William & Mary Bill of Rights Journal

Volume 30 (2021-2022)
Issue 2 *Algorithms and the Bill of Rights*

Article 6

12-2021

Seeking a Safe Harbor in a Widening Sea: Unpacking the Schrems Saga and What It Means for Transatlantic Relations and Global Cybersecurity

Scott J. Shackelford

SEEKING A SAFE HARBOR IN A WIDENING SEA: UNPACKING THE *SCHREMS* SAGA AND WHAT IT MEANS FOR TRANSATLANTIC RELATIONS AND GLOBAL CYBERSECURITY

Scott J. Shackelford*

INTRODUCTION

In June 2020, India banned TikTok along with fifty-nine other apps developed by Chinese firms.[1] The move, although not unexpected, was just part of a drive by the Indian government to challenge China's growing clout in the digital ecosystem, and in response to border clashes that left twenty Indian soldiers dead.[2] The rise of so-called "techno nationalism" is one component of a larger move toward greater data localization[3] and even cyber sovereignty.[4] This conceptualization of Internet

* Associate Professor of Business Law & Ethics, Indiana University Kelley School of Business; Chair, Indiana University–Bloomington Cybersecurity Risk Management Program; Executive Director, Ostrom Workshop.

[1] *See* Manish Singh, *India Bans TikTok, Dozens of Other Chinese Apps*, TECH. CRUNCH (June 29, 2020), https://techcrunch.com/2020/06/29/india-bans-tiktok-dozens-of-other-chinese-apps/ [https://perma.cc/HN68-G4D7].

[2] *See India Hits Back at China by Banning TikTok, Other Apps, As 'Techno-Nationalism' Rises*, WBUR (July 3, 2020), https://www.wbur.org/hereandnow/2020/07/03/india-china-tiktok-techno-nationalism [https://perma.cc/4ENH-N3YE].

[3] *See generally* Jennifer Huddleston & Jacqueline Varas, *Impact of Data Localization Requirements on Commerce and Innovation*, AM. ACTION F. (June 16, 2020), https://www.americanactionforum.org/insight/impact-of-data-localization-requirements-on-commerce-and-innovation/ [https://perma.cc/HQ8X-UDED].

[4] *See, e.g.*, Adam Segal, *China's Vision for Cyber Sovereignty and the Global Governance of Cyberspace*, NAT'L BUR. ASIAN RES. at 85–100 (Aug. 25, 2020), https://www.nbr.org/publication/chinas-vision-for-cyber-sovereignty-and-the-global-governance-of-cyberspace/ [https://perma.cc/Y9L7-4C6T].

governance represents a significant shift from long-held beliefs on the part of many Western nations about building a cyberspace that is "free, open, interoperable, secure, and resilient" and one that is more closed, highly regulated, and de-anonymized.[5] The debate over the future of Internet governance between those preferring more multilateral versus multi-stakeholder is an oversimplification, but it does highlight the different visions for cyberspace, including to what extent information sharing will be possible between digital walled gardens.[6] Such sharing is vital—if challenging—to permitting like-minded nations and other stakeholders to work together to defend against common threats and build a global culture of cybersecurity.[7] Yet even among historic allies, such as the transatlantic alliance between the United States and Europe, walls are going up that are making it more challenging for both the public and private sectors alike to pool their resources and expertise to better confront common challenges.

The drifting apart of the United States and Europe when it comes to privacy protections and data governance best practices predated the turbulence of the Trump administration. In 2015, for example,[8] the Court of Justice of the European Union (CJEU) invalidated the then fifteen-year-old EU-U.S. Safe Harbor Agreement in *Schrems v. Data Protection Commissioner*,[9] causing some consternation on the part of the more than 5,000 European and U.S. firms that relied on the Agreement to transfer EU data to U.S. servers.[10] With the benefit of hindsight, this decision may be seen as an important step in a growing rift between the EU and United States not only on privacy law, but also the future of Internet governance itself. Now, looking back six years later, while the feared economic harms were largely avoided, the ancestor agreement to Safe Harbor, called "Privacy Shield," faced another round of scrutiny before the CJEU tested many of the same legal issues that arose in the Safe Harbor

---

[5] *See* Robert Morgus & Justin Sherman, *The Five Ideals*: *The Idealized Internet vs. Internet Realities* (V. 1.0), NEW AM. FOUND., https://www.newamerica.org/cybersecurity-initiative/reports/idealized-internet-vs-internet-realities/the-five-ideals/ [https://perma.cc/SU7U-NVEX] (last visited Dec. 13, 2021).

