NATIONAL SECURITY LAW — SURVEILLANCE — COURT OF JUSTICE OF THE EUROPEAN UNION INVALIDATES THE EU-U.S. PRIVACY SHIELD. — Case C-311/18, *Data Protection Commissioner v. Facebook Ireland Ltd.*, ECLI:EU:C:2020:559 (July 16, 2020).

The United States and the European Union are the world's "largest net exporters of digitally-enabled services."[1] Transatlantic data flows between the two account for approximately half of the United States' data transfers and more than half of the European Union's.[2] Since 2016, the EU-U.S. Privacy Shield has facilitated these transfers by establishing data privacy safeguards and protections for EU data subjects.[3] Recently, in *Data Protection Commissioner v. Facebook Ireland Ltd.*[4] (*Schrems II*), the Court of Justice of the European Union (CJEU) invalidated the EU-U.S. Privacy Shield, finding that U.S. surveillance laws do not afford EU data subjects adequate levels of protection under the European Union's Charter of Fundamental Rights (the "Charter") and General Data Protection Regulation (GDPR).[5] Specifically, the court found that section 702 of the Foreign Intelligence Surveillance Act[6] (FISA) and Executive Order 12,333[7] are overly broad and lack sufficient redress for EU data subjects.[8] However, in reaching its decision, the court did not fully examine section 702 parameters and processes.[9] The court's incomplete analysis creates substantial uncertainty regarding the legal

---

[1] DANIEL S. HAMILTON & JOSEPH P. QUINLAN, THE TRANSATLANTIC ECONOMY 2020: ANNUAL SURVEY OF JOBS, TRADE AND INVESTMENT BETWEEN THE UNITED STATES AND EUROPE, at viii (2020).

[2] *Id.*

[3] *See* Council Regulation 2016/679, 2016 O.J. (L 119) 1, 61; U.S. DEP'T OF COM., EU-U.S. PRIVACY SHIELD FRAMEWORK PRINCIPLES 1, https://www.privacyshield.gov/privacy-shield-principles-full-text [https://perma.cc/V25V-GNKM]; Press Release, Wilbur Ross, Sec'y of Com., U.S. Dep't of Com., U.S. Secretary of Commerce Wilbur Ross Statement on *Schrems II* Ruling and the Importance of EU-U.S. Data Flows (July 16, 2020), https://www.commerce.gov/news/press-releases/2020/07/us-secretary-commerce-wilbur-ross-statement-schrems-ii-ruling-and [https://perma.cc/7M2L-AWB6].

[4] Case C-311/18, ECLI:EU:C:2020:559 (July 16, 2020).

[5] *See id.* ¶¶ 198–201. Under the GDPR, the protection of persons with respect to the processing of personal data is a "fundamental right." Council Regulation 2016/679, *supra* note 3, at 1.

[6] 50 U.S.C. § 1881a. Section 702 authorizes the U.S. government to acquire foreign intelligence information by targeting non–U.S. persons located outside of the United States. *Id.* § 1881a(a), (b)(3). Foreign intelligence information collected under section 702 is obtained "from or with the assistance of an electronic communication service provider." *Id.* § 1881a(h)(2)(A)(vi); *see also id.* § 1881a(i) (outlining compelled assistance from electronic communication service providers).

[7] Exec. Order No. 12,333, 3 C.F.R. § 200 (1982), *reprinted as amended in* 50 U.S.C. § 3001 note; *see also* Samuel J. Rascoff, *Presidential Intelligence*, 129 HARV. L. REV. 633, 648 n.65 (2016) (describing the order as "something like a basic charter for the intelligence community").

[8] *See Schrems II*, Case C-311/18, ¶¶ 184, 192.

[9] As the more restrictive authority, section 702's adequacy is likely determinative of that of Executive Order 12,333. *See* Laura K. Donohue, *Section 702 and the Collection of International Telephone and Internet Content*, 38 HARV. J.L. & PUB. POL'Y 117, 144–52 (2015).

framework under which it will analyze data-sharing mechanisms in the future and the data privacy standards to which third countries will be held.

