Privacy Shield backgrounder

When the Court of Justice of the European Union ("CJEU") struck down the EU-U.S. Safe Harbor Framework on October 6, 2015, it threatened to halt all transfers of personal data out of Europe, with significant implications on global trade. After months of negotiation, the EU and the U.S. announced the Privacy Shield, a replacement for Safe Harbor, to secure international data transfers. The following is an excerpt from Gabe Maldoff and Omer Tene’s article, forthcoming in the Wisconsin International Law Journal, outlining how we got to this point and what it all means for the law of international data transfers.

I. Background

A. The Data Protection Directive and International Data Transfers

On July 25, 1995, the European Union ("EU") formally enacted Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data, known as the Data Protection Directive.\(^1\) Coming into effect in 1998, the Data Protection Directive required each EU Member State to impose restrictions on the processing of personal data to “protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy.”\(^2\)

The Data Protection Directive aimed to reconcile the conflicting standards of data protection that had emerged in a number of EU Member States. Before the Data Protection Directive, EU data protection law was composed of a series of Member State statutes that were passed in the 1970s, beginning with a Länder-level law in Germany.\(^3\) Some of these statutes explicitly prohibited the transfer of personal data to other countries—including other European Countries—that did not provide “equivalent

---

2 Id. at art. 1.
protection." Other statutes banned international data transfers altogether in the absence of further legislation permitting such transfers.5

By the late 1970s, the need for a harmonized approach had become evident. The Organisation for Economic Co-operation and Development (OECD) recognized that “differing national legal regulations, superimposed on interconnecting communications technology, would produce serious inefficiencies and economic costs.”6 To address the potential for economic disruption, the OECD released a set of Guidelines on the protection of personal data that encouraged member countries to “refrain from restricting transborder flows of personal data . . . except where the latter does not yet substantially observe [the OECD] Guidelines.”7 One year later, the Council of Europe’s Data Protection Convention sought to promote “free flows of data”8 among countries

4 Law for the Protection of Personal Data with Regard to Automatic Processing, Law 10/91 (Apr. 29, 1991) (“uma protección equivalente”), at § 33 (Portugal); Law on the Regulation of the Automatic Processing of Personal Data (Oct. 29, 1992), at § 32 (“un nivel de protección equiparable”) (Spain).
6 Michael Kirby, Remarks on the 30th Anniversary of the OECD Privacy Guidelines, Thirty Years After: The OECD Privacy Guidelines 8 (2011), available at http://www.oecd.org/sti/ieconomy/49710223.pdf. When the OECD revised its guidelines in 2013, harmonizing international data transfers remained a significant focus of the initiative. See Org. for Econ. Co-operation & Dev. [OECD], Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (2013), available at http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderrflowsofpersonaldataln.htm, (warning that “there is a danger that disparities in national legislations could hamper the free flow of personal data across frontiers,” especially given that “these flows have greatly increased in recent years and are bound to grow further with the widespread introduction of new computer and communications technology”).
that were signatories to the treaty, while still allowing signatory countries to block transfers to non-signatory countries that did not provide “equivalent protection.”

The 1995 Data Protection Directive harmonized the disparate legislative frameworks in the EU by requiring each EU Member State to implement specific principles for data processing. The Data Protection Directive applied to private and public entities alike, imposing strict requirements on all organizations that process personal data, with an exemption when “a restriction constitutes a necessary measure to safeguard,” inter alia, national security, defence, and public security. It created “supervisory authorities” in each State (often referred to as “Data Protection Authorities” or “DPAs”), empowered to “act with complete independence” in overseeing personal data processing operations, and it mandated the free flow of data within the EU.

These robust protections would have been meaningless, however, if they could be easily circumvented by transferring data outside the EU. Given that data moves readily around the globe with negligible cost and at the speed of light, the EU needed to put in place virtual border controls to maintain the integrity of its framework. To resolve this, the Data Protection Directive introduced the concept of “adequacy.”

Article 25 of the Data Protection Directive forbade the transfer of personal data to a third country outside the EU, unless that country offers “an adequate level of protection.” Each Member State supervisory authority was empowered to determine the adequacy of a third country’s protections “in the light of all the circumstances surrounding the data transfer operation or set of data transfer operations.” The Data Protection Directive also created a mechanism by which the European Commission could find that a third country offered adequate protections “by reason of its domestic law or of the international commitments it has entered into.” Such a finding would permit the transfer of data from any EU Member State to that third country.