[6] *See generally*, *e.g.*, Scott J. Shackelford et al., *Back to the Future of Internet Governance?*, 16 GEO. J. INT'L AFF. 83 (2015).

[7] *See* Deborah Housen-Couriel, *Information Sharing as a Critical Best Practice for the Sustainability of Cyber Peace*, *in* CYBER PEACE: CHARTING A PATH TOWARD A SUSTAINABLE, STABLE, AND SECURE CYBERSPACE (Scott J. Shackelford, Frederick Douzet, & Chris Ankersen eds., 2021).

[8] *Europe Has to Rebuild Its Safe Harbor*, BLOOMBERG VIEW (Oct. 19, 2015), http://www.bloombergview.com/articles/2015-10-19/europe-has-to-rebuild-its-safe-harbor [https://perma.cc/G6DB-N7KK].

[9] Case C-362/14, Maximillian Schrems v. Data Protection Comm'r, ECLI:EU:C:2015:650, ¶ 107 (Oct. 6, 2015).

[10] Daniel Alvarez, *Safe Harbor Is Dead; Long Live the Privacy Shield?*, A.B.A. (May 20, 2016), https://www.americanbar.org/groups/business_law/publications/blt/2016/05/09_alvarez/ [https://perma.cc/T698-SCR4].

dispute, but with the addition of Standard Contractual Clauses (SCCs) that have been used for decades to help firms transfer data between EU and non-EU nations.[11]

This Article reviews this history as a case study for larger issues surrounding information sharing and assesses the *Schrems* saga, including what options exist for resolving this transatlantic impasse given the CJEU's July 2020 decision invalidating Privacy Shield.[12] At stake are larger questions about the ability of like-minded nations, and indeed the international community, to come together to meaningfully address common cyber-enabled threats. The Article is structured as follows. Part I examines *Schrems I* (*Schrems v. Data Protection Commissioner*) and the fall of the Safe Harbor regime. Part II analyzes *Schrems II* (*Data Protection Commissioner v. Facebook & Max Schrems*) along with the rise and fall of Privacy Shield. Part III focuses on opportunities to bridge the data governance divide and present a united front to help ensure a free, open, interoperable, secure, and resilient vision for cyberspace.

I. *SCHREMS I*: *SCHREMS V. DATA PROTECTION COMMISSIONER* (FALL OF SAFE HARBOR)

The case that has become colloquially known as *Schrems I* was brought by an Austrian law student and civil rights advocate, Maximilian Schrems, who sought to challenge Facebook's international data transfers from Ireland (where Facebook's European subsidiary is headquartered) to the United States, arguing that this practice infringed on his privacy rights due to the potential for U.S. government surveillance.[13] The Irish Data Protection Commissioner rejected Schrems' complaint on the grounds that the European Commission had already decided that the United States ensured an adequate level of privacy protections.[14] Schrems appealed that decision to the Irish High Court, which referred the dispute to the CJEU.[15]

At the heart of the case was the Safe Harbor Agreement negotiated between the EU and United States in response to the 1998 EU Data Protection Directive (DPD),

---

[11] *See* Jennifer Baker, *EU High Court Hearings to Determine Future of Privacy Shield*, SCCs, INT'L ASS'N PRIV. PROS. (June 25, 2019), https://iapp.org/news/a/eu-high-court-hearings-to-determine-future-of-privacy-shield-standard-contractual-clauses/ [https://perma.cc/EZ8J-7X45]; *Standard Contractual Clauses (SCC)*, EUR. COMM'N, https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en [https://perma.cc/6JUJ-Z44D] (last visited Dec. 13, 2021).

[12] *See* Alaap B. Shah, *CJEU Invalidated the EU-US Privacy Shield Framework*, NAT'L L. REV. (July 28, 2020), https://www.natlawreview.com/article/ecj-invalidated-eu-us-privacy-shield-framework#:~:text=On%20July%207%2C%20the%20Court,C%2D311%2F18) [https://perma.cc/4EMF-PDMD].

