these kinds of lines of communication and ability to talk beyond the scope of the nuclear agreement are promising.[123]

European Union and United States Conclude Agreement to Regulate Transatlantic Personal Data Transfers

On February 2, 2016, the European Union and United States concluded the EU-U.S. Privacy Shield, a political agreement that "was designed by the U.S. Department of Commerce and European Commission to provide companies on both sides of the Atlantic with a mechanism to comply with EU data protection requirements when transferring personal data from the European Union to the United States in support of transatlantic commerce."[1] Personal data covered by the agreement includes "online search queries, financial information, and employee records"[2] that facilitate targeted advertising, customer tracking, and employee management.[3] The Privacy Shield replaces the Safe Harbor framework, the agreement that had previously applied to such transfers.[4]

The European Union and United States had started negotiating a replacement for the Safe Harbor framework in 2013.[5] Concluding those negotiations became more urgent after the Court of Justice of the European Union (CJEU) identified shortcomings in the European Commission's implementation of the Safe Harbor Framework in a ruling published in October 2015.[6] The ruling required more robust protections for the transfer of personal data from EU member states to the United States in order to conform to fundamental guarantees under EU law.[7] EU and U.S. officials have stated that the new framework establishes "stronger

[123] U.S. Dep't of State Press Release, Daily Press Briefing (Jan. 13, 2016), *at* http://www.state.gov/r/pa/prs/dpb/2016/01/251198.htm.

[1] Privacy Shield Agreement, EU-U.S., Feb. 2, 2016, *at* https://www.commerce.gov/sites/commerce.gov/files/media/files/2016/eu_us_privacy_shield_full_text.pdf.pdf [hereinafter Privacy Shield]; *Fact Sheet: Overview of the EU-U.S. Privacy Shield Framework*, DEP'T OF COMMERCE (Feb. 29, 2016), *at* https://www.commerce.gov/news/fact-sheets/2016/02/fact-sheet-overview-eu-us-privacy-shield-framework [hereinafter Dep't of Commerce Fact Sheet]. S*ee also European Commission Unveils EU-U.S. Privacy Shield*, EUROPEAN COMMISSION (Feb. 29, 2016), *at* http://ec.europa.eu/justice/newsroom/data-protection/news/160229_en.htm; European Commission Press Release, EU Commission and United States Agree on New Framework for Transatlantic Data Flows: EU-U.S. Privacy Shield (Feb. 2, 2016), *at* http://europa.eu/rapid/press-release_IP-16-216_en.htm [hereinafter EC Feb. 2 Press Release] (describing the Privacy Shield as a political agreement).

[2] Mark Scott, *European Privacy Regulators Want Details on "Safe Harbor" Data Deal*, N.Y. TIMES, Feb. 3, 2016, at B3.

[3] Andrea Peterson, *The Massive New Privacy Deal Between U.S. and Europe, Explained*, WASH. POST (Feb. 2, 2016), *at* https://www.washingtonpost.com/news/the-switch/wp/2016/02/02/the-massive-new-privacy-deal-between-u-s-and-europe-explained/.

[4] *Safe Harbor Privacy Principles*, U.S. DEP'T OF COMMERCE (July 21, 2000), *at* http://web.archive.org/web/20150908060809/http://export.gov/safeharbor/eu/eg_main_018475.asp. *See also* DEP'T OF COMMERCE, U.S.-EU SAFE HARBOR FRAMEWORK: A GUIDE TO SELF-CERTIFICATION (2009) [hereinafter SAFE HARBOR FRAMEWORK], *available at* http://trade.gov/media/publications/pdf/safeharbor-selfcert2009.pdf.

[5] European Commission Press Release, European Commission Calls on the U.S. to Restore Trust in EU-U.S. Data Flows (Nov. 27, 2013), *at* http://europa.eu/rapid/press-release_IP-13-1166_en.htm.

