JULY 2016

PRIVACY SHIELD:
Essentially Equivalent

SIDLEY
150 YEARS

datamatters.sidley.com

SIDLEY
150 YEARS

THE PRIVACY SHIELD SATISFIES EU LAW REQUIREMENTS AND ADDRESSES CONCERNS THAT HAVE BEEN RAISED

With the final Privacy Shield decision, the European Commission and United States Government have concluded several years of discussion and negotiation concerning the Safe Harbour framework and the new Privacy Shield. The effort and thought by negotiators, EU institutions, and stakeholders alike to reach this point reflect the importance of private life and data protection in EU society and the significance of data flows to transatlantic commerce and discourse.

This labour has yielded a strong new framework that complies with EU law and sets a high standard for international data transfers. The Commission's Adequacy Decision of 12 July 2016 (C(2016)4176 final) is backed up by thorough examination and explanation of the safeguards provided by the US legal order and the added mechanisms of the Privacy Shield and responds to concerns by the Article 29 Working Party ("WP29"), European Data Protection Supervisor ("EDPS"), and European Parliament. As more fully detailed below, the Privacy Shield requirements far surpass those under Safe Harbour and ensure that EU residents whose data is transferred to the US receive protection essentially equivalent to what they receive in the EU.

SUMMARY

The Privacy Shield framework reflects strong political consensus on the shared importance of maintaining transatlantic data flows. This is a premise on which the Commission, the WP29, the EDPS, the Parliament, and the Member States all have concurred.

The "many improvements" strengthening principles, administration, and oversight make protection of data under the Privacy Shield essentially equivalent. Generalised assertions that the Privacy Shield differs little from Safe Harbour have no basis in the actual operation of the framework. The Privacy Shield and robust changes to US laws since 2000 cover all 13 recommendations made by the Commission in 2013, and clearly render the new framework "adequate" under EU law.

The major points of concern raised about the Privacy Shield are addressed by the final framework. The final Commission Decision clarifies numerous aspects of the Privacy Shield. In particular, it shows more specifically how US laws and the Privacy Shield address safeguards for national security surveillance consistently with CJEU and ECtHR jurisprudence and how the Ombudsperson will enlarge avenues of redress; makes data deletion explicit within the Data Integrity and Purpose Limitation Principle; clarifies onward transfer obligations; and takes steps to address automated processing.

The Privacy Shield framework reflects strong political consensus on the shared importance of maintaining transatlantic data flows.

The Commission's 29 February 2016 Communication accompanying the Privacy Shield framework[1] affirms the importance of data flows to the ties between the United States and the European Union : "[t]he transfer and exchange of personal data is an essential component underpinning the close links between the [EU] and the [US] in the commercial area as well as in the law enforcement sector".

Each reviewing body acknowledges this premise. In its 13 April 2016 Opinion 01/2016 on the draft EU-U.S. Privacy Shield ("Opinion WP238"),[2] the WP29 agreed notwithstanding its concerns: "Given the amount of data transfers that take place between the EU and the U.S. on a daily basis, which the WP29 recognises is a vital part of the economy on both sides of the Atlantic, legal clarity is needed sooner rather than later." Similarly, the EDPS recognised "the value, in the era of global, instantaneous and unpredictable data flows, of a sustainable frame for commercial transfers of data between the EU and the U.S., which represent the biggest trading partnership in the world".[3] The 26 May 2016 European Parliament resolution on the Privacy Shield notes that "cross-border data flows between the United States and Europe are the highest in the world" and are "an essential component underpinning the close links between the [EU] and the [US] in commercial activities and in the law enforcement sector".[4]

As former Swedish Prime Minister Carl Bildt and former US Ambassador to the EU William Kennard wrote, "Data privacy has been a difficult issue across the Atlantic, but abandoning the privacy shield would cause huge disruptions not only in transatlantic commerce, research, and investment but also within the EU itself".[5]

---

[1] http://ec.europa.eu/justice/data-protection/files/privacy-shield-adequacy-communication_en.pdf.

[2] WP29 13 April 2016, Opinion 01/2016 on the EU-U.S. Privacy Shield draft adequacy decision issued, WP 238, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2016/wp238_en.pdf, page 12 (para. 1.2).

[3] EDPS 30 May 2016, Opinion 4/2016, Opinion on the EU-U.S. Privacy Shield draft adequacy decision, https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2016/16-05-30_Privacy_Shield_EN.pdf, page 2 ("EDPS Opinion").

[4] Document P8_TA-PROV(2016)0233, European Parliament resolution of 26 May 2016 on transatlantic data flows (2016/2727(RSP)) http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+MOTION+B8-2016-0623+0+DOC+PDF+V0//EN, resolution 2 ("Parliament Resolution").

[5] "Obama and Merkel: a chance to make history in Hanover," *Politico* (23 April 2016).

The Privacy Shield Principles, Oversight by the EU and US Governments and Data Protection Authorities, and Remedies Far Surpass What Was Required under Safe Harbour.

The Privacy Shield introduces numerous measures to address any differences between levels of privacy and data protection in the EU and the US. The WP29 noted "significant improvements brought by the Privacy Shield compared to the Safe Harbour decision" and acknowledged that "many of the shortcomings of the Safe Harbour … have been addressed by the negotiators".[6] The European Parliament resolution similarly welcomed "substantial improvements in the Privacy Shield compared to the Safe Harbour decision ...".[7]

In its 27 November 2013 Communication on the Functioning of the Safe Harbour from the perspective of EU Citizens and Companies Established in the EU (the "2013 Safe Harbour Communication")[8], the Commission framed 13 recommendations to address issues identified in the Commission's review. The Privacy Shield responds to all 13 of these recommendations. The responses in the Privacy Shield to the most salient concerns are addressed below.