[13] *See, e.g.*, Leo Kelion, *Facebook Data Transfers Threatened by Safe Harbor Ruling*, BBC (Oct. 6, 2015), http://www.bbc.com/news/technology-34442618 [https://perma.cc/SN7S-4G6J]; Baker, *supra* note 11.

[14] *See* Scott Russell, *Unsafe Harbor?*, CTR. APPLIED CYBERSEC. RSCH. (Oct. 9, 2015), https://cacrcybersecurity.wordpress.com/2015/10/09/unsafe-harbor/ [https://perma.cc/3LS6-3Y8B].

[15] *Id.*

which directed EU Member States to enact legislation containing certain privacy safeguards and prohibited the transferring of data on EU persons to non-EU nations that do not maintain adequate privacy safeguards.[16] The architects of this provision had the best intentions, namely to ratchet up privacy protections in EU partners, but the agreement left U.S. firms (many of which then, as now, are global tech leaders) in a difficult position given that, until the Safe Harbor Agreement was finalized, U.S. privacy law was found to be inadequate.[17] Under Safe Harbor, U.S. companies transferring data on EU persons pledged to self-certify that safeguards were in place that went beyond those required by the more sector-specific U.S. privacy law.[18] It was largely successful at easing transatlantic data flows, at least until the 2013 revelations by former NSA contractor Edward Snowden, who succeeded in bringing to light a number of U.S. surveillance programs.[19] These resulted in thirteen recommendations by the European Commission for revising Safe Harbor and set the stage for *Schrems I*.[20]

Among other concerns, in its *Schrems I* decision the CJEU noted that carve outs in the Safe Harbor Agreement—such as for U.S. national security, public interest, and law enforcement—opened the door for bulk data collection, including the NSA program code-named PRISM.[21] This reasoning led the CJEU to hold that: (1) the U.S. bulk collection of personal data violated the privacy rights of EU citizens, stating that "generali[z]ed" data storage by a foreign government lacking any objective criteria being specified as to the extent of the data's use is inconsistent with the DPD;[22] and (2) that EU citizens were not afforded the opportunity to challenge these U.S. practices, compromising their right to judicial review.[23] Ultimately the CJEU decided that no amount of self-certification could get around U.S. surveillance practices, which were found to be irreconcilable with EU privacy law (even though the USA Freedom Act, passed prior to the *Schrems I* ruling, outlaws the kind of bulk data collection that this CJEU decision says violates the DPD).[24] It also found that the

---

[16] *See U.S.-EU Safe Harbor Framework*, FED. TRADE COMM'N, https://www.ftc.gov/tips-advice/business-center/privacy-and-security/u.s.-eu-safe-harbor-framework [https://perma.cc/8TCJ-U7CR] (last visited Dec. 13, 2021).

[17] *See* DOUGLAS K. VAN DUYNE ET AL., THE DESIGN OF SITES 328 (2003).

[18] *See* JOHN K. HALVEY & BARBARA MURPHY MELBY, BUSINESS PROCESS OUTSOURCING: PROCESS, STRATEGIES, AND CONTRACTS 472 (2007).

[19] *See, e.g.*, Kieren McCarthy, *Snowden, Schrems, Safe Harbor . . . It's Time to Rethink Privacy Policies, Says FTC Commish*, THE REG. (Oct. 23, 2015, 8:34 PM), http://www.theregister.co.uk/2015/10/23/ftc_eu_safe_harbor/ [https://perma.cc/Y896-ZJEY].

[20] *See* Russell, *supra* note 14; *see Europe Has to Rebuild Its Safe Harbor*, BLOOMBERG VIEW (Oct. 19, 2015, 12:01 AM), http://www.bloombergview.com/articles/2015-10-19/europe-has-to-rebuild-its-safe-harbor [https://perma.cc/2JZS-S5SC].

[21] Case C-362/14, Maximillian Schrems v. Data Protection Commissioner (*Schrems I*), ECLI:EU:C:2015:650, ¶ 22 (Oct. 6, 2015).

[22] *Id.* ¶ 93.

[23] *Id.* ¶ 23.

