioner of Canada filed an *amicus curiae* brief in the appeal of the FTC action and conducted its own investigation, concluding that Accusearch's practices also violated Canadian law.

⁷ See *FTC v. Accusearch, Inc.*, No. 06CV015D (D. Wyo. Dec. 20, 2007), *aff'd* 570 F.3d 1187 (10th Cir. 2009).

⁸ See *In the Matter of True Ultimate Standards Everywhere, Inc.*, No. C-4512 (F.T.C. Mar. 12, 2015) (decision and order), available at <https://www.ftc.gov/system/files/documents/cases/150318trust-edo.pdf>.

⁹ See *In the Matter of Google, Inc.*, No. C-4336 (F.T.C. Oct. 13 2011) (decision and order), available at <https://www.ftc.gov/news-events/press-releases/2011/03/ftc-charges-deceptive-privacy-practices-googles-rollout-its-buzz>; *In the Matter of Facebook, Inc.*, No. C-4365 (F.T.C. July 27, 2012) (decision and order), available at <https://www.ftc.gov/news-events/press-releases/2012/08/ftc-approves-final-settlement-facebook>; *In the Matter of Myspace LLC*, No. C-4369 (F.T.C. Aug. 30, 2012) (decision and order), available at <https://www.ftc.gov/news-events/press-releases/2012/09/ftc-finalizes-privacy-settlement-myspace>.

and services and to protect the privacy and confidentiality of personal information. The comprehensive privacy programs mandated under these orders must identify foreseeable material risks and have controls to address those risks. The companies must also submit to ongoing, independent assessments of their privacy programs, which must be provided to the FTC. The orders also prohibit these companies from misrepresenting their privacy practices and their participation in any privacy or security program. This prohibition would also apply to companies' acts and practices under the new Privacy Shield Framework. The FTC can enforce these orders by seeking civil penalties. In fact, Google paid a record \$22.5 million civil penalty in 2012 to resolve allegations it had violated its order. Consequently, these FTC orders help protect over a billion consumers worldwide, hundreds of millions of whom reside in Europe.

The FTC's cases have also focused on false, deceptive, or misleading claims of Safe Harbor participation. The FTC takes these claims seriously. For example, in *FTC v. Karnani*, the FTC brought an action in 2011 against an Internet marketer in the United States alleging that he and his company tricked British consumers into believing that the company was based in the United Kingdom, including by using .uk web extensions and referencing British currency and the UK postal system.¹⁰ However, when consumers received the products, they discovered unexpected import duties, warranties that were not valid in the United Kingdom, and charges associated with obtaining refunds. The FTC also charged that the defendants deceived consumers about their participation in the Safe Harbor program. Notably, all of the consumer victims were in the United Kingdom.

Many of our other Safe Harbor enforcement cases involved organizations that joined the Safe Harbor program but failed to renew their annual certification while they continued to represent themselves as current members. As discussed further below, the FTC also commits to addressing false claims of participation in the Privacy Shield Framework. This strategic enforcement activity will complement the Department of Commerce's increased actions to verify compliance with program requirements for certification and re-certification, its monitoring of effective compliance, including through the use of questionnaires to Framework participants, and its increased efforts to identify false Framework membership claims and misuse of any Framework certification mark.¹¹

II. Referral Prioritization and Investigations

As we did under the Safe Harbor program, the FTC commits to give priority to Privacy Shield referrals from EU Member States. We will also prioritize referrals of non-compliance with self-regulatory guidelines relating to the Privacy Shield Framework from privacy self-regulatory organizations and other independent dispute resolution bodies.

¹⁰ See *FTC v. Karnani*, No. 2:09-cv-05276 (C.D. Cal. May 20, 2011) (stipulated final order), available at <https://www.ftc.gov/sites/default/files/documents/cases/2011/06/110609karnanistip.pdf>; see also Lesley Fair, FTC Business Center Blog, *Around the World in Shady Ways*, <http://www.business.ftc.gov/blog/2011/06/around-world-shady-ways> (June 9, 2011).