The CJEU invalidated a previous EU-U.S. data-sharing provision — the "Safe Harbor Framework" — on October 6, 2015.[10] The decision arose from a 2013 complaint filed by Maximilian Schrems against Facebook Ireland Ltd. and submitted to the Irish Data Protection Commissioner.[11] Schrems sought to prohibit Facebook Ireland from transferring his personal data to the United States under the Safe Harbor Framework, arguing that U.S. laws did not ensure sufficient protection of data against U.S. government surveillance activities.[12] The court ultimately invalidated the Safe Harbor Framework in *Schrems v. Data Protection Commissioner*[13] (*Schrems I*), finding that it did not ensure privacy protections for EU data subjects "essentially equivalent" to those guaranteed under EU law.[14]

In the wake of the *Schrems I* decision, Facebook Ireland transferred data to U.S.-based Facebook, Inc. using standard contractual clauses (SCCs).[15] On December 1, 2015, Schrems filed an updated complaint against Facebook Ireland with the Irish Data Protection Commission, challenging the adequacy of SCCs.[16] The Commissioner published a draft decision, provisionally finding that data transferred to the United States might be accessed by the U.S. government in a manner that was not compatible with EU law and that did not provide effective legal remedies for EU data subjects.[17] The Commissioner further found that SCCs could not remedy this defect, as they were not binding on U.S. authorities.[18]

Following the invalidation of the Safe Harbor Framework and Schrems's revised complaint, the European Commission adopted the "Privacy Shield."[19] Under this new data-sharing framework, the United States created an independent Privacy Shield Ombudsperson, charged

---

10 Case C-362/14, Schrems v. Data Prot. Comm'r (*Schrems I*), ECLI:EU:C:2015:650, ¶ 98 (Oct. 6, 2015); *see id.* ¶¶ 96–106.

11 Complaint Against Facebook Ireland Ltd — 23 "PRISM" at 1, *Schrems I*, Case C-362/14.

12 *See id.* Schrems argued that the lack of sufficient protections violated the Irish Data Protection Act and the European Data Protection Directive. *Id.* Schrems cited a news article published by *The Guardian* that indicated that Facebook, Inc. had granted "mass access" to user data to the NSA under the PRISM national security program. *Id.*; *see also* Glenn Greenwald & Ewen MacAskill, *NSA Prism Program Taps In to User Data of Apple, Google and Others*, THE GUARDIAN (June 7, 2013, 3:23 PM), https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data [https://perma.cc/MQU9-X9U6].

13 Case C-362/14, ECLI:EU:C:2015:650.

14 *Id.* ¶ 96; *see id.* ¶¶ 96–106.

15 *See Schrems II*, Case C-311/18, ¶ 54.

16 *Id.* ¶ 55.

17 *Id.* ¶ 56.

18 *Id.*

19 Commission Decision 2016/1250, 2016 O.J. (L 207).

with oversight responsibilities regarding national security interference.[20] The United States also provided the European Union with detailed commitments regarding limitations and safeguards pertaining to data access for national security purposes.[21] The European Commission formally adopted the Privacy Shield via Commission Decision 2016/1250 (the "Privacy Shield Decision"), an "adequacy decision" that determined that the United States "ensure[d] an adequate level of [data privacy] protection" to EU data subjects.[22]

Meanwhile, the Data Protection Commissioner had brought the *Schrems II* proceedings before the High Court of Ireland,[23] which, in turn, referred eleven questions to the CJEU.[24] The High Court asked that the CJEU determine, inter alia, whether data transfers under SCCs violated privacy and data protection rights guaranteed under the Charter.[25] The High Court also asked the CJEU to determine whether the European Commission's Privacy Shield Decision was binding upon national data protection authorities and the courts of EU member states.[26]

The CJEU upheld SCCs as valid data transfer mechanisms, but placed monitoring responsibilities on supervising authorities to ensure the enforcement of the GDPR within the context of SCCs.[27] The court found that articles 46(1) and 46(2)(c) of the GDPR require that EU subjects whose data is transferred to a third country be "afforded a level of protection essentially equivalent to that guaranteed within the European Union," including "appropriate safeguards, enforceable rights and effective legal remedies."[28] According to the court, such protection may take the form of a valid European Commission adequacy decision

---

[20] *Id.* ¶ 65.

[21] EUR. COMM'N, ANNEXES TO THE COMMISSION IMPLEMENTING DECISION PURSUANT TO DIRECTIVE 95/46/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL ON THE ADEQUACY OF THE PROTECTION PROVIDED BY THE EU-U.S. PRIVACY SHIELD 77–94 (2016).