[24] *Id.* ¶¶ 86, 101 (For more on reactions to the USA Freedom Act, see Bill Chappell,

CJEU alone has the power to decide whether or not European Commission decisions on the privacy practices of other nations are valid.[25]

This outcome resulted in the fall of the Safe Harbor regime, calling into question whether U.S. firms could continue transferring data collected on EU citizens back to U.S.-based data centers. It also teed up larger questions as to the ability of the United States and Europe to come together on central questions of data governance including with regards to information sharing, which remained largely unresolved, setting the stage for *Schrems II*. These cases also highlight the extent to which national security considerations are influencing these debates about privacy rights that could fuel a new wave of data localization, which would not only be costly and challenging, but also risk the $7 trillion transatlantic economic and security relationship.[26]

II. *SCHREMS II*: *DATA PROTECTION COMMISSIONER V. FACEBOOK & MAX SCHREMS* (RISE AND FUTURE OF PRIVACY SHIELD)

Following the CJEU ruling invalidating Safe Harbor, Irish judges confirmed that U.S. authorities "did indeed engage in mass processing of Europeans' data."[27] This prompted the EU and the United States to come together and create a replacement regime for Safe Harbor called Privacy Shield.[28] The new agreement differed in several ways from its predecessor in response to the CJEU's *Schrems I* ruling, including instituting new requirements for privacy policies to be posted to the U.S. Department of Commerce Program List.[29] It also grants "[t]he right of data subjects to access [their] data," "[a]cknowledge[s] liability in relation to onward data transfers," accepts binding arbitration to resolve disputes, and requires covered entities to "[t]ake steps to stop unauthorized processing" and to minimize the amount of time that data is retained.[30] After Privacy Shield was created in 2016, by three years later

---

Senate Approves USA Freedom Act, Obama Signs It, After Amendments Fail, NPR (June 2, 2015, 4:07 PM), http://www.npr.org/sections/thetwo-way/2015/06/02/411534447/senateis-poised-to-vote-on-house-approved-usa-freedom-act [https://perma.cc/VAP6-DL7S]).

[25] *See* Russell, *supra* note 14.

[26] *See* Kenneth Propp & Peter Swire, *Geopolitical Implications of the European Court's Schrems II Decision*, LAWFARE (July 17, 2020, 11:31 AM), https://www.lawfareblog.com/geopolitical-implications-european-courts-schrems-ii-decision [https://perma.cc/ZDM6-9UNG]. *Schrems I*, Case C-362/14, ECLI:EU:C:2015:650.

[27] Baker, *supra* note 11.

[28] Press Release, Eur. Comm'n, EU-U.S. Privacy Shield: Third Review Welcomes Progress While Identifying Steps for Improvement, U.N. Press Release No. IP/16/6134 (Oct. 23, 2019) [hereinafter Press Release, EU-U.S. Privacy Shield].

[29] *Privacy Shield Program Overview*, PRIV. SHIELD (last visited Dec. 13, 2021), https://www.privacyshield.gov/Program-Overview [https://perma.cc/3KS4-6F3R].

[30] David A. Zetoony, *A Side-By-Side Comparison of "Privacy Shield" and the "Safe Harbor*," BRYAN CAVE (2016), https://iapp.org/media/pdf/resource_center/Comparison-of-Privacy-Shield-and-the-Safe-Harbor.pdf [https://perma.cc/AW2S-NGJR].

some 5,000 companies participated in Privacy Shield, with the EU Commissioner for Justice, Consumers and Gender Equality, Věra Jourová, calling it a "success story."[31]

Yet the status quo has its detractors, including Schrems, who launched a lawsuit challenging Facebook's reliance on so-called Standard Contractual Clauses (SCCs) to transfer data from Ireland back to its U.S. headquarters, along with three French digital rights groups who brought a separate but related action claiming that Privacy Shield "fail[ed] to uphold fundamental EU rights."[32] In essence, Schrems and these other groups argued that these data, both while they are being transferred and when at rest in U.S. data centers, could be accessed by U.S. intelligence agencies in violation of the EU's General Data Protection Regulation (GDPR).[33] This groundbreaking data governance regime, which came into force in 2018 after the outcome in *Schrems I*, is arguably among "the toughest privacy and security law[s] in the world."[34] It is notable both for its breadth (under GDPR Article 4 "any information relating to an identified or identifiable natural person" are afforded protections under GDPR including the IP addresses of users),[35] and enforcement with fines that could reach up to four percent of a firm's global total revenue.[36] Among other practices mandated under GDPR are provisions related to data transfers, which apply when personal data is being transferred to a non-EEA (European Economic Area) nation to which GDPR does not apply.[37] One way around this issue is through so-called "adequacy decision," in which "the EU Commission after thorough evolution of national laws have concluded that a country's data protection laws are essentially equally good as the GDPR."[38] As of February 2021, a dozen nations have been designated as "adequate" for purposes of EU data governance; negotiations are ongoing with South Korea.[39]