1. Because the promises that companies in the US make are legally enforceable, the Privacy Shield significantly strengthens protection by requiring additional information under the Notice Principle.

Annex II, containing the Principles and Supplemental Principles issued by the Commerce Department, sets out the obligations that companies accept by subscribing to the Privacy Shield. The new framework requires much greater detail in the notices and disclosures that subscribing companies must provide to data subjects. In particular, the expanded Notice Principle (pages 19-20) requires an explicit statement of a company's commitment to the Privacy Shield Principles, the types of personal data it collects, the type or identity of third parties to which such personal data is disclosed, and statements explaining the company's liability for improper onward transfers, as well as more detailed information about the enforceability of the Principles and means available for data subjects to seek redress.

As the Commission states, although participation in the Privacy Shield is voluntary "effective compliance with the Principles is compulsory"[9] because, as explained in the letter from the Chairwoman of the US Federal Trade Commission ("FTC") in Annex IV, the promises that companies make in their privacy policies and other public statements are legally binding and enforceable.

---

[6] WP238, page 2.

[7] Para. I.1.

[8] http://ec.europa.eu/justice/data-protection/files/com_2013_847_en.pdf

[9] Decision, recital 26.

The additional specific statements required under the Notice Principle clarify expectations for data controllers and data subjects alike and strengthen the ability to enforce Privacy Shield Principles. The 2013 Safe Harbour Communication found that "[l]ack of transparency by companies in the US renders Federal Trade Commission oversight more difficult and undermines the effectiveness of enforcement". The increase in transparency required by the Privacy Shield will facilitate oversight and enhance the effectiveness of enforcement.

2. *The Privacy Shield Principles add new accountability for onward transfers by requiring specific steps to ensure that third-party controllers and processors use transferred personal data only for limited and specified purposes.*

The 2013 Safe Harbour Communication identified onward transfers to third parties as a concern in light of the growth of data flows and cloud computing. The Safe Harbour framework generally allowed transfers to the third parties that subscribed to Safe Harbour and shifted responsibility for compliance to such third parties. A 10 April 2014 letter from the Article 29 Working Party to Commissioner Reding[10] recommended a specific accountability principle for onward transfers.

The Privacy Shield explicitly incorporates such a principle with a new Accountability for Onward Transfer Principle (page 21), eliminating any shift in responsibility and requiring the subscribing company to contract with third party controllers and take steps (that may include contracts) to ensure that third-party agents process data in ways consistent with the subscribing company's obligations. In response to the WP29's concerns in the WP238 about onward transfers to third countries, the final framework includes an obligation on the part of these third parties to notify the subscribing company if they determine they become unable to maintain the required level of protection.

3. *The Privacy Shield ensures much stronger administration and enforcement by increasing involvement of DPAs in the administration of the framework, expanding responsibilities of the US Department of Commerce, adding referral mechanisms, and strengthening the annual review process.*

The 2013 Safe Harbour Communication traced a history of concerns with the vigour of Safe Harbour enforcement beginning in 2004 and escalating from 2009-13. Concerns included missing privacy policies among Safe Harbour companies, companies on the US Commerce Department Safe Harbour list that failed to maintain their certifications, and subscriber non-compliance with Safe Harbour principles as well as procedures. In response, the Commerce Department stepped up its policing of Safe Harbour certifications and the public list of certified

[10] http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2014/20140410_wp29_to_ec_on_sh_recommendations.pdf

companies, and improved its Safe Harbour website. In 2009, the FTC brought its first case alleging unfair or deceptive practices or acts stemming from violation of Safe Harbour commitments and has brought at least 23 more cases since then. (See Annex IV).

The Privacy Shield incorporates these improvements and details numerous additional ones to reinforce oversight and enforcement. Annex I to the Privacy Shield, the commitments by the Commerce Department as augmented in the final version, reflects that the Commerce Department has increased resources dedicated to, among other responsibilities:

- verifying that company self-certifications are complete (including a privacy policy that commits to the Privacy Shield Principles and the designation of recourse mechanisms of regulatory bodies) and, as recommended by WP29, verifying that these policies conform to the Principles[11] (pages 6-7);
- conducting periodic compliance reviews, including the "ongoing *ex officio* reviews" recommended by WP29 and EDPS[12] (page 9);
- keeping the Privacy Shield list up-to-date by removing companies that withdraw, fail to re-certify, or persistently fail to comply, and check that such companies continue to apply the Privacy Shield Principles to any information they are able to retain (pages 7-8);
- maintaining a public listing of companies removed from the Privacy Shield list, with the reasons for their removal and (also as recommended by WP29[13]) monitoring these companies' compliance with requirements to return or delete data (page 17); and
- referring cases of abuse of the Privacy Shield certification or other false claims to the FTC or other agencies (page 17).