¹¹ Letter from Stefan M. Selig, Under Secretary of Commerce for International Trade, International Trade Administration, to Věra Jourová, Commissioner for Justice, Consumers and Gender Equality (Feb. 23, 2016).

To facilitate referrals under the Framework from EU Member States, the FTC is creating a standardized referral process and providing guidance to EU Member States on the type of information that would best assist the FTC in its inquiry into a referral. As part of this effort, the FTC will designate an agency point of contact for EU Member State referrals. It is most useful when the referring authority has conducted a preliminary inquiry into the alleged violation and can cooperate with the FTC in an investigation.

Upon receipt of a referral from an EU Member State or self-regulatory organization, the FTC can take a range of actions to address the issues raised. For example, we may review the company's privacy policies, obtain further information directly from the company or from third parties, follow up with the referring entity, assess whether there is a pattern of violations or significant number of consumers affected, determine whether the referral implicates issues within the purview of the Department of Commerce, assess whether consumer and business education would be helpful, and, as appropriate, initiate an enforcement proceeding.

The FTC also commits to exchange information on referrals with referring enforcement authorities, including the status of referrals, subject to confidentiality laws and restrictions. To the extent feasible given the number and type of referrals received, the information provided will include an evaluation of the referred matters, including a description of significant issues raised and any action taken to address law violations within the jurisdiction of the FTC. The FTC will also provide feedback to the referring authority on the types of referrals received in order to increase the effectiveness of efforts to address unlawful conduct. If a referring enforcement authority seeks information about the status of a particular referral for purposes of pursuing its own enforcement proceeding, the FTC will respond, taking into account the number of referrals under consideration and subject to confidentiality and other legal requirements.

The FTC will also work closely with EU DPAs to provide enforcement assistance. In appropriate cases, this could include information sharing and investigative assistance pursuant to the U.S. SAFE WEB Act, which authorizes FTC assistance to foreign law enforcement agencies when the foreign agency is enforcing laws prohibiting practices that are substantially similar to those prohibited by laws the FTC enforces.¹² As part of this assistance, the FTC can share information obtained in connection with an FTC investigation, issue compulsory process on behalf of the EU DPA conducting its own investigation, and seek oral testimony from witnesses or defendants in connection with the DPA's enforcement proceeding, subject to the requirements of the U.S. SAFE WEB Act. The FTC regularly uses this authority to assist other authorities around the world in privacy and consumer protection cases.¹³

¹² In determining whether to exercise its U.S. SAFE WEB Act authority, the FTC considers, inter alia: "(A) whether the requesting agency has agreed to provide or will provide reciprocal assistance to the Commission; (B) whether compliance with the request would prejudice the public interest of the United States; and (C) whether the requesting agency's investigation or enforcement proceeding concerns acts or practices that cause or are likely to cause injury to a significant number of persons." 15 U.S.C. § 46(j)(3). This authority does not apply to enforcement of competition laws.

¹³ In fiscal years 2012-2015, for example, the FTC used its U.S. SAFE WEB Act authority to share information in response to almost 60 requests from foreign agencies and it issued nearly 60 civil investigative demands (equivalent to administrative subpoenas) to aid 25 foreign investigations.

In addition to prioritizing Privacy Shield referrals from EU Member States and privacy self-regulatory organizations,¹⁴ the FTC commits to investigating possible Framework violations on its own initiative where appropriate using a range of tools.

For well over a decade, the FTC has maintained a robust program of investigating privacy and security issues involving commercial organizations. As part of these investigations, the FTC routinely examined whether the entity at issue was making Safe Harbor representations. If the entity was making such representations and the investigation revealed apparent violations of the Safe Harbor Privacy Principles, the FTC included allegations of Safe Harbor violations in its enforcement actions. We will continue this proactive approach under the new Framework. Importantly, the FTC conducts many more investigations than ultimately result in public enforcement actions. Many FTC investigations are closed because staff does not identify an apparent law violation. Because FTC investigations are non-public and confidential, the closing of an investigation is often not made public.