---

9 Id. at art. 12.
10 Id. at art. 12(3)(a).
11 Schwartz, supra note 5, at 480.
12 Data Protection Directive, supra note 1, art. 13(1).
13 Id. at art. 28(1).
14 Schwartz, supra note 5, at 473.
15 Data Protection Directive, supra note 1, art. 25(1).
16 Id. at art. 25(2). Assessment of a third country’s adequacy should include “the nature of the data, the purpose and duration of the proposed processing operation or operations, the country of origin and country of final destination, the rules 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.
17 Id. at art. 25(6).
18 Id.
The Data Protection Directive also established several other mechanisms, including standard contractual clauses and unambiguous consent, to facilitate cross-border data transfers. These mechanisms allowed organizations to transfer personal data to third countries, even if those countries had not been found adequate. Unlike adequacy findings, however, these mechanisms were cumbersome for organizations that transfer personal data. For example, to use a standard contractual clause, an organization was required to implement detailed contractual language, approved by Member State regulators, in its relationship with any other entity handling the data. These contractual relationships extended European-style data protection requirements to all the entities involved in data processing. For a large conglomerate, this meant hundreds or even thousands of contracts had to be put in place and revised regularly. An additional mechanism, called Binding Corporate Rules (BCRs), grew out of the need for a more streamlined, efficient process. BCRs allowed an organization to submit its practices for detailed auditing by regulators, in a process that could take several years but saved the organization the need to implement, monitor and revise innumerable contractual arrangements.

Because of the ease of transferring data to an “adequate” jurisdiction, adequacy remained the Holy Grail. Alas, only a handful of countries were successful in obtaining the seal of adequacy. Among the world’s developed economies, only Canada, Israel, New Zealand, and Switzerland secured adequate status, as well as the U.S. under a more limited framework outlined below. Important partners such as Japan and Australia were excluded, as were massive trading blocks such as China and India.

As the growth of information services in the 2000s raised the prospect of greater economic integration, the EU placed increased emphasis on legal privacy protections, especially for online activities. With the entry into force of the Lisbon Treaty in 2009, the Charter of Fundamental Rights of the European Union (“EU Charter”) became legally binding. The EU Charter enshrined, in Article 7, the right to respect for a person’s

---

19 Id. at art. 26.
“private and family life, home and communications.”23 Article 8’s right to “protection of personal data” provided individuals with the right to have their personal data “processed fairly and on the basis of the consent of the person concerned or some other legitimate basis laid down by law.”24

Relying on the EU Charter, the Court of Justice of the European Union (CJEU) became an important arbiter of privacy rights, handing down major privacy decisions.25 In one 2014 decision, Digital Rights Ireland and Others, a case that would become central to defining “adequacy,” the Court invalidated the EU Data Retention Directive, which had required telecommunications service providers to retain subscriber and location data so as to be accessible to public authorities investigating “serious crimes.”26 Relying on Articles 7 and 8 of the EU Charter, the Court held that the retention of the data, and access to it by national authorities, “constitutes a particularly serious interference with those [EU Charter] rights.”27 Thus, after Digital Rights Ireland, it became clear that the EU Charter compelled a strict reading of the national security, defence, and public security exemptions to the Data Protection Directive.28

B. EU-U.S. Safe Harbor

Rather than adopting omnibus privacy legislation, like the Data Protection Directive or PIPEDA, the U.S. opted for a different approach, creating a quilt of sector-specific federal legislation enmeshed with state laws. In the U.S., there are federal statutes governing health privacy,29 financial privacy,30 education privacy,31 and children’s online privacy,32 for example, as well as state-level privacy initiatives, most notably security

23 Id. at art. 7.
24 Id. at art. 8(2).
25 See Google Spain SL v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González, C-131/12 (May 13, 2014) (establishing a “right to be forgotten” that required search engines to remove embarrassing links to a person’s name upon that person’s request).
26 Digital Rights Ireland and Others, C-293/12 and C-594 (Apr. 8, 2014), available at http://curia.europa.eu/juris/document/document.jsf;jsessionid=9ea7d0f130d55a61733fca5a4dc93b7a9ae50b99d00.e34KaxiLc3eQc40LaxqMbN4pa3aSe0?text=&docid=150642&pagemIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=340236.
27 Id. at para. 39.
28 Id. at para. 48.
breach notification laws, and a federal statute that governs the public sector. However, no federal statute regulates data privacy for private entities that fall outside of these sectors.