Annex I summarizing the commitments of the Commerce Department sets out what the Parliament Resolution welcomed as "the prominent role" given to DPAs in monitoring the Privacy Shield framework. Their expanded role is reflected in numerous ways: "interested DPAs" can participate in the annual review and raise the full range of issues including enforcement, changes of law, and information disclosed by the US Intelligence Community (page 10); and the WP29 will have a dedicated point of contact in the Commerce Department to refer complaints of non-compliance, coordinate on compliance reviews, and share information concerning participating organizations and material for use on DPA websites (page 9). DPAs also will act as conduits for requests to the Ombudsperson by EU individuals concerning government surveillance (Annex III (A), pages 53-54) .

[11] WP238, page 28.

[12] WP238, page 14; EPDS Opinion page 12.

[13] WP238, page 29.

In addition, the Supplemental Principles in Annex II require companies to cooperate with DPAs and provide for "an informal panel of DPAs established at the EU level" to advise companies on compliance (page 26). The FTC commits in Annex IV to coordinate with DPAs on enforcement and to periodic meetings with WP29 on the working of the Privacy Shield (page 65). The sum total of these mechanisms goes beyond arrangements in place for any other third country and any other Article 25(6) Decision.

In the *Schrems* judgment, the Court of Justice of the European Union ("CJEU") gave a clear command to the European Commission to "check periodically"[14] whether an adequacy decision is still justified in light of changes in law or circumstances. The Commission will be monitoring "continuously" and will also conduct an annual review that will consider changes in law both in the US and the EU, including the application of the GDPR as of 25 May 2018 and also a dialogue to consider automated processing. The Commission also expresses in clear detail in both its Privacy Shield Communication and the Adequacy Opinion that ongoing review of the Privacy Shield and its operation can lead to suspension if "the level of protection can no longer be regarded as essentially equivalent to the one in the Union" (page 41).

In light of these changes, the framework clearly will be subject to rigourous oversight and will not remain static if circumstances warrant change. The annual reviews will provide opportunities to rectify any deficiencies, including any further concerns raised by the WP29 that prove to be problematic in operation.

Even if the Commission and the Department of Commerce were somehow inclined to disregard their commitments to careful oversight of the framework, they would be prevented from doing so by the expanded role of DPAs in administration of the Privacy Shield and the scrutiny that the framework undoubtedly will receive in the Parliament, press, and civil society.

4. The Privacy Shield provides a menu of redress options for individuals that ensures a path for judicial review, enables dispute resolution at no cost, and sets deadlines.

The provisions for individual redress created in the Supplemental Principles of Annex II offer several paths for individuals to pursue, taking into account a number of considerations from the *Schrems* judgment and other Safe Harbour criticism through the years.

These avenues address the CJEU's criticism of the Safe Harbour Decision that it did not "refer to the existence of effective legal protection against interference"[15], and clarify that the US is nowhere near the hypothetical situation of having no

[14] CJEU 6 October 2015, Case C-362/14, Maximillian Schrems v. Data Protection Commissioner, ECLI:EU:C:2015:650, para. 76.

[15] Schrems, para. 89.

redress options at all ("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" would interfere with "the fundamental right to judicial protection").[16]

First, the Privacy Shield makes available a judicial remedy to obtain rectification or erasure by establishing recourse to an arbitration panel, whose decisions are appealable under the Federal Arbitration Act.[17]

A second avenue stems from the recommendation of the 2013 Safe Harbour Communication that alternative dispute resolutions be "readily available and affordable." Principle 7 and Supplemental Principles 11 (d) on recourse mechanisms accomplishes this by requiring that subscribing companies make independent recourse mechanisms available "*free of charge to individuals".* (Annex II, pages 22, 38). Additionally, in Annex I the Commerce Department undertakes to facilitate resolution of disputes referred by DPAs, again with no fees to the individual (page 10). The Notice Principle enhances the functioning of alternative dispute resolution by requiring clearer identification of the redress bodies available (page 19), and the Supplemental Principles define timelines for meaningful resolution (page 38).

Finally, in addition to the Commerce Department responding to complaints referred by DPAs, the Recourse, Enforcement and Liability Principle strengthens the role of supervising authorities in dispute resolution by providing for companies to elect to have complaints go to DPAs, and *requiring* that companies that receive human resources data from the EU do so (page 23). These provisions make it possible for individuals in the EU to go to DPAs and, if DPAs so desire, to receive assistance from these bodies. The ability of DPAs to refer complaints makes it possible for individuals in the EU to bring their complaints to their national supervising authorities rather than US bodies, and for DPAs to act as intermediaries as suggested by WP29.[18]

These multiple avenues of redress in relation to companies[19] ensure that EU data subjects have accessible and affordable recourse that makes it possible to pursue a judicial remedy. The final Decision addresses the concern shared by the WP29, Parliament, and EDPS that these redress choices could be confusing by providing a clear roadmap to the choices and process in "a certain logical order that is advisable to follow". Together with clear and simple notices and

[16] Schrems, para. 95.

[17] Annex I, pages 12-15. The Federal Arbitration Act, 9 U.S.C. §§ 1 *et seq*., provides for arbitration of agreements within federal jurisdiction; Section 4 provides for judicial enforcement of agreements to arbitrate and Section 16 allows appeals of an arbitrator's final decision to a federal court.

[18] WP238, page 27.

[19] For remedies in case of government surveillance, see pages 10 *et seq.* below.

other publicly accessible explanations, the Commission's roadmap will enable individuals to choose the path most convenient and suitable for them.

5. The strengthened protections of the Privacy Shield establish the effective supervision and detection mechanisms required by the CJEU.