---

[31] Press Release, EU-U.S. Privacy Shield, *supra* note 28.

[32] Baker, *supra* note 11.

[33] *See, e.g.*, *Schrems II a Summary—All You Need to Know*, GDPR SUMMARY (Nov. 23, 2020), https://www.gdprsummary.com/schrems-ii/ [https://perma.cc/D29E-AEJ6].

[34] *What Is GDPR, the EU's New Data Protection Law?*, GDPR.EU, https://gdpr.eu/what-is-gdpr/ [https://perma.cc/9U3T-LQ38] (last visited Dec. 13, 2021).

[35] Luke Irwin, *GDPR: How the Definition of Personal Data Has Changed*, IT GOVERNANCE BLOG (Apr. 10, 2019), https://www.itgovernance.co.uk/blog/gdpr-how-the-definition-of-personal-data-will-change [https://perma.cc/6BH7-TWKW] (noting that "Article 2 of the GDPR stating that the Regulation applies to 'the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system'").

[36] *What Are the GDPR Fines?*, GDPR.EU, https://gdpr.eu/fines/ [https://perma.cc/65EC-V9GZ] (last visited Dec. 13, 2021).

[37] *Id.*

[38] *Schrems II a Summary—All You Need to Know*, *supra* note 33 (noting that there are also options for binding corporate rules for intragroup transfers, and under GDPR Article 49 derogations).

[39] These nations include: Andorra, Argentina, Canada (commercial organizations), Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Switzerland and Uruguay.

It should come as no surprise that the United States is not on the list, calling Facebook's data transfers into question.[40]

Initial hearings in Ireland's Supreme Court in July 2019 were postponed until the suit brought by Ireland's Data Protection Commissioner (DPC) against Schrems and Facebook before the CJEU was resolved (*Schrems II*).[41] Among other topics, the CJEU was asked to decide "whether Facebook data transfers to the U.S. meet EU privacy standards."[42] Facebook argued that they do, given that they comport with Privacy Shield, but the bigger question remained as to whether U.S. government surveillance violate the privacy rights of Europeans under GDPR.[43] A decision came down in July 2020, with the CJEU deciding to invalidate Privacy Shield, particularly citing the wide surveillance that they saw as being enabled under the Foreign Intelligence Surveillance Act (FISA) Section 702, Executive Order 12333, and Presidential Decision Directive 28.[44] In particular, the Court noted that the United States would disregard Privacy Shield for "national security, public interest, or law enforcement requirements," thus violating the EU Charter of Fundamental Rights.[45] Additionally, because the rights of EU data subjects were not actionable in U.S. courts, aggrieved EU citizens did not have a means to challenge this data collection even under the Ombudsman envisioned under Privacy Shield; the Court deemed the regime to be ineffective given that it is not a tribunal, is managed solely by the executive branch, and as such cannot hold the intelligence community accountable.[46]

The CJEU answered a series of key questions related to transatlantic data governance in *Schrems II*. This includes the CJEU ruling that Facebook Ireland sending data on Europe-based users back to Facebook servers in the United States does fall under Article 45(2)(a) of GDPR.[47] It further underscored the level of

---

See Adequacy Decisions, EU COMM'N, https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en [https://perma.cc/JN53-BMUZ] (last visited Dec. 13, 2021).

[40] *See id.* (noting that the United States is not on the list of states that the EU has designated as "adequate").