The U.S. does not limit transfers of data to other countries. Cynics may argue that this is because the U.S. is notorious for exercising long-arm jurisdiction. In the privacy context, for example, any website directed at U.S. children under the age of 13, regardless of its location, could be subject to enforcement under the Children’s Online Privacy Protection Act (COPPA). And this phenomenon is not limited to privacy laws. The Foreign Account Tax Compliance Act, for example, requires foreign financial institutions to report asset and identity information of any U.S. persons using their services. In another example, U.S. authorities have used the Unlawful Internet Gambling Enforcement Act to target foreign-operated online gambling sites, including PokerStars, which was founded by a Canadian.

Similarly, the U.S. has no designated privacy regulator, akin to a European Data Protection Authority. The Federal Trade Commission (“FTC”), state Attorneys General and several other federal regulators that have limited privacy mandates, including the U.S. Department of Health and Human Services Office for Civil Rights, the Consumer Financial Protection Bureau, and the Securities and Exchange Commission have stepped in to fill this void.

---

The FTC has been the regulator most active in enforccing privacy protections. Under Section 5 of the Federal Trade Commission Act, the FTC has the authority to proscribe “unfair or deceptive acts or practices in or affecting commerce.” Section 5 allows the FTC to enforce any material promise made by a company subject to the FTC’s jurisdiction. Since the late 1990s, the FTC has used this authority to pursue more than 200 cases of alleged violations of consumer privacy. In addition to enforcing several sectoral statutes, the FTC has encouraged companies to provide notice of their data processing activities and has held those companies to the terms of their notice. Increasingly, the FTC has used its “unfairness” authority to proscribe data handling practices that fall short of consumer expectations. State Attorneys General have secured similar, and in some cases stronger, privacy protections under State-level statutes regulating “unfair or deceptive acts or practices.”

Because the U.S. did not enact omnibus privacy legislation and had no dedicated DPA, it likely would not have met the threshold for adequacy. As a result, U.S. officials never applied for an adequacy determination based on the U.S. framework. But, as the U.S. remained the EU’s largest trading partner, transfers to the U.S. simply could not be ignored. In 1998, the European Commission and the U.S. Department of Commerce began negotiations on an alternative framework for transatlantic data flows. After two years of negotiations, the European Commission released the final text of the EU-U.S.

---

46 Citron, supra note 33.
Safe Harbor Arrangement ("Safe Harbor") on July 25, 2000.49 The resulting framework created an “adequate” mechanism by which participating U.S. companies could transfer personal data from the EU.50

Safe Harbor operated as a voluntary self-certification program.51 Under Safe Harbor, U.S. companies promised to adhere to the Safe Harbor Principles, which included protections similar to those of the Data Protection Directive, particularly around notice, choice, access, security, data integrity, and onward transfers to third parties.52 U.S. companies that wished to participate were required to certify their compliance to the Principles to the Department of Commerce and to publicize their adherence to Safe Harbor in their privacy notices.53

By requiring companies to publicize their commitment to Safe Harbor, the commitment became binding and enforceable by the FTC under its Section 5 authority against deceptive trade practices.54 To be sure, the FTC did not become authorized to enforce European data protection legislation, but a company that failed to live up to its promises committed a Section 5 violation. From 2000 to 2015, the FTC brought cases against Google, Facebook, MySpace, and TES Franchising for violations of the Safe Harbor Principles as well as thirty-six cases against companies that failed to renew their self-certification or that claimed Safe Harbor certification but never filed with the Department of Commerce.55

Neither the Safe Harbor Principles nor the European Commission’s adequacy decision placed limits on national security access. In fact, the Principles stated that an organization’s adherence to the framework “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 authorizations, provided that, in exercising any such authorization, an organization can

50 Id.
52 Chuan Sun, supra note 48, at 107-08.
53 Ioanna Tourkochoriti, supra note 51, at 470.
54 Id.
demonstrate that its non-compliance with the Principles is limited to the extent necessary to meet the overriding legitimate interests furthered by such authorization.”

Hence, Safe Harbor included a broad exemption for national security access.

By 2015, more than four thousand U.S. companies of all sizes relied on Safe Harbor to transfer data.