In the *Schrems* judgment, the CJEU held that a system of self-certification like that in the Privacy Shield can be consistent with Article 25(6) of Directive 95/46 provided it establishes "effective detection and supervision mechanisms" to detect and punish fundamental rights to private life and data protection (Schrems, para. 81). The increased scrutiny of certifications and intensified oversight by the Commerce Department; the cooperation among that agency, the FTC, the Commission, and DPAs; and expanded and clearer ways for individuals to protect their rights themselves provide effective detection and supervision mechanisms in the Privacy Shield.

In addition to these Privacy-Shield-specific mechanisms, as shown in the Sidley Austin LLP report, *Essentially Equivalent: a comparison of the legal orders for privacy and data protection in the European Union and United States* (January 2016),[20] the general legal order for privacy and protection in the US has changed significantly since 2000, when the Commission approved the Safe Harbour framework. In that time, the US has adopted new sectoral laws and regulations for sensitive data such as health records, financial, and genetic information; data breach notification laws in most states along with other state laws; the FTC role along with that of other agencies has expanded significantly; and privacy officers have become common and influential in US companies. Compared to the earlier framework, the Privacy Shield has much less to supplement in order to ensure that EU citizens retain an equivalent level of protection when data is transferred to the US.

Against this backdrop, the increased detail and force in the Privacy Shield framework will ensure that personal data transferred to the US receives protection of fundamental rights and freedoms that is essentially equivalent to that in the EU.

[20] See *http://datamatters.sidley.com/wp-content/uploads/2016/01/Essentially-Equivalent-Final-01-25-16-9AM3.pdf*

The Major Points of Concern Raised by EU Institutions Are Addressed by the Privacy Shield Framework.

The European Commission published its draft Privacy Shield Adequacy Decision on 29 February 2016. Since then, the WP29, EDPS, and Parliament each have weighed in on the draft Decision. In turn, the Commission and the US Government have taken into account concerns raised by these bodies by clarifying and adding to the principles and annexes in the final Decision. The Decision integrates this content into a coherent whole that explains and clarifies how the Privacy Shield addresses the issues raised.

In Opinion 238, the WP29 noted that the Privacy Shield reflects "many improvements" over the Safe Harbour framework. The WP29 nevertheless expressed "three major points of concern" (page 57): (A) a perceived absence of rules on deleting data; (B) a perceived failure to exclude absolutely any large-scale data collection; and (C) the contribution of the Privacy Shield Ombudsperson to the US redress system. The Parliament and the EDPS each echoed these concerns. The former suggested that the language regarding bulk collection "does not meet the stricter criteria of and proportionality as laid down in the Charter" and the latter suggested a need to get "additional reassurances in terms of necessity and proportionality", and both expressed a need for greater clarity in general.

The final Decision and revisions to the annexes from the Commerce Department, State Department, and Office of Director of National Intelligence (ODNI) reflect the lengths the Commission and US Government have gone to address concerns from these bodies. Some of these revisions and clarifications have been touched in the foregoing pages. This section addresses the three recurring major points.

1. The Data Integrity and Purpose Limitation Principle encompasses deletion of data that is no longer relevant or current.

The Data Integrity and Purpose Limitation Principle in the Privacy Shield is an expression of the "data quality and proportionality principle" in Article 6(1)(e)[21] of Directive 95/46. Although neither that article nor subsequent WP29 adequacy opinions contain explicit language on data deletion, the WP29 expressed concern that the language in the draft adequacy decision did not expressly oblige organisations to delete data that become no longer necessary or obsolete.

The final Decision and Principles accommodate this concern by adding to the Data Integrity and Purpose Limitation Principle a requirement that "[i]nformation

[21] Pursuant to Article 6(1) of the Data Privacy Directive, "Member States shall provide that personal data must be (…) "(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed. Member States shall lay down appropriate safeguards for personal data stored for longer periods for historical, statistical or scientific use".

may be retained in a form identifying or making identifiable the individual only for so long as it serves a purpose of processing [as defined in the prior provision]". This tracks the language of Article 6(1(e) while also incorporating notes and exceptions that anticipate GDPR treatment of "compatible processing", public interest purposes, and re-identification.

2. The findings and reasoning in the draft Adequacy Decision concerning safeguards on US government surveillance are consistent with EU jurisprudence.

In its Opinion 238, the WP29 recognised that to date in the EU "there is no conclusive jurisprudence on the legality of massive and indiscriminate data collection and subsequent use of personal data for the purpose of combating crime, including the question under what circumstances such collection and use of personal data could take place" (page 39).

WP29 nevertheless expressed a concern that Annex VI of the draft Adequacy Decision (the letter from the US ODNI "does not fully exclude the continued collection of massive and indiscriminate data",[22] and stated its view that "such data collection, is an unjustified interference with the fundamental rights of individual". Given the WP29's characterisation of EU jurisprudence, this view appears to reflect mainly a policy statement. Similar views were voiced in the Parliament resolution and EDPS opinion as well.