The nearly 40 enforcement actions initiated by the FTC involving the Safe Harbor program evidence the agency's commitment to proactive enforcement of cross-border privacy programs. The FTC will look for potential Framework violations as part of the privacy and security investigations we undertake on a regular basis.

III. Addressing False or Deceptive Privacy Shield Membership Claims

As referenced above, the FTC will take action against entities that misrepresent their participation in the Framework. The FTC will give priority consideration to referrals from the Department of Commerce regarding organizations that it identifies as improperly holding themselves out to be current members of the Framework or using any Framework certification mark without authorization.

In addition, we note that if an organization's privacy policy promises that it complies with the Privacy Shield Principles, its failure to make or maintain a registration with the Department of Commerce likely will not, by itself, excuse the organization from FTC enforcement of those Framework commitments.

IV. Order Monitoring

The FTC also affirms its commitment to monitor enforcement orders to ensure compliance with the Privacy Shield Framework.

We will require compliance with the Framework through a variety of appropriate injunctive provisions in future FTC Framework orders. This includes prohibiting

¹⁴ Although the FTC does not resolve or mediate individual consumer complaints, the FTC affirms that it will prioritize Privacy Shield referrals from EU DPAs. In addition, the FTC uses complaints in its Consumer Sentinel database, which is accessible by many other law enforcement agencies, to identify trends, determine enforcement priorities, and identify potential investigative targets. EU citizens can use the same complaint system available to U.S. citizens to submit a complaint to the FTC at www.ftc.gov/complaint. For individual Privacy Shield complaints, however, it may be most useful for EU citizens to submit complaints to their Member State DPA or alternative dispute resolution provider.

misrepresentations regarding the Framework and other privacy programs when these are the basis for the underlying FTC action.

The FTC's cases enforcing the original Safe Harbor program are instructive. In the 36 cases involving false or deceptive claims of Safe Harbor certification, each order prohibits the defendant from misrepresenting its participation in Safe Harbor or any other privacy or security program and requires the company to make compliance reports available to the FTC. In cases that involved violations of Safe Harbor Privacy Principles, companies have been required to implement comprehensive privacy programs and obtain independent third-party assessments of those programs every other year for twenty years, which they must provide to the FTC.

Violations of the FTC's administrative orders can lead to civil penalties of up to \$16,000 per violation, or \$16,000 per day for a continuing violation,¹⁵ which, in the case of practices affecting many consumers, can amount to millions of dollars. Each consent order also has reporting and compliance provisions. The entities under order must retain documents demonstrating their compliance for a specified number of years. The orders must also be disseminated to employees responsible for ensuring order compliance.

The FTC systematically monitors compliance with Safe Harbor orders, as it does with all of its orders. The FTC takes enforcement of its privacy and data security orders seriously and brings actions to enforce them when necessary. For example, as noted above, Google paid a \$22.5 million civil penalty to resolve allegations it had violated its FTC order. Importantly, FTC orders will continue to protect all consumers worldwide who interact with a business, not just those consumers who have lodged complaints.

Finally, the FTC will continue to maintain an online list of companies subject to orders obtained in connection with enforcement of both the Safe Harbor program and the new Privacy Shield Framework.¹⁶ In addition, the Privacy Shield Principles now require companies subject to an FTC or court order based on non-compliance with the Principles to make public any relevant Framework-related sections of any compliance or assessment report submitted to the FTC, to the extent consistent with confidentiality laws and rules.

V. Engagement With EU DPAs and Enforcement Cooperation

The FTC recognizes the important role that EU DPAs play with respect to Framework compliance and encourages increased consultation and enforcement cooperation. In addition to any consultation with referring DPAs on case-specific matters, the FTC commits to participate in periodic meetings with designated representatives of the Article 29 Working Party to discuss in general terms how to improve enforcement cooperation with respect to the Framework. The FTC will also participate, along with the Department of Commerce, the European Commission, and Article 29 Working Party representatives, in the annual review of the Framework to discuss its implementation.

¹⁵ 15 U.S.C. § 45(m); 16 C.F.R. § 1.98.