II. The Fall of Safe Harbor

Safe Harbor was a carefully-negotiated compromise, striking a balance between divergent concepts of privacy protection. Even after its approval by the European Commission, EU officials as well as the FTC and advocates in the U.S. continued to call on the U.S. to enact federal privacy legislation to govern the commercial use of personal data. But until its demise in 2015, Safe Harbor remained the most important mechanism for transferring personal data to the U.S.

A. Edward Snowden and the Max Schrems Story

i. Revelations of Secret Surveillance

On June 5, 2013, The Guardian reported that “[t]he National Security Agency [“NSA”] is currently collecting the telephone records of millions of US customers of Verizon, one of America’s largest telecoms providers, under a top secret court order . . . .” Over the

56 Safe Harbor Decision, supra note 49.
58 See Ioanna Tourkochoriti, supra note 51, at 468 (“The differences [between the U.S. and EU approaches to privacy] concern first, the fundamental presumptions concerning the processing of personal data. The presumption in the U.S. is that the processing of personal data is permitted unless it causes harm or is limited by law. The opposite presumption is dominant in the EU where processing is prohibited unless there is a legal basis that allows it.”).
days that followed, a series of reports in The Guardian and The Washington Post detailed aspects of the U.S. surveillance architecture. The reports revealed NSA surveillance programs directed at U.S. and foreign communications alike. They also revealed cooperation between the NSA and several foreign intelligence agencies. Within a few days of the first report, Edward Snowden, a 29-year-old NSA contractor, came forward as the source for the leaked information.

Snowden’s leaked documents alleged the existence of two NSA programs directed at foreign communications. The first, reported on June 6, was a top-secret NSA program called “PRISM” that, according to a leaked document, provided the NSA “direct access from the servers of these US service providers: Microsoft, Yahoo, Google, Facebook, Paltalk, AOL, Skype, YouTube, Apple.” The program allegedly permitted the NSA to access “records such as emails, chat conversations, voice calls, documents and more.” The extent of the PRISM program and the NSA’s ability to directly access the contents of the servers of these companies remains a subject of debate. Subsequent reports have clarified that, under the PRISM program, the NSA, by way of the FBI, sent specific selectors (such as an email or Internet Protocol (IP) address) to U.S.-based electronic communications service providers. The service provider would then be required to turn over any communications involving the selector to the NSA. Notably, all of the

---

63 Id.
64 Id.
67 Id.
70 Id.
allegedly participating companies were certified to transfer EU data to the U.S. under Safe Harbor.\footnote{71}{Ioanna Tourkochoriti, supra note 51; European Court of Justice May Invalidate Safe Harbor Framework, BALLARD SPAHR LLP (Sept. 30, 2015), available at http://www.ballardspahr.com/alertspublications/legalalerts/2015-09-30-european-court-of-justice-may-invalidate-safe-harbor-framework.aspx.}

On June 8, a leak described another program, which used a technique known as upstream collection. This program allegedly enabled the NSA to collect “communications on fiber cables and infrastructure as data flows past”\footnote{72}{James Ball, NSA Prism surveillance program: how it works and what it can do, GUARDIAN (Jun. 8, 2013), http://www.theguardian.com/world/2013/jun/08/nsa-prism-server-collection-facebook-google.} with devices connected to high capacity cables, switches and routers that form the backbone of the internet’s infrastructure. Using upstream collection, the NSA allegedly copied, stored and analyzed email and other communications that flowed across the internet.\footnote{73}{PCLOB Report, supra note 69, at 36.}

Critically, these NSA programs allegedly were authorized by law. To strengthen its counterterrorism efforts after the attacks of September 11, the U.S. had passed the USA PATRIOT ACT\footnote{74}{115 Stat. 272 (2001).} in 2001 and the FISA Amendments Act of 2008 (“FAA”).\footnote{75}{122 Stat. 2436 (2008).} The FAA created Section 702 of the Foreign Intelligence Surveillance Act (“FISA”), which established a framework for the bulk interception of foreign communications.\footnote{76}{Id.}