[6] Case C-362/14, Maximillian Schrems v. Data Protection Comm'r (June 25, 2013), *at* http://curia.europa.eu/juris/celex.jsf?celex=62001CJ0286&lang1=en&type=TXT&ancre= [hereinafter Schrems]. *See also* Megan Graham, *Adding Some Nuance to the European Court's Safe Harbor Decision*, JUST SECURITY (Oct. 7, 2015), *at* https://www.justsecurity.org/26651/adding-nuance-ecj-safe-harbor-decision/.

[7] *See* Article 29 Working Party, Statement of the Article 29 Working Party (Oct. 16, 2015), *at* http://ec.europa.eu/justice/data-protection/article-29/press-material/press-release/art29_press_material/2015/20151016_wp29_statement_on_schrems_judgement.pdf [hereinafter Article 29 Working Party Statement]. *See also* Zoya Sheftalovich, *The Phone Call that Saved Safe Harbor*, POLITICO (Feb. 5, 2016), *at* http://www.politico.eu/article/the-phone-call-that-saved-safe-harbor-john-kerry-frans-timmermans/.

obligations on companies in the U.S.,"[8] including stricter conditions for transfer of data to third parties for processing;[9] more robust redress mechanisms, including the possibility of cost-free, binding arbitration;[10] a new procedure to address complaints stemming from government access to personal data for national security purposes;[11] and stronger oversight by and cooperation between EU and U.S. agencies, including a joint annual review of compliance with the framework.[12]

The impetus for negotiating the Privacy Shield and its predecessor, the Safe Harbor framework, is a Data Protection Directive that the EU legislature issued in 1995.[13] That Directive regulates data flow within and from the EU; it requires EU member states to prohibit transfers of personal data to third countries outside the EU unless the third country to which data is transferred "ensures an adequate level of protection."[14] The Directive provides that "[t]he adequacy of the level of protection afforded by a third country shall be assessed in the light of all the circumstances surrounding a data transfer operation or set of data transfer operations."[15] The Directive also provides that that the European Commission may find "that a third country ensures an adequate level of protection . . . by reason of its domestic law or of the international commitments it has entered into . . . for the protection of the private lives and basic freedoms and rights of individuals."[16]

Following consultation with the European Union, industry, and public, the U.S. Department of Commerce issued Safe Harbor Privacy Principles for use by private U.S. firms "for the purpose of qualifying for the safe harbor and presumption of 'adequacy' [under European law] it creates."[17] Participating companies self-certified that they adhered to Safe Harbor's principles relating to notice, choice, data transfer to third parties, access, security, data integrity, and enforcement.[18] Participation in Safe Harbor was voluntary.[19] (Companies that chose not to

[8] European Commission Press Release, EU-U.S. Privacy Shield: Frequently Asked Questions (Feb. 29, 2016), *at* http://europa.eu/rapid/press-release_MEMO-16-434_en.htm; Privacy Shield, *supra* note 1, at 5 (Letter from Under Secretary for Trade Stefan Stelig to EU Commissioner Vera Jourova (Feb. 23, 2016)).

[9] *See infra* notes 48–50.

[10] *See infra* notes 60–61.

[11] *See infra* notes 66–68.

[12] *See infra* note 43.

[13] 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 O.J. (L. 281) [hereinafter Data Protection Directive]. The Directive will be replaced by the General Data Protection Regulation, which will create a "single set of rules" regarding the transfer of personal data while increasing mechanisms for individuals' access to information on how their data is processed. European Commission Press Release, Agreement on Commission's EU Data Protection Reform will Boost Digital Single Market (Dec. 15, 2015), *at* http://europa.eu/rapid/press-release_IP-15-6321_en.htm.

[14] Data Protection Directive, *supra* note 13, Art. 25(1).

[15] *Id.* Art. 25(2). This provision continues: "[P]articular consideration shall be given to the nature of the data, the purposes and duration of the proposed processing operation or operations, the country of origin and country of final destination, the rule of law, both general and sectoral, in force in the third country in question and the professional rules and security measures which are complied with in that country." *Id.*

[16] *Id.* Art. 25(6).

[17] SAFE HARBOR FRAMEWORK, *supra* note 4, at 10.