In a long line of cases, the European Court of Human Rights ("ECtHR") has confirmed that Member States have a margin of discretion in setting national rules for collection, storage, and subsequent use of data for national security purposes that is "necessary in a democratic society". In its Opinion WP 237 of 13 April 2016, the WP29 acknowledged that Member States have a "fairly wide margin of appreciation in choosing the means for achieving the legitimate aim of protecting national security" (page 5). This approach, laid down in ECtHR case law since *Klass v. Germany*[23] and again in *Weber and Saravia*[24] shows, for example, that a far-reaching surveillance mechanism must be accompanied by far-reaching safeguards, oversight, and redress. The more intrusive a surveillance mechanism is, and the more "prone to abuse", the higher the safeguards against abuse must be. No particular method of surveillance as such has ever been condemned. The Commission correctly noted in point 89 (footnote 98) of the Decision that the ECtHR has confirmed that "strategic

[22] A note on the terminology used by the WP29 and EDPS: the CJEU did not use the term "collection of mass and indiscriminate data" in its legal reasoning in *Schrems*. The referring Irish High Court used the term "mass and undifferentiated" but only in relation to *accessing* (Schrems, para. 33).

[23] ECtHR [Plenary Court] 6 September 1978, Klass & Others v. Germany, ,ECLI:CE:ECHR:1978:0906JUD000502971.

[24] ECtHR 29 June 2006, Weber & Saravia v.Germany (admissibility decision), ECLI:CE:ECHR:2006:0629DEC005493400.

surveillance" covering "a broader range of possible actors" and "a wider geographic area" are permitted under the *Weber and Saravia* case law.

In its Working Document on justification of interferences with fundamental rights of privacy and data protection issued on 13 April 2016 ("WP 237"),[25] the WP29 provided a nuanced and thoughtful overview of the criteria for such safeguards in the case law of the CJEU and especially the ECtHR, and correctly distilled from this jurisprudence four "Essential Guarantees" against abuse of surveillance mechanisms. These are (A) clear, precise and accessible rules; (B) demonstration of necessity and proportionality; (C) independent oversight; and (D) effective remedies. The WP29 also acknowledged that proportionality in light of these four Essential Guarantees must not be assessed independently, but on an overall basis.

As noted above, there is no rule in EU law that condemns the collection of data *as such* even if collection occurs on a large scale. In *Schrems* and *Digital Rights Ireland*, the CJEU invalidated EU legislative acts because they enabled large-scale collection or storage without providing safeguards against abuse and without limiting data access. The CJEU differentiated *collection and storage* of personal data, which by themselves do not affect the "essence" of data privacy rights, in contrast to *access*, which does have such effect;[26] and discussed objections against unlimited storage and against unlimited access separately. The CJEU indicated it would object to "*storage* of all the personal data of all the persons whose data has been transferred" where such storage is "without any differentiation, limitation or exception being made, and without an objective criterion … by which to determine the limits of the *access*" (*Schrems*, para. 93, emphasis added). The CJEU also would object to "access on a generalised basis to the content of electronic communications" (*Schrems*, para. 94).

As shown in the report by European Union Agency for Fundamental Rights, *Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU* (2015),[27] and the Sidley Austin *Essentially Equivalent* report referred to above, the laws of a number of EU Member States authorize forms of untargeted surveillance and many Council of Europe countries conduct forms of "bulk, untargeted surveillance by security services".

Moreover, on 20 April 2016, the European Commission published its Communication delivering on the European Agenda on Security to fight against terrorism and pave the way towards an effective and genuine Security Union

[25] WP29 13 April 2016, Working Document 01/2016 on the justification of interferences with the fundamental rights to privacy and data protection through surveillance measures when transferring personal data (European Essential Guarantees, WP 237, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2016/wp237_en.pdf.

[26] Schrems, para. 93/94; CJEU 8 April 2014, Case C-293/12, Digital Rights Ireland, ECLI:EU:C:2014:238, para. 40.

[27] http://fra.europa.eu/en/publication/2015/surveillance-intelligence-services

COM (2016) 230.[28] This Communication recalls that the EU Treaties envisage the need to ensure a high level of security, including through preventive measures. The plans include:

- "a European common repository of data and EU-integrated biometric identity management for travel, migration and security";
- "an EU Entry Exit System for the EU External border using biometrics, providing for law enforcement access and interoperability with other systems (notably the Visa Information System)"; and
- "The existing Prüm framework must be implemented and used fully. It offers automated comparison of DNA profiles, fingerprint data and vehicle registration data".

The WP29 suggested that the *Tele2* and *Davis* cases[29] pending before the CJEU may change the existing legal order. However, neither case is about "massive and indiscriminate data collection and subsequent use". Rather, these cases involve collection and storage of telecommunications metadata for a limited amount of time, where storage and subsequent use are subject to limitations laid down by national law (as opposed to the general absence of such limits in the Data Retention Directive, the subject of the CJEU judgment in *Digital Rights Ireland*).

In considering the US legal order governing surveillance, WP29 correctly noted that the Foreign Intelligence Surveillance Act ("FISA") does not permit mass and indiscriminate surveillance, and "does not operate by collecting communications in bulk" (WP238, p. 39). The WP29 nevertheless appeared to consider that data transferred to the US are protected only by Presidential Policy Directive 28 ("PPD 28") and Executive Order 12,333. This understanding does not take into account that once such data are within the US, the US government's ability to collect, store, and access these is also constrained by several federal statutes, including FISA and the Electronic Communications Privacy Act ("ECPA").