The revealed practices of the NSA were met with widespread condemnation in the EU and depicted by critics as overreach by U.S. security services.\footnote{77}{Hannah Allam and Jonathan S. Landay, World’s Anger at Obama Policies Goes Beyond Europe and the NSA, McCLATCHY DC (Oct. 25, 2013), http://www.mcclatchydc.com/news/nation-world/world/article24757900.html; Jedidiah Bracy, Reactions to NSA Disclosures Continue, IAPP PRIVACY ADVISOR (Jun. 10, 2013), https://iapp.org/news/a/Reactions-to-NSA-Disclosures-Continue.} To be sure, the EU had recognized the right of third countries to engage in national security surveillance, and had allowed exemptions from data protection legislation for such practices both in Europe and in the approved adequacy decisions, including the Safe Harbor framework. But, at the time, few if any policymakers imagined the enormity of the data collection apparatus revealed by the Snowden leaks. In March 2014, after a six-month review of the U.S. national security framework, the European Parliament passed a resolution calling for the “immediate suspension” of transfers to the U.S. under Safe Harbor.\footnote{78}{US NSA: stop mass surveillance now or face consequences, MEPs say, European Parliament News (Mar. 12, 2014), available at...
Max Schrems Takes On Facebook

In the spring of 2011, Max Schrems was an Austrian law student on exchange at Santa Clara University School of Law.\(^79\) In a privacy law seminar, the professor invited a lawyer from Facebook to speak to the class. Schrems was “taken aback” when the lawyer explained that “they didn’t take Europe’s strict privacy laws very seriously, since companies rarely faced significant penalties for breaking them.”\(^80\) Schrems decided to write a term paper on the subject, and, upon return to Austria, he formed a non-profit to challenge Facebook’s privacy policies.\(^81\) His organization filed more than twenty complaints against Facebook with the Irish Data Protection Commissioner (“DPC”), where Facebook’s European operations are based.\(^82\)

Two years later, just days after Snowden’s revelations, Schrems filed another complaint with the DPC, asking it “to inquire if ‘Facebook Inc’ is forwarding my data to the NSA for compelling reasons of national security or if merely cooperating with the NSA voluntarily.”\(^83\) Furthermore, because Facebook used Safe Harbor to transfer data, Schrems challenged whether Safe Harbor’s national security exemption was consistent with the Data Protection Directive and with the EU Charter of Fundamental Rights. Thus, Schrems asked the DPC “to review the validity of the ‘Safe Harbor’ Decision.”\(^84\) Finding that the European Commission’s Safe Harbor Decision precluded independent review of data transfers by national authorities, and that Schrems had presented no evidence that his own data had been accessed, the DPC refused to investigate the complaint.\(^85\)


\(^84\) Id. at 6.

Schrems appealed the DPC’s refusal to take action to the High Court of Ireland.86 Schrems argued that the DPC “unlawfully fettered his own discretion” because “[i]t was irrational to rely upon [the Commission’s Safe Harbor] Decision in circumstances where the Applicant’s complaint is specifically contesting its validity and arises from facts that were unknown or did not exist at the date of EU Commission Decision C2000/520/EC.”87 Therefore, he asked the court to order the DPC to investigate his complaint.88

The High Court first considered the question as a matter of Irish law.89 Since “surveillance directly engages the constitutional right to privacy” as well as “the inviolability of the dwelling,”90 if the question was controlled entirely by Irish law, the court found that “a significant issue would arise as to whether the United States ‘ensures an adequate level of protection for the privacy and the fundamental rights and freedoms.’”91 Recognizing, however, that Irish law was pre-empted by the European Commission’s adequacy finding, pursuant to Article 25 of the Data Protection Directive, the court held that EU law must control.92

As a matter of EU law, the court noted that although the Safe Harbor Decision purported to prevent the DPC from investigating the complaint, two important developments had undermined its continued validity. First, the entry into force of the EU Charter required the European Commission to ensure that all data access, including by government authorities, was consistent with the EU Charter.93 Second, “disclosures regarding mass and undifferentiated surveillance of personal data by the US security authorities, [and] the advent of social media” since the Commission decision in 2000 had undermined previous assumptions about the extent of U.S. national security access.94 Thus, pursuant to EU procedure, the court referred to the CJEU the question of whether given these new legal and factual developments, the DPC was bound by the

87 Id. at (E)(1).
88 Id.
90 Id. at paras. 48-49.
91 Id. at paras. 52, 56.
92 Id. at para. 57.
94 Id.
Commission’s adequacy finding not to conduct its own independent investigation where an individual claims an interference with his EU Charter rights.  

B. Schrems v. Data Protection Commissioner

On September 23, 2015, after the CJEU heard arguments in Maximilian Schrems v. Data Protection Commissioner (“Schrems”), the Advocate General, Yves Bot, delivered his assessment of the case. The Advocate General, a neutral party, found 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.” Two weeks later, the CJEU struck down the Safe Harbor Decision.