[18] *Id*. at 4–6.

[19] *Id*. at 4 ("The decision by U.S. organizations to enter the Safe Harbor is entirely voluntary. Organizations that decide to participate in the Safe Harbor must comply with the Safe Harbor's requirements and publicly declare that they do so. To be assured of Safe Harbor benefits, an organization needs to self-certify annually in writing to the Department of Commerce that it agrees to adhere to the Safe Harbor's requirements, which include elements such

participate in the Safe Harbor framework but wished to transfer data from the European Union to the United States had to find another legal basis for the transfer of data and remained subject to enforcement action by European data protection authorities.[20])

In 2000, the European Commission determined that the Safe Harbor principles for the transfer of data to the United States "are considered to ensure an adequate level of protection for personal data."[21]

In 2013, Austrian national Maximillian Schrems filed a complaint with the Irish Data Protection Commissioner seeking to enjoin Facebook's Irish subsidiary (and headquarters for Facebook's European operations) from transferring his personal data to Facebook's servers in the United States. Citing Edward Snowden's revelations regarding the National Security Agency's mass surveillance programs,[22] Schrems argued that the "law and practice in force in [the United States] did not ensure adequate protection of the personal data held in its territory against the surveillance activities that were engaged in there by the public authorities."[23]

The Irish Data Protection Commissioner denied Schrems's request, citing the Commission's 2000 adequacy decision.[24] Schrems then brought an action before the Irish High Court.[25] Recognizing that Schrems's suit challenged the European Commission's 2000 adequacy decision, the Irish High Court asked the CJEU for a ruling on whether national-level supervisory authorities, such as the Irish Data Protection Commissioner, were "absolutely bound" by the 2000 decision—or whether such supervisory authorities could independently investigate challenges to the adequacy of protections provided by third states.[26]

In its ruling in *Maximillian Schrems v. Irish Data Protection Commissioner*, the CJEU ultimately concluded that the Commission's 2000 adequacy decision regarding the Safe Harbor

as notice, choice, access, and enforcement. It must also state in its published privacy policy statement complies with the U.S.-EU Safe Harbor Framework and that it has certified its adherence to the Safe Harbor Privacy Principles."). *See also* Mark Scott, *U.S. and Europe in "Safe Harbor" Data Deal, but Legal Fight May Await*, N.Y. TIMES, Feb. 2, 2016, at B1.

[20] For example, as an alternative, parties might use Standard Contractual Clauses. *See* EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS & COUNCIL OF EUROPE, HANDBOOK ON EUROPEAN DATA PROTECTION LAW 137 (2014), *available at* http://www.echr.coe.int/Documents/Handbook_data_protection_ENG.pdf. Both the data-exporting controller and third-party recipient (the American company) would sign the clause, which had been developed by the European Commission. This, in turn, would "provide the supervisory authority with sufficient proof that adequate safeguards are in place." *Id.* at 137. *See also Model Contracts for the Transfer of Personal Data to Third Countries*, EUROPEAN COMMISSION (Feb. 12, 2015), *at* http://ec.europa.eu/justice/data-protection/international-transfers/transfer/index_en.htm.

[21] Commission Decision 2000/520/EC, 2000 O.J. (L 215) 8.

[22] Schrems, *supra* note 6, para 28. *See also* Barton Gellman, Julie Tate & Ashkan Soltani, *In NSA-Intercepted Data, Those not Targeted far Outnumber the Foreigners Who Are*, WASH. POST (July 5, 2014), *at* https://www.washingtonpost.com/world/national-security/in-nsa-intercepted-data-those-not-targeted-far-outnumber-the-foreigners-who-are/2014/07/05/8139adf8-045a-11e4-8572-4b1b969b6322_story.html; Barton Gellman & Laura Poitras, *U.S., British Intelligence Mining Data from Nine U.S. Internet Companies in Broad Secret Program*, WASH. POST (June 7, 2013), *at* https://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html. *See also* Kristina Daugirdas & Julian Davis Mortenson, Contemporary Practice of the United States, 108 AJIL 783, 816 (2014).