[41] Case C-311/18, Data Prot. Comm'r v. Facebook Ir. (*Schrems II*), ECLI:EU:C:2020:559, ¶ 167 (July 16, 2020); Derek Scally, *Irish Watchdog's Case Against Facebook to Be Heard in Europe's Highest Court*, IRISH TIMES (July 9, 2019, 5:13 AM), https://www.irishtimes.com/business/technology/irish-watchdog-s-case-against-facebook-to-be-heard-in-europe-s-highest-court-1.3950568 [https://perma.cc/56B3-SFK6].

[42] Scally, *supra* note 41.

[43] *See* Ashley Gorski, *EU Court of Justice Grapples with U.S. Surveillance in Schrems II*, JUST SEC. (July 26, 2019), https://www.justsecurity.org/65069/eu-court-of-justice-grapples-with-u-s-surveillance-in-schrems-ii/ [https://perma.cc/T4B4-L4BF].

[44] *Schrems II a Summary—All You Need to Know*, *supra* note 33.

[45] *Data Prot. Comm'r*, ECLI:EU:C:2020:559, ¶ 167.

[46] *Id.* ¶¶ 181, 191.

[47] *Id.* ¶¶ 87–88 ("Indeed, by expressly requiring the Commission, when assessing the adequacy of the level of protection afforded by a third country, to take account, inter alia, of 'relevant legislation, both general and sectoral, including concerning public security, defence,

protection required by GDPR for these data flows, namely that "data subjects must be afforded appropriate safeguards, enforceable rights and effective legal remedies[,]"[48] and that such protection must be "essentially equivalent" to that guaranteed in the European Union.[49] Moreover, the CJEU took the additional step of calling the use of SCCs to transfer personal data into question.[50] In effect, it now places the onus on companies to verify the privacy regimes in place across the nations in which they do business, including the United States.[51] As such, even though the CJEU ruled that SCCs are still presumptively valid even if they do not apply to supervisory authorities such as the NSA, they still need to incorporate "effective mechanisms."[52]

In essence, then, the CJEU repeated the "essential equivalence" standard from *Schrems I* in *Schrems II*, including "with respect to how [a] government might access the data."[53] The failure of Privacy Shield to guarantee "'actionable' rights of redress before 'an independent and impartial court'" sealed the fate of the regime, according to the CJEU,[54] given that the right to effective judicial protection is guaranteed in Article 47 of the EU Charter.[55] Ironically, of course, EU governments need not meet this same high standard, given that "the Union's governing treaties state that 'national security remains the sole responsibility of each member state.'"[56] As such, it is left to each EU Member State how to balance "necessary and proportionate" limitations on the privacy rights of their citizens for national security purposes, even though such flexibility has not been accorded to non-EU nations by the CJEU by the *Schrems* cases.

---

national security and criminal law and the access of public authorities to personal data, as well as the implementation of such legislation.'").

[48] *Id.* ¶ 103.

[49] *Id.* ¶ 105.

[50] *Id.* (noting that consideration must be given to contractual clauses of the controller or processor in the EU and the recipient in the third country, as well as the "relevant aspects of the legal system" of countries that allow access for public authorities).

[51] *Id.*

[52] *Id.* ¶¶ 136, 146 (noting at paragraph 136 that "the mere fact that standard data protection clauses in a Commission decision adopted pursuant to Article 46(2)(c) of the GDPR, such as those in the annex to the SCC Decision, do not bind the authorities of third countries to which personal data may be transferred cannot affect the validity of that decision").

[53] *See* Kenneth Propp & Peter Swire, *After Schrems II: A Proposal to Meet the Individual Redress Challenge*, LAWFARE (Aug. 13, 2020, 7:28 PM), https://www.lawfareblog.com/after-schrems-ii-proposal-meet-individual-redress-challenge [https://perma.cc/NN2P-CFM8].

[54] *Id.*

[55] *Id.* (noting that the CJEU also determined that "there is a lack of 'proportionality' in the scale of U.S. intelligence activities. The Court did not dwell much on the issue of proportionality, other than expressing its disapproval of the scope of bulk personal data collection programs conducted under the authority of FISA Section 702 and EO 12333.").

[56] *Id.* (noting that many EU nations lack the same safeguards found to be deficient in the United States under *Schrems I* and *Schrems II*, and that this interpretation of EU nations having greater leeway under this regime is also up for review before the CJEU).