¹⁶ See FTC, Business Center, Legal Resources, https://www.ftc.gov/tips-advice/business-center/legal-resources?type=case&field_consumer_protection_topics_tid=251.

The FTC also encourages the development of tools that will enhance enforcement cooperation with EU DPAs, as well as other privacy enforcement authorities around the world. In particular, the FTC, along with enforcement partners in the European Union and around the globe, last year launched an alert system within the Global Privacy Enforcement Network (“GPEN”) to share information about investigations and promote enforcement coordination. This GPEN Alert tool could be particularly useful in the context of the Privacy Shield Framework. The FTC and EU DPAs could use it to coordinate with respect to the Framework and other privacy investigations, including as a starting point for sharing information in order to deliver coordinated and more effective privacy protection for consumers. We look forward to continuing to work with participating EU authorities to deploy the GPEN Alert system more broadly and develop other tools to improve enforcement cooperation in privacy cases, including those involving the Framework.

The FTC is pleased to affirm its commitment to enforcing the new Privacy Shield Framework. We also look forward to continuing engagement with our EU colleagues as we work together to protect consumer privacy on both sides of the Atlantic.

Sincerely,

A handwritten signature in black ink that reads "Edith Ramirez". The signature is written in a cursive, flowing style.

Edith Ramirez
Chairwoman

ANNEX V



THE SECRETARY OF TRANSPORTATION
WASHINGTON, DC 20590

February 19, 2016

Commissioner Věra Jourová
European Commission
Rue de la Loi / Wetstraat 200
1049 1049 Brussels
Belgium

Re: EU-U.S. Privacy Shield Framework

Dear Commissioner Jourová:

The United States Department of Transportation (“Department” or “DOT”) appreciates the opportunity to describe its role in enforcing the EU-U.S. Privacy Shield Framework. This Framework plays a critical role in protecting personal data provided during commercial transactions in an increasingly interconnected world. It enables businesses to conduct important operations in the global economy, while at the same time ensuring that EU consumers retain important privacy protections.

The DOT first publicly expressed its commitment to enforcement of the Safe Harbor Framework in a letter sent to the European Commission over 15 years ago. The DOT pledged to vigorously enforce the Safe Harbor Privacy Principles in that letter. The DOT continues to uphold this commitment and this letter memorializes that commitment.

Notably, the DOT renews its commitment in the following key areas: (1) prioritization of investigation of alleged Privacy Shield violations; (2) appropriate enforcement action against entities making false or deceptive Privacy Shield certification claims; and (3) monitoring and making public enforcement orders concerning Privacy Shield violations. We provide information about each of these commitments and, for necessary context, pertinent background about the DOT’s role in protecting consumer privacy and enforcing the Privacy Shield Framework.

I. Background

A. DOT’s Privacy Authority

The Department is strongly committed to ensuring the privacy of information provided by consumers to airlines and ticket agents. The DOT’s authority to take action in this area is found in 49 U.S.C. 41712, which prohibits a carrier or ticket agent from engaging in “an unfair or deceptive practice or an unfair method of competition” in the sale of air transportation that results or is likely to result in consumer harm. Section 41712 is patterned after Section 5 of the Federal Trade Commission (FTC) Act (15 U.S.C. 45). We interpret our unfair or deceptive practice statute as prohibiting an airline or ticket agent from: (1) violating the terms of its

privacy policy; or (2) gathering or disclosing private information in a way that violates public policy, is immoral, or causes substantial consumer injury not offset by any countervailing benefits. We also interpret section 41712 as prohibiting carriers and ticket agents from: (1) violating any rule issued by the Department that identifies specific privacy practices as unfair or deceptive; or (2) violating the Children's Online Privacy Protection Act (COPPA) or FTC rules implementing COPPA. Under federal law, the DOT has exclusive authority to regulate the privacy practices of airlines, and it shares jurisdiction with the FTC with respect to the privacy practices of ticket agents in the sale of air transportation.

As such, once a carrier or seller of air transportation publicly commits to the Privacy Shield Framework's privacy principles the Department is able to use the statutory powers of section 41712 to ensure compliance with those principles. Therefore, once a passenger provides information to a carrier or ticket agent that has committed to honoring the Privacy Shield Framework's privacy principles, any failure to do so by the carrier or ticket agent would be a violation of section 41712.