[23] Schrems, *supra* note 6, para. 28.

[24] *Id.*, para. 29.

[25] *Id.*, para. 30.

[26] *Id.*, para. 36.

framework was invalid.[27] The CJEU stated that the phrase "adequate level of protection" found in the 1995 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 [the 1995 Directive] read in light of the Charter [on Fundamental Rights]."[28] The CJEU also emphasized that, in examining the level of protection afforded by a third country, the 1995 Directive required it to "take account of all the circumstances surrounding a transfer of personal data to a third country."[29]

The CJEU focused in particular on a provision in the Safe Harbor Principles that stated: "Adherence to these Principles may be limited: (a) to the extent necessary to meet national security, public interest, or law enforcement requirements; [or] (b) by statute, government regulation, or case-law that create conflicting obligations or explicit authorisations."[30] In the view of the CJEU, this provision significantly limited the protections provided by the Safe Harbor Principles by giving primacy to "national security, public interest, or law enforcement requirements" over those principles.[31] By approving the Safe Harbor Principles even though they included this provision, the Commission's 2000 Decision "enable[d] interference . . . with the fundamental rights of the persons whose personal data is or could be transferred from the European Union to the United States."[32]

Such interference with fundamental rights required safeguards, according to the CJEU, and the Commission failed to establish that the United States had put such safeguards in place:

> 90. [T]he Commission found 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. Also, the Commission noted that the data subjects had no administrative or judicial means of redress enabling, in particular, the data relating to them to be accessed and, as the case may be, rectified or erased.
>
> 91. . . . EU legislation involving interference with . . . fundamental rights . . . must . . . lay down clear and precise rules governing the scope and application of a measure and imposing minimum safeguards, so that the persons whose personal data is concerned have sufficient guarantees enabling their data to be effectively protected against the risk of abuse and against any unlawful access and use of that data. . . .

[27] *Id.*, paras. 98, 104–05. *See also* European Commission, Communication from the Commission to the European Parliament and Council on the Transfer of Personal Data from the EU to the United State 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 (Nov. 6, 2015).

[28] Schrems, *supra* note 6, para. 73.

[29] *Id.*, para. 75. *See also* Case C-362/14, Maximillian Schrems v. Data Protection Comm'r, Opinion of Advocate General Bot, para. 82 (Sept. 23, 2015), *at* http://curia.europa.eu/juris/document/document.jsf?docid=168421&doclang=EN ("It is undisputed, as set out in Article 25(2) of Directive 95/46, that the adequacy of the level of protection afforded by a third country is to be assessed in the light of a range of circumstances, both factual and legal. If one of those circumstances changes and appears to be such as to call into question the adequacy of the level of protection afforded by a third country, the national supervisory authority to which a complaint has been submitted must be able to draw the appropriate conclusions in relation to the contested transfer.").

[30] Schrems, *supra* note 6, para. 8.

[31] *Id.*, para. 86.

[32] *Id.*, para. 87.

> 92. Furthermore and above all, protection of the fundamental right to respect for private life at EU level requires derogations and limitations in relation to the protection of personal data to apply only in so far as is strictly necessary. . . .
>
> 94. In particular, 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. . . .
>
> 95. Likewise, 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. . . .
>
> 96. . . . [I]n order for the Commission to adopt a decision [that a third country ensures an adequate level of protection], it must find, duly stating reasons, that the third country concerned in fact ensures, by reason of its domestic law or its international commitments, a level of protection of fundamental rights essentially equivalent to that guaranteed in the EU legal order. . . .[33]

Without such findings, the Commission could not conclude that the United States provided adequate protection, and the CJEU held the Commission's 2000 decision invalid.[34] The CJEU directed the Irish Data Protection Commissioner to investigate Schrems's complaint and decide independently whether the transfer of data from Facebook's Irish subsidiary to the U.S. should be suspended on the "ground that the country does not afford an adequate level of protection of personal data."[35]

Industry groups, data protection advocates, and commentators reacted strongly to the CJEU's language about fundamental rights—especially the CJEU's assertion 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."[36] Commentators emphasized that the ruling's consequences extended beyond the Safe Harbor agreement—and implicated data gathering and mass surveillance programs more broadly.[37]

The United States and European Union had already been working on a new framework for regulating data flow before this decision; the Court's ruling added an element of urgency to the negotiations.[38] According to media reports, negotiations stalled until U.S. Secretary of State John Kerry was able to guarantee an independent ombudsperson in the Department of State

[33] *Id*., paras. 90–96.