FISA – including Title I, Section 501, and Section 702 – expressly requires judicial orders authorising collection, and it mandates the use of discriminants when collecting data. The USA FREEDOM Act specifically amended Section 501, which authorises collection of metadata, to prohibit bulk surveillance. Opinion WP238 does not mention ECPA, though it is discussed in Annex VI. This statute governs law enforcement's collection and use of data and requires

[28] http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/european-agenda-security/legislative-documents/docs/20160420/communication_eas_progress_since_april_2015_en.pdf

[29] Case C-203/15, Tele2 Sverige AB v. Post- och telestyrelsen; Case C-698/15, Secretary of State for the Home Department v. David Davis, Tom Watson, Peter Brice, Geoffrey Lewis, intervening parties: Open Rights Group, Privacy International, The Law Society of England and Wales, expedited procedure granted by Order of the President of the Court of Justice of 1 February 2016, ECLI:EU:C:2016:70. See WP238, p. 39.

judicial authorisation and the use of discriminants to collect the contents of communications. These protections apply to all data received or stored in the United States, regardless of the sender's or owner's citizenship.

The WP29 nonetheless focused on the statement in Annex VI that US law does not entirely exclude bulk collection in certain circumstances, but, as the statutes above make clear, the latter caveat does not affect data transferred to the US under the Privacy Shield. Like any EU Member State, the US can engage in surveillance activities *outside of its own territory* to protect its national security interests[30] (the example in a supplemental letter from the ODNI in Annex VI is "a terrorist group in a region of a Middle Eastern country, that is believed to be plotting attacks against Western European countries") and the Decision notes that foreign intelligence collection as defined in US law is "a legitimate policy objective" (pages 23-24). Such surveillance outside the United States has no bearing on the question whether the transfer of personal data from the EU to the US by Privacy Shield companies would lower the level of protection accorded to such data.

Moreover, Annex VI as further clarified by the additional letter from the ODNI makes clear that the circumstances in which such surveillance outside the US can occur are strictly limited – "to identify new and emerging threats and other vital national security interests" within six enumerated purposes – and subject to "the application of methods and tools to filter collection in order to focus collection" on these specific purposes as further refined by policy-makers (pages 79-81, 95-96).

Responding to recommendations to clarify this issue, the Commission in turn expanded its review in the final Decision, stressing the limitation under the law to specifically identified purposes, to persons who may have some connection to these purposes, and in circumstances where it is not feasible to target such persons specifically. This meets the standard articulated by the EDPS that untargeted surveillance access "should only take place in exceptional circumstances and where indispensable for specified public interest purposes".[31] On this basis, the Commission properly concludes that US intelligence collection in this regard is limited "to what is strictly necessary to achieve the legitimate objective in question".

The WP29 and the EDPS raised a concern about the mere possibility of interception of data in transit (through access to transatlantic cables or otherwise). Such collection would have no direct impact on the question whether the act of transferring such data to the US by Privacy Shield companies would lower the level of protection accorded to such data. Moreover, as WP29 recognised, "there continues to be a lack of established jurisprudence determining the legality of cables interception if it were to be carried out by any

[30] United Nations Charter, art. 51 (1945).

[31] EDPS Opinion, page 2.

country" (WP238, page 36). In other words, there appears to be agreement that cable interception – if it were to occur – would not necessarily infringe EU law or any other laws.

For the sake of completeness, it must be noted that the EU could not hold the US to a rule that does not exist in the EU legal order. It would be a plain violation of the GATT and GATS rules if the EU were to prevent data flows to the US on the basis of a "generic risk" that data flowing through cables can be intercepted, whilst permitting data flows between Member States that are subject to precisely the same considerations or data flows to third countries where data transfers may be subject to the same sorts of surveillance that the WP29 raises as concerns.[32]

Combined with the limitations set out above, these facts show that it is not possible to regard US laws as legislation that "authorizes, 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" (*Schrems*, para. 93).

As shown in the Adequacy Decision, the laws that apply to data that is transferred by companies that subscribe to the Privacy Shield framework contain (A) clear, precise and accessible rules; (B) demonstration of necessity and proportionality; (C) independent oversight; and (D) effective remedies that are consistent with the four Essential Guarantees distilled from EU jurisprudence. Dutch Security and Justice Minister van der Steur concluded in his brief to the Dutch Parliament, "with what the Commission has achieved, in my view the recommendations from the abovementioned 2013 Communication of November 2013, relating to government access to data transferred to the US pursuant to the Shield, have been followed".[33]

3. The Privacy Shield Ombudsperson will have sufficient authority to perform a complaint review function similar to that of EU supervisory authorities that adds to the avenues of judicial redress available.

The WP29 recognised that the commitment to an Ombudsperson to respond to individual EU complaints is an "unprecedented step creating an additional oversight and redress mechanism" relating to government surveillance (WP238,

[32] As noted in each of the existing Article 25(6) decisions, these decisions are subject to the EU's international trade law obligations. For at least eight of the eleven such decisions (Argentina, Canada, Switzerland, Faeroe Islands, Israel, Isle of Man, New Zealand and Uruguay), this includes the principles of National Treatment/Most Favoured Nation treatment and the obligation to "administer measures on a reasonable way" (GATS Articles II, XVII, XVI:2(a); GATT 1994, Articles I:1, III:4; X:3(a)). Data privacy protection measures cannot constitute "a means of arbitrary or unjustifiable discrimination between countries where like conditions prevail" (GATT 1994, Article XX(d)).