B. Enforcement Practices

The Department's Office of Aviation Enforcement and Proceedings (Aviation Enforcement Office) investigates and prosecutes cases under 49 U.S.C. 41712. It enforces the statutory prohibition in section 41712 against unfair and deceptive practices primarily through negotiation, preparing cease and desist orders, and drafting orders assessing civil penalties. The office learns of potential violations largely from complaints it receives from individuals, travel agents, airlines, and U.S. and foreign government agencies. Consumers may use the DOT's website to file privacy complaints against airlines and ticket agents.¹

If a reasonable and appropriate settlement in a case is not reached, the Aviation Enforcement Office has the authority to institute an enforcement proceeding involving an evidentiary hearing before a DOT administrative law judge (ALJ). The ALJ has the authority to issue cease-and-desist orders and civil penalties. Violations of section 41712 can result in the issuance of cease and desist orders and the imposition of civil penalties of up to \$27,500 for each violation of section 41712.

The Department does not have the authority to award damages or provide pecuniary relief to individual complainants. However, the Department does have the authority to approve settlements resulting from investigations brought by its Aviation Enforcement Office that directly benefit consumers (e.g., cash, vouchers) as an offset to monetary penalties otherwise payable to the U.S. Government. This has occurred in the past, and may also occur in the context of the Privacy Shield Framework principles when circumstances warrant. Repeated violations of section 41712 by an airline would also raise questions regarding the airline's compliance disposition which could, in egregious situations, result in an airline being found to be no longer fit to operate and, therefore, losing its economic operating authority.

¹ <http://www.transportation.gov/airconsumer/privacy-complaints>.

To date, the DOT has received relatively few complaints involving alleged privacy violations by ticket agents or airlines. When they arise, they are investigated according to the principles set forth above.

C. DOT Legal Protections Benefiting EU Consumers

Under section 41712, the prohibition on unfair or deceptive practices in air transportation or the sale of air transportation applies to U.S. and foreign air carriers as well as ticket agents. The DOT frequently takes action against U.S. and foreign airlines for practices that affect both foreign and U.S. consumers on the basis that the airline's practices took place in the course of providing transportation to or from the United States. The DOT does and will continue to use all remedies that are available to protect both foreign and U.S. consumers from unfair or deceptive practices in air transportation by regulated entities.

The DOT also enforces, with respect to airlines, other targeted laws whose protections extend to non-U.S. consumers such as COPPA. Among other things, COPPA requires that operators of child-directed websites and online services, or general audience sites that knowingly collect personal information from children under 13 provide parental notice and obtain verifiable parental consent. U.S.-based websites and services that are subject to COPPA and collect personal information from foreign children are required to comply with COPPA. Foreign-based websites and online services must also comply with COPPA if they are directed to children in the United States, or if they knowingly collect personal information from children in the United States. To the extent that U.S. or foreign airlines doing business in the United States violate COPPA, the DOT would have jurisdiction to take enforcement action.

II. **Privacy Shield Enforcement**

If an airline or ticket agent chooses to participate in the Privacy Shield Framework and the Department receives a complaint that such an airline or ticket agent had allegedly violated the Framework, the Department would take the following steps to vigorously enforce the Framework.

A. Prioritizing Investigation of Alleged Violations

The Department's Aviation Enforcement Office will investigate each complaint alleging Privacy Shield violations (including complaints received from EU Data Protection Authorities) and take enforcement action where there is evidence of a violation. Further, the Aviation Enforcement Office will cooperate with the FTC and Department of Commerce and give priority consideration to allegations that the regulated entities are not complying with privacy commitments made as part of the Privacy Shield Framework.