[34] *Id*., para. 98.

[35] CJEU Press Release, The Court of Justice Declares that the Commission's U.S. Safe Harbour Decision is Invalid (Oct. 6, 2015), *at* http://curia.europa.eu/jcms/upload/docs/application/pdf/2015-10/cp150117en.pdf.

[36] Schrems, *supra* note 6, para. 94.

[37] Christopher Kuner, *Reality and Illusion in EU Data Transfer Regulation Post Schrems*, UNIVERSITY OF CAMBRIDGE LEGAL STUDIES RESEARCH 14/2016, March 2016, at 29; Martin Scheinin, *Mass Surveillance and the Right to Privacy: Adding Nuance to the Schrems Case*, JUST SECURITY (Oct. 13, 2015), *at* https://www.justsecurity.org/26781/adding-nuance-context-max-schrems-case-safe-harbor; Mark Scott, *Data Transfer Pact Between U.S. and Europe is Ruled Invalid*, N.Y. TIMES, Oct. 6, 2015, at B1.

[38] Scott, *supra* note 20. Article 29 Working Party Statement, *supra* note 7 (noting that unless an agreement is reached by the end of January 2016, "EU data protection authorities are committed to take all necessary and appropriate actions, which may include coordinated enforcement actions").

to oversee the complaints regarding American security agencies' access to Europeans' data.[39] On February 2, 2016, the United States and European Union announced a new political agreement to create the Privacy Shield as a replacement for the Safe Harbor framework.[40] The Privacy Shield retains some key features of the Safe Harbor framework. Participation remains voluntary and participating companies continue to self-certify compliance with the Privacy Shield Framework's requirements.[41] Moreover, the Privacy Shield Framework Principles provide that "[a]dherence to these Principles may be limited: (a) to the extent necessary to meet national security, public interest, or law enforcement requirements," and "(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."[42]

In a press release, European officials have highlighted four aspects of the deal:

- *Strong obligations on companies and robust enforcement*: the new arrangement will be transparent and contain effective supervision mechanisms to ensure that companies respect their obligations, including sanctions or exclusion if they do not comply. The new rules also include tightened conditions for onward transfers to other partners by the companies participating in the scheme.
- *Clear safeguards and transparency obligations on U.S. government access*: for the first time, the U.S. government has given the EU written assurance from the Office of the Director of National Intelligence that any access of public authorities for national security purposes will be subject to clear limitations, safeguards and oversight mechanisms, preventing generalised access to personal data. U.S. Secretary of State John Kerry committed to establishing a redress possibility in the area of national intelligence for Europeans through an Ombudsperson mechanism within the Department of State, who will be independent from national security services. The Ombudsperson will follow-up complaints and enquiries by individuals and inform them whether the relevant laws have been complied with. These written commitments will be published in the U.S. federal register.
- *Effective protection of EU citizens' rights with several redress possibilities*: Complaints have to be resolved by companies within 45 days. A free of charge Alternative Dispute Resolution solution will be available. EU citizens can also go to their national Data Protection Authorities, who will work with the Federal Trade Commission to ensure that unresolved complaints by EU citizens are investigated and resolved. If a case is not resolved by any of the other means, as a last resort there will be an arbitration mechanism ensuring an enforceable remedy. Moreover, companies can commit to comply with advice from European [Data Protection Authorities]. This is obligatory for companies handling human resource data.
- *Annual joint review mechanism*: the mechanism will monitor the functioning of the Privacy Shield, including the commitments and assurance as regards access to data for law enforcement and national security purposes. The European Commission and the

[39] Sheftalovich, *supra* note 7.
[40] *See supra* note 1.
[41] Dep't of Commerce Fact Sheet, *supra* note 1.
[42] Privacy Shield, *supra* note 1, at 19.