[33] "Kamerbrief over EU US Privacy Shield", page 12 (29 April 2016), https://www.rijksoverheid.nl/documenten/kamerstukken/2016/04/29/tk-brief-eu-us-privacy-shield.

p. 57). In response to desire for clarification of the Ombudsperson's powers on the part of the WP29 and EDPS, the US Department of State has provided additional explanation of the Ombudsperson's independence from and powers over intelligence agencies.

As explained in Annex III, the Department of State submission, and reflected in the Commission decision, the official designated as the Ombudsperson is the Under Secretary of State for Economic Growth, Energy & Environment. This Under Secretary is nominated by the President and confirmed by the US Senate, reports directly to the Secretary of State, and is outside the chain of command of those branches of the State Department that deal with national security and intelligence (page 53). The Department of State clarifies that the Secretary will ensure that this official can carry out the Ombudsperson "objectively and free from improper influence", and that that Ombudsperson will be able to refer questions of the lawfulness of surveillance to independent bodies with investigatory powers (which are described in the Annex at pages 57-59).

This same Under Secretary is delegated authority under PPD-28, the presidential order that directs US agencies that "[a]ll persons should be treated with dignity and respect, regardless of their nationality or where they might reside, and all persons have legitimate privacy interests in the handling of their personal". PPD-28 vests the authority "to coordinate with the responsible departments and agencies" and "to serve as a point of contact for foreign governments who wish to raise concerns regarding signals intelligence activities conducted by the United States". The functions of the Privacy Shield Ombudsperson are a specific application of this general authority, and therefore will bring to bear the coordinating authority conferred by the President.

The Privacy Shield charges the Ombudsperson to investigate and to establish that US laws and policies have been followed or that any noncompliance has been remedied, without disclosing either whether the complaining individual has been a target of surveillance or what specific remedy may have been applied (page 55). This function is modeled on the role of certain administrative supervisory agencies in the EU. In France and in Italy, for example, the CNIL and the Garante respectively, may review surveillance at the request of individuals, but their review is limited to the regularity under national laws and rules, and they do not confirm or deny surveillance or disclose the disposition of the matter.

To be sure, the Ombudsperson will not be a quasi-judicial tribunal, as the WP29 seems to suggest it should be, but the test is not whether the US has adopted avenues of redress that are identical to those in Europe. The test is whether the US provides protection essentially equivalent to the level of protection guaranteed within the EU.

The applicable standard guaranteed within the EU does not tolerate "legislation not providing for any possibility for an individual to pursue legal remedies". This does not mean that the EU legal order guarantees universal and automatic

redress in every single situation. Indeed, the case law of the ECtHR specifically notes that data subjects' rights of redress must be balanced in situations of security surveillance – and, as a result, there is no universal or automatic right of redress. As the Plenary Court Judgment in *Klass v. Germany* noted, "an effective remedy" under Article 13 of the ECHR (the article corresponding to Article 47 of the Charter) "must mean a remedy that is as effective *as can be* having regard to the restricted scope for recourse inherent in any system of secret surveillance" (para. 69, emphasis added). Moreover, the ECtHR does not provide or require automatic redress, either. There is no *actio popularis*,[34] and there is no remedy against the "state of domestic law".[35]

There are no grounds to assume that the US falls short of this standard. In addition to the Ombudsperson introduced by the Privacy Shield, the US has multiple other avenues of redress for unlawful surveillance, which merit more attention than accorded in the WP29 Opinion. The Commission Decision adds several paragraphs setting out these remedies (recitals 130-134).

For instance, while it is correct that the Fourth Amendment to the US Constitution alone does not apply to non-US citizens located outside the United States (though PPD-28 extends equivalent protections), there are statutory causes of action that are available to such persons independent of the Fourth Amendment. The WP29 does not address ECPA, which provides criminal sanction as well a civil cause of action for "any person whose wire, oral, or electronic communication is intercepted, disclosed, or intentionally used" in violation of the Act.[36] The federal courts have concluded that this cause of action is open to foreign citizens.[37]

Similarly, under FISA, "an aggrieved person, other than a foreign power or an agent of a foreign power, . . . who has been subjected to an electronic surveillance or about whom information obtained by electronic surveillance of such person has been disclosed or used in violation of section 1809 of this title shall have a cause of action against any person who committed such violation".[38] WP29 dismisses this cause of action as insufficient because it

---

[34] See, by analogy, Klass v. Germany, para. 33: "Article 25 (art. 25) does not institute for individuals a kind of actio popularis for the interpretation of the Convention; it *does not permit individuals to complain against a law in abstracto simply because they feel that it contravenes the Convention*" (emphasis added).

[35] Szabó para. 93: "The Court reiterates that Article 13 cannot be interpreted as requiring a remedy against the state of domestic law (see Ostrovar v. Moldova, no. 35207/03, § 113, 13 September 2005; Iordachi, cited above, § 56). In these circumstances, the Court finds no breach of Article 13 of the Convention taken together with Article 8."

[36] 18 U.S.C. § 2520(a).

[37] *See, e.g.*, Suzlon Energy Ltd. v. Microsoft Corp., 671 F.3d 726, 731 (9th Cir. 2011); *see also* Privacy and Civil Liberties Oversight Board, *Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act* 99 n.444 (July 2, 2014) (citing *Suzlon* for the proposition that "any person" includes "non-U.S. persons").

[38] 50 U.S.C. § 1810.

excludes foreign powers and their agents. But FISA defines a foreign power specifically as a foreign nation, an entity controlled by a foreign government, or an international terrorist organization, and an agent of a foreign power as a person acting on behalf of a foreign government or terrorist organization.[39] These definitions do not encompass ordinary citizens of another country. FISA therefore provides another clear available redress mechanism for such citizens.