The CJEU overturned the adequacy decision on two grounds. First, the Court held that the decision improperly limited the ability of DPAs to independently fulfill their mandates of protecting European citizens’ data. Second, the Court determined that the Commission’s decision failed to limit—or point to existing national law or international obligations that limit—the U.S. government’s ability to conduct indiscriminate surveillance.

i. The Role of Data Protection Authorities

In Schrems, the specific provision at issue was Article 3 of the Safe Harbor Decision. Article 3 allowed a DPA to suspend data flows only when (a) the FTC has found that the U.S. organization transferring data has violated the Principles of Safe Harbor, or (b) “there is a substantial likelihood that the Principles are being violated,” as well as a reasonable basis for believing the FTC is not taking adequate steps, the transfer created an imminent risk of grave harm, and the DPA has made reasonable efforts to provide the organization with notice and an opportunity to respond.

95 Id.
97 Id. at para. 237.
99 Id. at para. 104.
100 Safe Harbor Decision, supra note 49, art. 3.
The CJEU first noted that the “an essential component” of Data Protection Directive’s protections was its requirement for Member States “to set up one or more public authorities responsible for monitoring, with complete independence, compliance with EU rules.”\textsuperscript{101} The Data Protection Directive empowered DPAs with investigative authority, including “the power to collect all information necessary for the performance of their supervisory duties,” as well as the authority to intervene by banning data transfers or engaging in legal proceedings.\textsuperscript{102} This mandate, the Court explained, was further strengthened by Article 8 of the EU Charter, which guaranteed a right to the protection of personal data, under the control of an independent authority.\textsuperscript{103}

Given the central role of DPA oversight to the rights enumerated in the Data Protection Directive and the EU Charter, the Court found that, “even if the Commission has adopted a[n adequacy] decision, . . . [DPAs] must be able to examine, with complete independence, whether the transfer of that data complies with the requirements laid down by the directive.”\textsuperscript{104} Thus, the Court held Article 3 exceeded the Commission’s authority by imposing limits upon the independent operation of DPAs.\textsuperscript{105}

The Court established a process for individuals to challenge adequacy decisions before an appropriate DPA. DPAs must examine, “with all due diligence,” any claim that data has been transferred to a country lacking adequate protections.\textsuperscript{106} A DPA ruling must be appealable to a national court, which may refer the question to the CJEU if it finds that protections were inadequate.\textsuperscript{107} Thus, in the case of Schrem’s complaint, the Irish DPC was not entitled merely to rely on the Safe Harbor Decision to avoid investigating the complaint.

\textit{ii. Limits to Surveillance}

The CJEU next considered the Safe Harbor Decision’s national security exemption.\textsuperscript{108} If the national security exemption was read to contain no restrictions on government access, the Court found, then data transferred to a third country could be subjected to surveillance, “without any differentiation, limitation or exception . . . and without an objective criterion being laid down by which to determine the limits of the access of the public authorities to the data.”\textsuperscript{109} Such “generalized” surveillance, the Court held, “must

\begin{footnotes}
\item[\textsuperscript{101}] Schrems Decision, supra note 98, at para. 40.
\item[\textsuperscript{102}] Id. at para. 43.
\item[\textsuperscript{103}] Id. at para. 47.
\item[\textsuperscript{104}] Id. at para. 57.
\item[\textsuperscript{105}] Id. at para. 66.
\item[\textsuperscript{106}] Schrems Decision, supra note 98, at paras. 62-65.
\item[\textsuperscript{107}] Id.
\item[\textsuperscript{108}] Id. at para. 86.
\item[\textsuperscript{109}] Id. at para. 93.
\end{footnotes}
be regarded as compromising the essence of the fundamental right to respect for private life, as guaranteed by Article 7 of the [EU] Charter.”

The Court, therefore, found that an “adequate level of protection” requires “the third country in fact to ensure, by reason of its domestic law or its international commitments, a level of protection of fundamental rights that is essentially equivalent to that guaranteed within the European Union.” While “the means to which that third country has recourse . . . may differ” from those in the EU, “those means must nevertheless prove, in practice, effective in order to ensure protection essentially equivalent to that guaranteed within the European Union.”