> U.S. Department of Commerce will conduct the review and associate national intelligence experts from the U.S. and European Data Protection Authorities. The Commission will draw on all other sources of information available, including transparency reports by companies on the extent of government access requests. The Commission will also hold an annual privacy summit with interested NGOs and stakeholders to discuss broader developments in the area of U.S. privacy law and their impact on Europeans. On the basis of the annual review, the Commission will issue a public report to the European Parliament and the Council.[43]

On the U.S. side, the Department of Commerce explained that it was issuing the Privacy Shield Principles "under its statutory authority to foster, promote, and develop international commerce."[44] Pursuant to those principles, participating companies may make a commitment to comply with them and self-certify their adherence to the Commerce Department; such commitments then become enforceable under U.S. law.[45] (In addition, the company must re-certify annually.[46]) Participating companies must inform individuals of their rights to access their personal data.[47] Such companies must also offer individuals "the opportunity to choose . . . 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."[48] When a participating company transfers information to a third party, that company must enter into a contract providing that such data may only be processed for limited purposes consistent with the consent of the individual and that the data will continue to be protected according to the Privacy Shield's standards.[49]

Turning to enforcement, the Department of Commerce will monitor whether companies publish their privacy commitments and will conduct periodic compliance reviews.[50] The Department of Commerce has also committed to creating a point of contact for the European Data Protection Authorities (DPAs); this contact will assist the DPAs in uncovering information related to particular companies.[51] The Federal Trade Commission will, in turn, enforce companies' commitments.[52] U.S. companies may also choose to resolve any complaints

[43] European Commission Press Release, Restoring Trust in Transatlantic Data Flows through Strong Safeguards: European Commission Presents EU-U.S. Privacy Shield (Feb. 29, 2016), *at* http://europa.eu/rapid/press-release_IP-16-433_en.htm. *See also Fact Sheet, EU-U.S. Privacy Shield*, EUROPEAN COMMISSION (Feb. 2016), *at* http://ec.europa.eu/justice/data-protection/files/factsheets/factsheet_eu-us_privacy_shield_en.pdf.

[44] Privacy Shield, *supra* note 1, at 18 (EU-U.S. Privacy Shield Principles) (citing 15 U.S.C. § 1512, which provides: "It shall be the province and duty of said Department to foster, promote, and develop the foreign and domestic commerce, the mining, manufacturing, and fishery industries of the United States; and to this end it shall be vested with jurisdiction and control of the departments, bureaus, offices, and branches of the public service hereinafter specified, and with such other powers and duties as may be prescribed by law").

[45] Privacy Shield, *supra* note 1, at 18 (EU-U.S. Privacy Shield Principles); *id.* at 4 (Letter from Under Secretary for Trade Stefan Stelig to EU Commissioner Vera Jourova).

[46] *Id.* at 19 (EU-U.S. Privacy Shield Principles).

[47] *Id.* at 21 (including "the type or identity of third parties to which it discloses personal information"). *See also Id.* at 5 (Letter from Under Secretary for Trade Stefan Stelig to EU Commissioner Vera Jourova).

[48] *Id.* at 22 (EU-U.S. Privacy Shield Principles).

[49] *Id.* at 20.

[50] *Id.* at 6–9 (Letter from Under Secretary for Trade Stefan Stelig to EU Commissioner Vera Jourova).

[51] *Id.* at 9.