Upon receipt of an allegation of a violation of the Privacy Shield Framework, the Department's Aviation Enforcement Office may take a range of actions as part of its investigation. For example, it may review the ticket agent or airline's privacy policies, obtain further information from the ticket agent or airline or from third parties, follow up with the referring entity, and assess whether there is a pattern of violations or significant number of consumers affected. In

addition, it would determine whether the issue implicates matters within the purview of the Department of Commerce or FTC, assess whether consumer education and business education would be helpful, and as appropriate, initiate an enforcement proceeding.

If the Department becomes aware of potential Privacy Shield violations by ticket agents, it will coordinate with the FTC on the matter. We will also advise the FTC and the Department of Commerce of the outcome of any Privacy Shield enforcement action.

B. Addressing False or Deceptive Membership Claims

The Department remains committed to investigating Privacy Shield violations, including false or deceptive claims of membership in the Privacy Shield Program. We will give priority consideration to referrals from the Department of Commerce regarding organizations that it identifies as improperly holding themselves out to be current members of Privacy Shield or using the Privacy Shield Framework certification mark without authorization.

In addition, we note that if an organization's privacy policy promises that it complies with the substantive Privacy Shield principles, its failure to make or maintain a registration with the Department of Commerce likely will not, by itself, excuse the organization from DOT enforcement of those commitments.

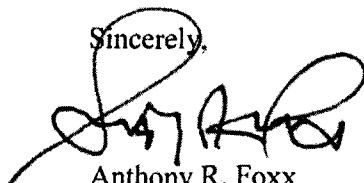
C. Monitoring and Making Public Enforcement Orders Concerning Privacy Shield Violations

The Department's Aviation Enforcement Office also remains committed to monitoring enforcement orders as needed to ensure compliance with the Privacy Shield program. Specifically, if the office issues an order directing an airline or ticket agent to cease and desist from future violations of Privacy Shield and section 41712, it will monitor the entity's compliance with the cease-and-desist provision in the order. In addition, the office will ensure that orders resulting from Privacy Shield cases are available on its website.

We look forward to our continued work with our federal partners and EU stakeholders on Privacy Shield matters.

I hope that this information proves helpful. If you have any questions or need further information, please feel free to contact me.

Sincerely,



Anthony R. Foxx
Secretary of Transportation

Ms. Isabelle Falque-Pierrotin
Chairman, Article 29 Working Party

MEP Claude Moraes
Chair of the Committee on Civil Liberties, Justice, and Home Affairs

HE Pieter de Gooijer
Ambassador and Permanent Representative of the Netherlands to the EU

cc: Secretary Penny Pritzker
Commissioner Věra Jourová

March 16, 2016

Ms. Falque-Pierrotin, MEP Moraes, and Ambassador de Gooijer,

We, the undersigned organizations do not believe that the Privacy Shield arrangement between the United States and the European Union complies with the standards set by the Court of Justice of the European Union (CJEU), including in the recent case invalidating the legal underpinnings of the Safe Harbor Framework.¹ Without more substantial reforms to ensure protection for fundamental rights of individuals on both sides of the Atlantic, the Privacy Shield will put users at risk, undermine trust in the digital economy, and perpetuate the human rights violations that are already occurring as a result of surveillance programs and other activities.

The Article 29 Working Party thoughtfully outlined four key conditions for an agreement to meet the standards of European legislation and guarantee the protection of human rights in intelligence activity, including clarity of law, use of human rights standards, incorporation of independent oversight, and availability of effective remedy.² Unfortunately, the Privacy Shield manifestly fails to provide for these objectives.³

While questions remain about the scope and utility of certain provisions of the Privacy Shield,⁴ it is beyond doubt that the continued existence of the same inadequacies in US law

¹ C-362/14, Maximilian Schrems v Data Protection Commissioner, 2015 <http://curia.europa.eu> (Oct. 6, 2015), <http://curia.europa.eu/juris/document/document.jsf?text=&docid=169195&pageIndex=0&doclang=EN&mode=req>.

² Statement of the Article 29 Working Party on the Consequences of the Schrems Judgment (Feb. 3, 2016) http://ec.europa.eu/justice/data-protection/article-29/press-material/press-release/art29_press_material/2016/20160203_statement_consequences_schrems_judgement_en.pdf.