[22] Council Regulation 2016/679, *supra* note 3, art. 45, at 61; *see* Commission Decision 2016/1250, *supra* note 19, ¶ 13. The European Commission may adopt adequacy decisions for "[a] third country, a territory or one or more specified sectors within that third country, or [for] international organisation[s]." Council Regulation 2016/679, *supra* note 3, art. 45, at 61.

[23] *Schrems II*, Case C-311/18, ¶ 57.

[24] *Id.* ¶ 68.

[25] *See id.*

[26] *See id.*

[27] *See id.* ¶ 108. Supervisory authorities are independent public authorities of EU member states that monitor compliance with the GDPR. Council Regulation 2016/679, *supra* note 3, art. 4, at 34; *id.* art. 51, at 65.

[28] *Schrems II*, Case C-311/18, ¶ 105. The CJEU noted that "the assessment of the level of protection afforded in the context of such a transfer must," inter alia, consider the relevant laws of a third country "as regards any access by the public authorities of that third country to the personal data transferred." *Id.* The court found that the GDPR's protections apply to the commercial transfer of data to a third country, regardless of the likelihood that that data will "be processed by the authorities of [that] third country . . . for the purposes of public security, defence and State security." *Id.* ¶ 89.

or be ensured through SCCs.[29] If data is transferred through SCCs, however, the relevant supervisory authority must ensure that the SCCs can be complied with in the third country or that EU standards for data protection can otherwise be maintained.[30]

Turning to the validity of the European Commission's Privacy Shield Decision, the CJEU found that U.S. limitations on data protection violate the principle of proportionality.[31] In order to satisfy the requirement of proportionality, legislation must incorporate "clear and precise rules governing the scope and application of the measure in question and imposing minimum safeguards."[32] Moreover, any legislation infringing upon an EU data subject's data privacy rights must be "limited to what is strictly necessary."[33] The court first acknowledged that U.S. national security, public interest, and law enforcement interests have primacy over and may interfere with the fundamental rights of EU data subjects.[34] However, the court then held that U.S. surveillance laws are not sufficiently circumscribed to ensure EU data subjects privacy protections essentially equivalent to those ensured under the Charter.[35] In particular, the court concluded that U.S. limitations on data protection violate the principle of proportionality, as it found that U.S. surveillance programs — specifically section 702 of FISA and Executive Order 12,333 — do not impose "minimum safeguards" and are not "limited to what is strictly necessary."[36]

The CJEU further found that U.S. law does not provide effective remedies to EU subjects whose data privacy has been compromised, cementing the invalidity of the Privacy Shield.[37] The court determined that Presidential Policy Directive 28, which sets forth legal requirements for U.S. "signals intelligence" activities,[38] "does not grant data subjects actionable rights before the courts against the US authorities."[39] The court then determined that the Privacy Shield Ombudsperson mechanism is not sufficiently independent from the Executive and does not provide for a cause of action before a body that has the power to adopt

---

[29] *See id.* ¶¶ 94–96.
[30] *See id.* ¶ 121.
[31] *Id.* ¶ 184.
[32] *Id.* ¶ 176.
[33] *Id.*
[34] *See id.* ¶¶ 164–65.
[35] *Id.* ¶ 185.
[36] *Id.* ¶ 184.
[37] *See id.* ¶¶ 186, 190, 192.
[38] *See generally* Press Release, Off. of the Press Sec'y, Presidential Policy Directive — Signals Intelligence Activities (Jan. 17, 2014), http://www.whitehouse.gov/the-press-office/2014/01/17/presidential-policy-directive-signals-intelligence-activities [https://perma.cc/RKG4-MN9A].
[39] *Schrems II*, Case C-311/18, ¶ 181.

binding decisions.[40] In light of these findings, the court held that EU subjects are without effective remedy to address U.S. data transfer deficiencies.[41] The court therefore declared the Privacy Shield Decision invalid.[42]

In invalidating the Privacy Shield, the CJEU failed to set forth a legal framework through which the European Commission may make and assess adequacy decisions. The court's invalidation of the Privacy Shield rested, in large part, on the court's determination that the United States does not provide an "adequate level of protection" for personal data transferred from the European Union.[43] Yet the court's proportionality assessment of U.S. surveillance laws — particularly section 702 — was at times cursory, and frequently unclear. As a result, it is not apparent what aspects of section 702 expand collection beyond what is strictly necessary or lack minimum safeguards. The court's incomplete analysis therefore provides little guidance regarding the validity of current and future adequacy decisions.