When determining the adequacy of protections in a third country, the Commission must consider “the content of the applicable rules in that country resulting from its domestic law and international commitments and the practice designed to ensure compliance with those rules.” The Commission also must “check periodically whether the finding relating to the adequacy of the level of protection ensured by the third country in question is still factually and legally justified,” taking into account “the circumstances that have arisen after the decision’s adoption.” Thus, review of the third country’s protections “should be strict.”

Importantly, the Court did not consider the substance of U.S. surveillance law. Rather it assessed only the European Commission’s process for determining adequacy, which lacked any substantive review of U.S. surveillance law. Under this review, the Safe Harbor Decision fell because it did not itself consider the equivalency of national security legislation, leaving a loophole, which according to Snowden and Schrems, was in fact used extensively to access European data without due safeguards. Without assessing either the national security protections offered in the U.S. or those offered by EU Member States, the Court made clear that any future adequacy decision would have to account for national security access.

C. Privacy Shield

---

110 Id. at para. 94.
111 Id. at para. 73 (emphasis added).
112 Id. at para. 74 (emphasis added).
113 Schrems Decision, supra note 98, at para. 75.
114 Id. at para. 76.
115 Id. at para 77.
116 Id. at para. 78.
117 Id. at para. 98.
118 Id. at para. 88.
Following the Snowden disclosures, the European Commission issued thirteen recommendations for “restoring trust in EU-U.S. data flows,” which set off a round of negotiations between EU and U.S. officials on strengthening the Safe Harbor framework. On February 2, 2016, almost four months after Schrems invalidated Safe Harbor, the European Commission and the U.S. Department of Commerce announced they had reached an agreement on the “EU-U.S. Privacy Shield,” a rebranded replacement for Safe Harbor. A draft adequacy decision and supporting documentation were released on February 29, 2016, and the Article 29 Working Party issued its assessment on April 13, finding that Privacy Shield did not fully address all the issues in the Schrems decision. After revising the agreement to address these concerns, however, the European Commission officially approved the Privacy Shield package on July 12, 2016. As the latest and most high-profile statement on international data transfers, Privacy Shield may come to define the standard for future adequacy decisions, or at least to inform the negotiation of future adequacy decisions before the European Commission.

Spanning more than 130 pages, including supporting materials provided by high-level U.S. officials, Privacy Shield is clearly different from previous adequacy decisions. It included statements and commitments from the Department of Commerce, Secretary of State, Federal Trade Commission, Secretary of Transportation, Office of the Director of

---

123 See Opinion 01/2016 on the EU – U.S. Privacy Shield draft adequacy decision, supra note Error! Bookmark not defined. (finding that the Privacy Shield does not fully exclude the possibility of massive and indiscriminate collection of personal data by U.S. authorities and that the Ombudsperson mechanism “is not sufficiently independent and is not vested with adequate powers to effectively exercise its duty and does not guarantee a satisfactory remedy in case of disagreement”).
125 The Canadian adequacy decision, by contrast, is scarcely four pages. See supra note Error! Bookmark not defined.
National Intelligence (“ODNI”), and Department of Justice. It also heightened the requirements on organizations that certify to its principles. A notable similarity, however, is that Privacy Shield maintained Safe Harbor’s system of self-certification.

The Privacy Shield adequacy decision detailed the limits to national security access that exist in U.S. law, including some of the changes that were implemented since 2013. One important legislative development was the passage of the USA FREEDOM Act, which placed new limits on the NSA’s bulk telephony metadata program, introduced reforms to FISA Court oversight, and imposed new transparency and reporting requirements associated with government data collection. The Judicial Redress Act extended the protections of the U.S. Privacy Act of 1974 to non-U.S. residents, including the ability to bring civil claims against U.S. agencies. Most significantly, Presidential Policy Directive 28, which was executed in response to the Snowden disclosures and binds all federal executive agencies, limited bulk foreign surveillance to only six specific purposes.