[52] *Id.* at 68–73 (Letter from FTC Chairwoman Edith Ramirez to EU Commissioner Vera Jourova (Feb. 23, 2016)). The FTC has cited its authority under the Federal Trade Commission Act "to protect consumers worldwide

through the DPAs.[53] As under the Safe Harbor agreement, DPAs may refer any complaints they receive to the FTC for enforcement assistance.[54] Finally, the FTC, Department of Commerce, Department of State, and EU DPAs together will review the agreement annually.[55]

European individuals will have several routes available to challenge the transfer of their personal data to U.S. servers in violation of the Privacy Shield. Among these, EU citizens can complain directly to U.S. companies that they believe are violating the Privacy Shield.[56] U.S. companies participating in the Privacy Shield must also provide an independent recourse mechanism to EU citizens at no cost;[57] possible sanctions "include both publicity for findings of non-compliance and the requirement to delete data in certain circumstances."[58] If such mechanisms do not work, companies have committed to participating in binding arbitration;[59] the EU and U.S. have designed such arbitration as a last resort.[60] The arbitration panel "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."[61]

In regard to the U.S. surveillance program, the General Counsel for the Director of National Intelligence provided written assurances of the constitutional, statutory, and policy limitations that apply to its operations.[62] Similarly, the Department of Justice provided a written overview of the limitations on the U.S. government's ability to access commercial data.[63]

Finally, the U.S. government has established the Privacy Shield Ombudsperson at the U.S. Department of State to investigate and respond to European citizens' complaints about surveillance and access to personal data by U.S. national security agencies.[64] Kerry has appointed Under Secretary of State Catherine Novelli—who currently serves as a point

from practices taking place in the United States" as the basis for its authority to undertake enforcement actions outlined in the Privacy Shield. Privacy Shield, *supra* note 1, at 75–76 (The EU-U.S. Privacy Shield Framework in Context). *See also* 15 U.S.C. § 45(a)(4); Federal Trade Commission Press Release, Statement of FTC Chairwoman Edith Ramirez on EU-U.S. Privacy Shield Framework (Feb. 29, 2016), *at* https://www.ftc.gov/news-events/press-releases/2016/02/statement-ftc-chairwoman-edith-ramirez-eu-us-privacy-shield-0.

[53] Privacy Shield, *supra* note 1, at 28 (EU-U.S. Privacy Shield Principles).

[54] *Id.* at 72–73 (Letter from FTC Chairwoman Edith Ramirez to EU Commissioner Vera Jourova). *See also* EC Feb. 2 Press Release, *supra* note 1.

[55] Privacy Shield, *supra* note 1, at 71 (Letter from FTC Chairwoman Edith Ramirez to EU Commissioner Vera Jourova). *See also* Dep't of Commerce Fact Sheet, *supra* note 1.

[56] Privacy Shield, *supra* note 1, at 39 (EU-U.S. Privacy Shield Principles).

[57] *Id.* at 24.

[58] *Id.* at 41.

[59] *Id.* at 40. *See also id.* (Annex I: Arbitral Model).

[60] *Id.* at 49 (Annex I: Arbitral Model).

[61] *Id.*

[62] *Id.* at 105 (Letter from Director of National Intelligence General Counsel Robert Litt to U.S. Dep't of Commerce Counselor Justin Antonipillai and Int'l Trade Adm'n Deputy Assistant Sec'y Ted Dean).

[63] *Id.* at 124–28 (Letter from Deputy Assistant Attorney General Bruce Swartz to U.S. Dep't of Commerce Counselor Justin Antonipillai and Int'l Trade Adm'n Deputy Assistant Sec'y Ted Dean).

[64] *Id.* at 57 (EU-U.S. Privacy Shield Framework Mechanism Regarding Signals Intelligence). *See also* Department of Commerce Fact Sheet, *supra* note 1; EC Feb. 2 Press Release, *supra* note 1. The Department of State has cited Section 4(d) of Presidential Policy Directive 28—directing the Secretary of State to designate a senior official to "serve as point of contact for foreign governments who wish to raise concerns regarding signals intelligence activities conducted by the United States"—as the basis for the creation of the Ombudsperson. Privacy Shield, *supra* note 1, at 55 (EU-US Privacy Shield Framework Mechanism Regarding Signals Intelligence).

of contact for foreign governments with concerns about U.S. signal intelligence activities—as the Ombudsperson.[65]