First, the court failed to engage fully with the limitations that section 702 incorporates. Instead, it summarily determined that the legislation "does not indicate *any* limitations on the power it confers to implement surveillance programmes for the purposes of foreign intelligence."[44] While the court's language seemingly construes section 702 as an indiscriminate surveillance authority, section 702 collection "consists entirely of targeting specific persons about whom an individualized determination has been made."[45] Under section 702, communications are targeted through the use of identifiers called "selectors," such as email addresses and phone numbers, that are "used by a non–U.S. person who is reasonably believed to be located outside the United States and who is expected to possess, receive, and/or is likely to communicate foreign intelligence information."[46] Selectors are "never key words or names of

---

[40] *See id.* ¶¶ 195–97. The CJEU did not acknowledge that, if any complaint submitted to the Ombudsperson reveals a violation of U.S. law, the unlawfully collected data is purged from U.S. government databases and removed from U.S. intelligence reports. EUR. COMM'N, REPORT FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL ON THE THIRD ANNUAL REVIEW OF THE FUNCTIONING OF THE EU-U.S. PRIVACY SHIELD 7 (2019). Under this system, an EU subject may "obtain the deletion of his or her personal data if it was unlawfully collected and processed by the U.S. Intelligence Community." *Id.*

[41] *See Schrems II*, Case C-311/18, ¶ 192.

[42] *Id.* ¶¶ 199–201.

[43] *See id.* ¶¶ 198–201.

[44] *Id.* ¶ 180 (emphasis added).

[45] PRIV. & C.L. OVERSIGHT BD., REPORT ON THE SURVEILLANCE PROGRAM OPERATED PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT 111 (2014), https://documents.pclob.gov/prod/Documents/OversightReport/823399ae-92ea-447a-ab60-oda28b555437/702-Report-2.pdf [https://perma.cc/4KY5-BL4D] [hereinafter PCLOB REPORT].

[46] OFF. OF THE DIR. OF NAT'L INTEL., STATISTICAL TRANSPARENCY REPORT REGARDING THE USE OF NATIONAL SECURITY AUTHORITIES: CALENDAR YEAR 2019, at 11 (2020); *accord* NAT'L SEC. AGENCY, NSA'S SECTION 702 TARGETING PROCEDURES 4 (2018).

persons,"[47] and the U.S. government may not intentionally collect communications referencing, but not to or from, an individual.[48] An analyst who requests selector tasking must provide a targeting rationale,[49] including a written explanation detailing the analyst's determination that the target will produce foreign intelligence information.[50] While the court took issue with the fact that the Foreign Intelligence Surveillance Court (FISC) does not approve individual section 702 targeting requests,[51] it did not consider any of these procedural requirements, all of which operate apart from FISC review. As such, the court failed to engage in a nuanced assessment of whether section 702 targeting requirements and procedures achieve functionally similar protections to the individual approval measures the court desired.

Second, the court determined that section 702 does not impose minimum safeguards to protect against abuse, but failed to evaluate the safeguards section 702 *does* incorporate, including FISC oversight, administrative reviews, and democratic reassessment. The FISC is not a mere "rubber stamp" on section 702 certifications.[52] The FISC reviews annual certifications submitted by the Attorney General and the Director of National Intelligence detailing targeting procedures to ensure they are consistent with statutory requirements,[53] and must issue a written opinion explaining its approval or nonapproval of the certifications.[54] The court has denied annual certifications due to deficiencies in agency querying and minimization procedures, requiring revised procedures prior to approval.[55] Moreover, the NSA is required to report all instances of targeting procedure noncompliance to the Office of the Director of National Intelligence and the Department of Justice,[56] and the FISC

---

47 EUR. COMM'N, COMMISSION STAFF WORKING DOCUMENT ACCOMPANYING THE DOCUMENT: REPORT FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL ON THE THIRD ANNUAL REVIEW OF THE FUNCTIONING OF THE EU-U.S. PRIVACY SHIELD 20 (2019).

48 NAT'L SEC. AGENCY, *supra* note 46, at 2. The FISA Amendments Reauthorization Act of 2017 implemented limitations on "abouts" collection under section 702. Pub. L. No. 115-118, § 103(a), 132 Stat. 3, 10 (2018) (codified at 50 U.S.C. § 1881a(b)(5)).