---

127 Gabe Maldoff, We read privacy Shield so you don’t have to, IAPP Privacy Tracker (Mar. 7, 2016), https://iapp.org/news/a/we-read-privacy-shield-so-you-dont-have-to/.
131 Judicial Redress Act of 2015, H.R. 1428. Note, however, that redress for violations related to national security access is specifically exempt. Id.
132 See The White House, Office of the Press Secretary, Presidential Policy Directive/PPD-28, Signals Intelligence Activities (Jan. 17, 2014), http://www.whitehouse.gov/the-press-office/2014/01/17/presidential-policy-directive-signals-intelligence-activities (“In particular, when the United States collects nonpublicly available signals intelligence in bulk, it shall use that data only for the purposes of detecting and countering: (1) espionage and other threats and activities directed by foreign powers or their intelligence services against the United States and its interests; (2) threats to the United States and its interests from terrorism; (3) threats to the United States and its interests from the development, possession, proliferation, or use of weapons of mass destruction; (4) cybersecurity threats; (5) threats to U.S. or allied Armed Forces or other U.S or allied personnel; and (6) transnational criminal threats, including illicit finance and sanctions evasion related to the other purposes named in this section. In no
As a result of the Privacy Shield negotiation, the U.S. State Department agreed to appoint an Ombudsperson with responsibility for investigating complaints by EU residents, even if they cannot demonstrate that their data have in fact been accessed.\(^{133}\) Additionally, in supporting letters, high-level U.S. officials provided explicit assurances on the limits of national security access to EU data. For example, ODNI stated that the U.S. Intelligence Community “does not engage in indiscriminate surveillance of anyone, including ordinary European citizens,” and that U.S. limitations on access would apply to any interception of communications outside the U.S., such as in transit on transatlantic cables.\(^{134}\) It is not clear to what extent these assurances denote new limits on surveillance, or whether they repeat existing policy and are designed to assure the European public. If they do supply new limits, some have questioned whether they will have binding effect on future administrations.\(^{135}\) Regardless of any criticism, however, these letters could raise the bar for future adequacy decisions, which will perhaps have to include similar assurances.

D. Crafting a Standard for Evaluating Adequacy

Whatever the case was pre-Schrems, post-Schrems adequacy decisions will have to compare foreign regimes to the standard set out in the EU Charter. Although in Schrems the CJEU did not evaluate U.S. national security access, it made clear that the EU Charter prohibits mass and indiscriminate surveillance.

In pointing to the failures of the Safe Harbor Decision, the Schrems Court enunciated broad principles that could inform the essential equivalence test required by the EU Charter. The Court found that, where legislation interferes with the EU Charter, it must “lay down clear and precise rules . . . so that the persons whose personal data is concerned have sufficient guarantees . . . against the risk of abuse and against any unlawful access and use of that data.”\(^{136}\) The Court also noted that Safe Harbor may have permitted U.S. authorities to access data “beyond what was strictly necessary and proportionate to the protection of national security” and without providing EU residents “administrative or judicial means of redress enabling, in particular, the data relating to

---

\(^{133}\) Privacy Shield Annexes, supra note 126.

\(^{134}\) Id.


\(^{136}\) Schrems Decision, supra note 98, para. 91.
them to be accessed and, as the case may be, rectified or erased.\textsuperscript{137} Similarly, in \textit{Digital Rights Ireland}, the Court found, “the Charter provides that any limitation on the exercise of the rights and freedoms laid down by the Charter must be provided for by law, respect their essence and, subject to the principle of proportionality, limitations may be made to those rights and freedoms only if they are necessary and genuinely meet the objectives of general interest recognized by the Union or the need to protect the rights and freedoms of others.”\textsuperscript{138}

Summarizing these principles, the Article 29 Working Party articulated the “essentially equivalent” test as follows:\textsuperscript{139}

(1) processing must be based on clear, precise, and accessible rules so that a reasonably informed person can foresee what might happen with her data when transferred (“clear, precise, and accessible rules”);
(2) government access to personal data must be strictly necessary and proportionate to the protection of national security (“strictly necessary and proportionate”);
(3) there must be a mechanism of independent oversight of national security access that is effective and impartial (“independent oversight”); and,
(4) adversely affected individuals must have access to effective judicial or administrative redress before an independent body (“effective redress”).

In sum, the test for essential equivalence under the EU Charter, as enunciated in \textit{Schrems}, requires a third country to meet the four guarantees outlined by the Article 29 Working Party. Because the Court has never evaluated a third country under this test, and because the ECHR contains a right to privacy similar to that in the EU Charter, the case law of the ECtHR helps to inform the application of this test. Additionally, as the first regime specifically designed to address the concerns in \textit{Schrems}, Privacy Shield may further elaborate the appropriate application of the test.


\textsuperscript{137} \textit{Id.} at para. 90.
\textsuperscript{138} Digital Rights Ireland, \textit{supra} note 26, para. 38.