Officials and commentators are divided as to whether the EU-U.S. Privacy Shield will survive the scrutiny of the CJEU in light of the *Schrems* ruling. U.S. Commerce Secretary Penny Pritzker stated, "We are confident that we have met the requirements of the [CJEU] ruling," further noting that the agreement "will allow the digital economy in the European Union and United States to grow, which is so critical to jobs and economic security."[66] Perhaps unsurprisingly, Schrems himself disagrees: "A couple of letters by the outgoing Obama administration is by no means a legal basis to guarantee the fundamental rights of 500 million European users in the long run."[67] According to press reports, several consumer groups have indicated they plan to file complaints with European data protection authorities to challenge the new agreement.[68]

INTERNATIONAL ORGANIZATIONS

After Lengthy Delay, Congress Approves IMF Governance Reforms that Empower Emerging Market and Developing Countries

In 2010, the United States pressed for a package of governance reforms to the International Monetary Fund (IMF) that would change the IMF's quota system and executive board composition.[1] Five years later, in December 2015, the U.S. Congress finally approved those reforms. Although the IMF and other states welcomed this development, they also expressed disappointment and frustration about the long delay.[2]

The IMF Executive Board approved the proposed reforms in December 2010. Dominique Strauss-Kahn, then the IMF's managing director, explained that the reforms would effect "the most fundamental governance overhaul in the Fund's 65-year history and the biggest ever shift of influence in favor of emerging market and developing countries to recognize their growing

[65] *Id.* at 54 (Letter from Sec'y of State John Kerry to EU Commissioner Vera Jourova (Feb. 22, 2016)).

[66] Ellen Nakashima & Andrea Peterson, *European and US Negotiators Agree on New "Safe Harbor" Data Deal*, WASH. POST (Feb. 2, 2016), *at* https://www.washingtonpost.com/world/national-security/european-and-us-negotiators-agree-on-new-safe-harbor-data-deal/2016/02/02/f576e706-c9e5-11e5-a7b2-5a2f824b02c9_story.html. *See also* Department of Commerce Press Release, Statement from U.S. Sec'y of Commerce Penny Pritzker on EU-U.S. Privacy Shield (Feb. 2, 2016), *at* https://www.commerce.gov/news/press-releases/2016/02/statement-us-secretary-commerce-penny-pritzker-eu-us-privacy-shield.

[67] Nakashima & Peterson, *supra* note 66. Scott, *supra* note 19.

[68] Scott, *supra* note 19.

[1] Int'l Monetary Fund Board of Governors Res. 66-2, Fourteenth General Review of Quotas and Reform of the Executive Board (Dec. 15, 2010), *in* IMF, SELECTED DECISIONS AND SELECTED DOCUMENTS OF THE INTERNATIONAL MONETARY FUND 14–18 (2014), *at* http://www.imf.org/external/pubs/ft/sd/2013/123113.pdf [hereinafter IMF Selected Decisions and Documents] (proposing amendments to Articles XII, XXI, and XXIX, and to Schedules A, D, E, and L of the IMF's Articles of Agreements); *G-20: Fact Sheet on IMF Reform*, THE WHITE HOUSE (Nov. 12, 2010), *at* https://www.whitehouse.gov/the-press-office/2010/11/12/g-20-fact-sheet-imf-reform; Sewell Chan, *Debt Crisis Highlights I.M.F.'s Renewed Role*, N.Y. TIMES, Nov. 26, 2010, at B3 ("Under pressure from the United States, Europe has ceded two seats on the fund's board. . . ."); *see also* Edwin M. Truman, *IMF Reform is Waiting on the United States*, PETERSON INST. INT'L ECON., Mar. 2014, at 1, *available at* https://www.piie.com/publications/pb/pb14-9.pdf (identifying the Obama administration as the "principal architect" of the reform package).

[2] *See* Jackie Calmes, *I.M.F. Breakthrough Is Seen to Bolster U.S. on World Stage*, N.Y. TIMES, Jan. 6, 2016, at B1.