The WP29 also views the doctrine of "standing" as a significant obstacle to obtaining meaningful judicial redress in the United States. It is not accurate to state that such a requirement "nullifie[s]" the availability of review or even that it makes bringing a legitimate suit "very difficult". The federal courts have concluded on multiple occasions that standing exists to challenge bulk and mass surveillance.[40] A standing threshold is a common legal standard to multiple comparable legal orders, including to related doctrines governing the jurisdiction of various Member States' courts. It does not bar the doors of court to those with concrete reasons to believe their rights have been violated.

In addition to these specific avenues of judicial redress, the US has what the WP29 acknowledges is "a multi-layered approach of both internal and external oversight mechanisms". These include internal agency controls, independent inspectors general within each agency, several congressional committees, the independent Privacy and Civil Liberties Oversight Board, and review by independent judges of a federal court under FISA. The totality of these multiple oversight mechanisms compares favorably to the powers of the UK Investigatory Powers Tribunal approved in the ECtHR *Kennedy* decision.

Against this background, it is valid to conclude that the system of legal redress in the US provides protection that is essentially equivalent to the protection guaranteed in the EU legal order.

[39] 50 U.S.C. § 1801(a), (b).

[40] *See, e.g.*, Am. Civil Liberties Union v. Clapper, 785 F.3d 787, 800-01 (2d Cir. 2015) (holding that plaintiffs have standing to challenge Section 215 metadata program); Klayman v. Obama, --- F. Supp. 3d ---, 2015 WL 6873127, at *8 (D.D.C. Nov. 9, 2015) (same), *stay granted*, 2015 WL 9010330 (D.C. Cir. Nov. 16, 2015).

CONCLUSION

Spurred by the outcome and the principles in the CJEU *Schrems* judgment and with the input of EU institutions, the Privacy Shield negotiators have produced a robust and detailed framework to protect data that are transferred to the United States. The test is not whether the safeguards in the US subject to this framework are either identical to those in the EU or perfect in all respects. The test is the practical effect of these safeguards, and the framework provides ample opportunity to address ongoing issues through the annual review process.

The Commission's conclusion that "the United States ensures an adequate level of protection for personal data transferred under the EU-U.S. Privacy Shield from the Union to self-certified organizations in the United States" is well supported by the evidence discussed in the Privacy Shield Decision and should stand up to legal challenge.

Cameron F. Kerry
Sidley Austin LLP, Boston

Maarten Meulenbelt
Sidley Austin LLP, Brussels

Sidley Austin LLP represents international clients on data transfers and privacy and data protection matters.

ABOUT THE AUTHORS

Sidley Austin LLP is a premier global law firm celebrating its 150th anniversary in 2016. With more than 1,900 lawyers and 20 offices worldwide, the firm provides a broad range of services to meet the needs of large and small businesses and other organizations across a multitude of industries, forums and governments. Sidley has a broad transactional practice and consistently ranks among the top global capital markets firms. Sidley also has an extensive litigation and arbitration practice, spanning nearly every area of substantive law. The firm also provides regulatory counseling and advocacy regarding communications, energy, environmental, food, drug and device, healthcare, insurance, Internet, life sciences, financial and securities law, and represents clients in virtually every major industry. Sidley is rated among the top law firms, recognized in the United States and globally for service and responsiveness, and widely recognized for its pro bono and diversity programs.

Sidley's Privacy, Data Security and Information Law practice group is a global and interdisciplinary team of lawyers focused on a broad range of emerging issues, including privacy and data protection; cybersecurity and data breach preparedness and response; Big Data; government surveillance; data localization; Internet law; cross-border data flows; and e-Commerce. The group handles litigation and investigations, cybersecurity compliance and regulatory counseling, data breach incident response, legislative and policy developments and sector-specific counseling internationally. Clients cover a broad range of industries. The practice and its lawyers consistently rank in the top tiers of *Chambers USA*, *Chambers Global*, and *The Legal 500*.

Cameron F. Kerry
Senior Counsel
Boston
ckerry@sidley.com
+1 617 223 0305

Cameron F. Kerry is senior counsel in Sidley's Boston and Washington, D.C. offices. He is former General Counsel and Acting Secretary of the United States Department of Commerce, where he played a leadership role in consumer privacy issues and the flow of information and technology across international borders, including on the EU-U.S. Safe Harbour Framework. Cam is also a visiting scholar with the MIT Media Lab and a frequent speaker and writer on privacy and the digital economy. At Sidley, his broad practice operates at the intersection of law, technology and public policy, and is informed by his years of government service and more than three decades in private practice.

Maarten Meulenbelt
Partner
Brussels
mmeulenbelt@sidley.com
+32 2 504 6467

Maarten Meulenbelt is a partner in Sidley's Brussels office. He has extensive litigation experience before the EU Courts, national courts and competition authorities, the European Commission and national regulatory authorities in several EU Member States with a specific focus on the life sciences sector. He is a member of Sidley's Privacy, Data Protection and Information Law, Global Life Sciences and Antitrust practices focusing on EU regulatory affairs, litigation and competition law issues affecting clients in Europe.

SIDLEY
150 YEARS

sidley.com

AMERICA • ASIA PACIFIC • EUROPE

MN-4314-07/16