49 OFF. OF THE DIR. OF NAT'L INTEL., *supra* note 46, at 12.

50 *See* NAT'L SEC. AGENCY, *supra* note 46, at 8.

51 *See Schrems II*, Case C-311/18, ¶ 179.

52 *See* Testimony of Professor Peter Swire at 5-2, 5-9 to 5-18, Data Prot. Comm'r v. Facebook Ir. Ltd. [2017] IEHC 545 (Ir.).

53 *See* 50 U.S.C. § 1881a(j).

54 *See id.* § 1881a(j)(3)(A)–(C).

55 *See In re* DNI/AG 702(H) Certifications 2018 [Redacted], 941 F.3d 547, 565 (FISA Ct. Rev. 2019); [Redacted], 402 F. Supp. 3d 45, 108–09 (FISA Ct. 2018), *aff'd in part sub nom. In re* DNI/AG 702(H) Certifications 2018 [Redacted], 941 F.3d 547.

56 NAT'L SEC. AGENCY, NSA DIRECTOR OF CIVIL LIBERTIES AND PRIVACY OFFICE REPORT: NSA'S IMPLEMENTATION OF FOREIGN INTELLIGENCE SURVEILLANCE ACT SECTION 702, at 3 (2014), https://www.nsa.gov/Portals/70/documents/about/civil-liberties/reports/nsa_report_on_section_702_program.pdf [https://perma.cc/SDU5-GLP4].

Rules of Procedure require that the government immediately notify the FISC of all incidents of noncompliance with FISC authorization or applicable law.[57] Thus, the FISC's review of certification procedures "is not limited to the procedures as written, but also includes an examination of how the procedures have been and will be implemented."[58] Apart from noting that the FISC does not approve individual targeting procedures, the CJEU did not evaluate the FISC's "[i]ndependent and [e]ffective [o]versight" role with regard to section 702 surveillance.[59]

Furthermore, the CJEU did not consider the oversight mechanisms that operate separately from and in addition to the FISC. The Attorney General and the Director of National Intelligence are statutorily required to conduct periodic compliance reviews and to provide such reviews to elements within the judicial and legislative branches.[60] Moreover, section 702 is subject to periodic democratic debate and reauthorization. Section 702, in its current form, is authorized through December 31, 2023.[61] The "robust democratic deliberation" surrounding reauthorization has "produced important alterations to the program and a contemporary democratic reaffirmation of the program's value and legitimacy."[62] The sunset clause contained within section 702 ensures that the authority does not merely rely on prior authorizations and evaluations; it must continually prove that its national security aims are subject to sufficient safeguards regarding individual privacy and civil liberties.

The indeterminacy of the CJEU's invalidation of the Privacy Shield extends beyond section 702. Post–*Schrems II*, all existing adequacy decisions appear vulnerable to judicial invalidation,[63] and the path to

---

[57] U.S. FISC R.P. 13(b). Between December 2016 and May 2017, compliance incidents occurred in 0.37% of section 702 collection activity. ATT'Y GEN. & DIR. OF NAT'L INTEL., SEMIANNUAL ASSESSMENT OF COMPLIANCE WITH PROCEDURES AND GUIDELINES ISSUED PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT 5 (2018).

[58] OFF. OF THE DIR. OF NAT'L INTEL., *supra* note 46, at 11–12.

[59] Testimony of Professor Peter Swire, *supra* note 52, at 5-3; *see also id.* at 5-3 to 5-47 (discussing the FISC's effective independent oversight of surveillance applications, compliance monitoring and enforcement, and transparency initiatives).

[60] 50 U.S.C. § 1881a(m)(1). The Privacy and Civil Liberties Oversight Board has also conducted a comprehensive review of section 702 activities. PCLOB REPORT, *supra* note 45, at 2.

[61] FISA Amendments Reauthorization Act of 2017, Pub. L. No. 115-118, § 201(a)–(b), 132 Stat. 3, 19 (2018).

[62] Jack Goldsmith & Susan Hennessey, *The Merits of Supporting 702 Reauthorization (Despite Worries About Trump and the Rule of Law)*, LAWFARE (Jan. 18, 2018, 9:20 AM), https://www.lawfareblog.com/merits-supporting-702-reauthorization-despite-worries-about-trump-and-rule-law [https://perma.cc/MU4G-8USJ].