³ See, e.g., Netzwerk Datenschutzexpertise (Data Protection Expertise Network), *Privacy Shield – Darstellung und rechtliche Bewertung*, <http://www.netzwerk-datenschutzexpertise.de>.

⁴ For example, what level of redress does the proposed Alternative Dispute Mechanism offer as compared to independent judicial oversight? Are the exemptions from the opt-in system proportionate? What is the legal status of the written assurances provided by the intelligence community? What limits are placed on the collection of EU data by the intelligence community? Have the EU and US reached a common understanding on the definitions of key surveillance terms, like “bulk surveillance”?

that existed at the time of the CJEU's judgment mean EU citizens still cannot be sure what will happen to their data once transferred to the US. Specifically, the US government continues to deny the relevance and application of the internationally-accepted standards of necessity and proportionality in its surveillance operations. In addition, the oversight mechanism established by the Privacy Shield to respond to complaints about US surveillance is not independent, nor does the office come empowered with sufficient authority to initiate investigations or respond adequately to complaints.⁵ Finally, due to the fact that individuals are never notified when their information has been collected, disseminated, or used, any remedy for individuals will be unavailable for all practical purposes.

In order for the Privacy Shield to survive, the US must formally commit to substantial reforms to respect human rights and international law in order to meet the standards set forth by the CJEU and the Article 29 Working Group.⁶ The Privacy Shield contains no such commitment.

The Privacy Shield should be contingent on US legislative reform of surveillance laws within a reasonable time. These reforms must include, at a minimum, the incorporation of human rights standards (applying to both US persons and non-US persons), a narrowed definition of “foreign intelligence information” to limit the scope of data collection, and more limited access to, retention of, and use of data after it is collected. Indiscriminate scanning of communications content and metadata, specifically, must be discontinued.

In addition to surveillance reform, a lasting data transfer framework requires increased protections for personal data collected or used commercially in order to meet the standards set forth by the CJEU. Wider data protection reforms, which must include robust and comprehensive enforcement mechanisms, are necessary to ensure that the US provides a level of essentially equivalent protection to that available under the European legal framework.

Finally, the Privacy Shield must include provisions to ensure appropriate redress and transparency.

In recognition of the changes needed in order to build a solid foundation for mutual trust across the Atlantic, we urge you to send the Privacy Shield back to the negotiators for further consideration in order to address the identified issues. These reforms and

⁵ Emily O'Reilly, Use of the title 'ombudsman' in the 'EU-US Privacy Shield' agreement, European Ombudsman (Febr. 22, 2016), <http://www.ombudsman.europa.eu/resources/otherdocument.faces/en/64157/html.bookmark>. When reviewing complaints, the Ombudsperson only ensures that data was handled appropriately under existing US law and policy, which lack adequate data protections. Even in cases where the Ombudsperson does find that data was handled improperly, she will neither confirm nor deny that the complainant was the target of surveillance, nor will she inform the individual of the specific remedial action taken. And, the Ombudsperson will not respond to any general claims that the agreement is inconsistent with EU data protection laws.

⁶ To prevent a double standard, the Commission must seek a similar pledge from EU Member States to commit to reforming their surveillance authorities.

safeguards would help protect individuals' human rights and provide the legal certainty needed by companies operating trans-nationally.

Sincerely,

Access Now

Advocacy for Principled Action in Government

American-Arab Anti-Discrimination Committee (ADC)

American Civil Liberties Union (ACLU)

Amnesty International USA

Association for Technology and Internet (APTI)

Bits of Freedom

Center for Digital Democracy

Consumer Action

Consumer Federation of America

Consumer Watchdog

Cyber Privacy Project

Defending Dissent/Bill of Rights Defense Committee

Digitale Gesellschaft e.V.

Digital Rights Ireland

Electronic Frontier Foundation

Electronic Privacy Information Center

European Digital Rights (EDRi)

Fight for the Future

IT-Political Association of Denmark

Panoptikon Foundation

Patient Privacy Rights

Privacy International

Privacy Rights Clearinghouse

La Quadrature du Net

Restore the Fourth

X-Lab