[63] *See* EUR. DATA PROT. BD., FREQUENTLY ASKED QUESTIONS ON THE JUDGMENT OF THE COURT OF JUSTICE OF THE EUROPEAN UNION IN CASE C-311/18 — *DATA PROTECTION COMMISSIONER V FACEBOOK IRELAND LTD AND MAXIMILLIAN SCHREMS* 4 (2020), https://edpb.europa.eu/sites/edpb/files/files/file1/20200724_edpb_faqoncjeuc31118_en.pdf [https://perma.cc/A8GP-CG9S] ("[T]he threshold set by the Court for transfers to the U.S. applies for any

future adequacy decisions is unclear.[64] The court's ruling leaves non–EU states without clear guidelines by which to assess compatibility with the European Charter and GDPR — legal standards to which EU member states' national security apparatuses are not themselves required to conform.[65] The GDPR provides little additional guidance, requiring that adequacy assessments take account of indeterminate elements such as a third country's "rule of law" and "respect for human rights."[66] Taken together, neither the GDPR nor the EU Charter define "adequate" or set forth clear metrics by which adequacy decisions can be appropriately made. And, as the CJEU has now invalidated two European Commission adequacy decisions, the viability of using existing adequacy decisions as a benchmark for future agreements is unsettled. Finally, because entities that rely on SCCs to transfer data to a third country bear the responsibility for assessing whether that country's surveillance laws and privacy protections meet EU standards, the court's unclear adequacy analysis extends to SCCs.[67]

The CJEU's invalidation of the Privacy Shield is less of a roadmap for adequacy and more of a warning. Rather than engage fully with U.S. surveillance law, the court contravened existing European Commission adequacy assessments, misconstrued the legal scope of section 702, and performed an incomplete assessment of the oversight mechanisms that prevent section 702's abuse. The CJEU's act of "solipsistic Europocrisy meets judicial imperialism"[68] invalidated the data transfer framework upon which over 5,000 U.S. and EU companies currently rely, leaving no discernible alternative — and substantial uncertainty — in its place.[69]

---

third country."); Joshua P. Meltzer, *The Court of Justice of the European Union in* Schrems II*: The Impact of GDPR on Data Flows and National Security*, BROOKINGS INST. (Aug. 5, 2020), https://www.brookings.edu/research/the-court-of-justice-of-the-european-union-in-schrems-ii-the-impact-of-gdpr-on-data-flows-and-national-security [https://perma.cc/9HF4-KRJ2].

64 *See* Meltzer, *supra* note 63.

65 Council Regulation 2016/679, *supra* note 3, at 3 ("[The GDPR] does not apply to issues of protection of fundamental rights and freedoms or the free flow of personal data related to activities which fall outside the scope of Union law, such as activities concerning national security.").

66 *Id.* art. 45, at 61.

67 *See* U.S. DEP'T OF COM. ET AL., INFORMATION ON U.S. PRIVACY SAFEGUARDS RELEVANT TO SCCS AND OTHER EU LEGAL BASES FOR EU-U.S. DATA TRANSFERS AFTER *SCHREMS II* 1 (2020), https://www.commerce.gov/sites/default/files/2020-09/SCCsWhitePaperFORMATTEDFINAL508COMPLIANT.PDF [https://perma.cc/J6WC-C6NG]; Sam Schechner & Emily Glazer, *Ireland to Order Facebook to Stop Sending User Data to U.S.*, WALL ST. J. (Sept. 9, 2020, 1:19 PM), https://www.wsj.com/articles/ireland-to-order-facebook-to-stop-sending-user-data-to-u-s-11599671980 [https://perma.cc/2U8M-WMQA].

68 Stewart Baker, *The Cyberlaw Podcast: Solipsistic Europocrisy Meets Judicial Imperialism*, LAWFARE (July 21, 2020, 2:08 PM), https://www.lawfareblog.com/cyberlaw-podcast-solipsistic-europocrisy-meets-judicial-imperialism [https://perma.cc/T64M-T4XP] (capitalization omitted).

69 Adam Satariano, *E.U. Court Strikes Down Trans-Atlantic Data Transfer Pact*, N.Y. TIMES (July 16, 2020), https://nyti.ms/393VklG [https://perma.cc/KUZ7-28FE].