The implications of *Schrems II*, and the finding by the Court of "a fundamental right for a citizen of one nation to receive redress concerning surveillance by another nation," are potentially far-reaching indeed.[57] Predictably, the decision was derided in the U.S. national security community, with former NSA General Counsel Stewart Baker describing it as "a 'mix of judicial imperialism and Eurocentric hypocrisy.'"[58] Such a confrontational tone was balanced with a more conciliatory reaction from industry groups that pushed for a new round of negotiations to avoid undue economic damage to the transatlantic trade in data, which is valued in excess of $1.3 trillion annually.[59] The broader national security implications, along with the impact of *Schrems II* on emerging strategic technologies such as AI, are likewise manifold.[60] Not only are big tech platforms being impacted by the manifest "fragility" of the existing regime in which any European Commission finding of "adequacy" is "potentially suspect," but so are an increasing number of data-driven industries ranging from manufacturing to finance and health care.[61] *Schrems II* also highlights the extent to which GDPR's broad mandate, as interpreted by the CJEU, to extend "EU privacy rights and obligations" to all nations receiving data on EU persons is shaping not only transatlantic, but global data flows and governance structures.[62] This "nakedly extraterritorial assertion of EU jurisdiction," to use Swire's evocative phrasing, ignored both relevant jurisprudence from the European Court of Human Rights and EU Member State constitutional decisions.[63] In essence, then, the CJEU made GDPR the yardstick by which to measure what is "'necessary in a democratic society' to safeguard national security," with little in the way of nuance or flexibility owing to unique national circumstances or legal traditions.[64]

SCCs as well do not bind government agencies, so their use in this context does not necessarily remedy the core issue in play.[65] This will hit small firms particularly hard given the costs associated with this revised regime, such as putting the onus on SMEs in third-party nations like the United States to notify the EU of changes in

---

[57] *Id.* (noting that *Schrems II* mirrors a decision by the German Federal Constitutional Court about the rights of foreign persons in devising "proportionate surveillance regime[s]," but that even the German court did not go so far as to accord a right of judicial redress).

[58] *Id.*

[59] *Id.*

[60] *See* 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/9YGD-R3ZF].

[61] *Id.*

[62] *Id.* (noting that this fragility, and the differing views on the "adequacy" matter that have been put forward by the European Commission and European courts, are the result of "competing institutional incentives" and stakeholders).

[63] Propp & Swire, *supra* note 26.

[64] *Id.*

[65] Meltzer, *supra* note 60.

legislation that would prevent them from complying with their SCC obligations.[66] This degree of monitoring and data governance due diligence is simply beyond the means, and ability, of many small firms.[67]

Further, the CJEU's holding on SCCs are also potentially far more destabilizing than the demise of Safe Harbor. Among other things, the *Schrems* saga could further fuel the wave of data localization we are already witnessing around the world.[68] It could, in a worst-case scenario, also lead to a "self-imposed data isolation" as more nations, including but not limited to the United States, focus more on cybersecurity in their data governance regimes bringing them further out of alignment with GDPR.[69]

In sum, the end result of the *Schrems* saga, as Joshua Meltzer from the Brookings Institution has argued, is that "all GDPR mechanisms for transferring personal data to third countries are much more limited in scope, durability and stability."[70] Indeed, aside from the United States, there is an argument to be made that the greatest geo-political impacts of *Schrems II* may well be on authoritarian regimes such as China and Russia.[71] Nations practicing a robust interpretation of cyber sovereignty, for example, will be hard pressed to show that the protections that they offer are "essentially equivalent" to those in the EU, or to ensure "that the GDPR is fully enforced with all due diligence."[72] The EU Data Protection Supervisor Wojciech Wiewiórowski, for example, is on the record as stating that the United States is "much closer" to the EU with regards to data governance than the likes of China.[73] Even nations with well-developed commitments to the rule of law, such as the United Kingdom post-Brexit, may also run afoul of this ruling given the "extensive surveillance for national security purposes" that is undertaken by the likes of the GCHQ.[74] As such, the impacts of *Schrems* are likely not just transatlantic but global, potentially exacerbating digital divides over data governance.

III. BRIDGING THE DIVIDE ON PRIVACY RIGHTS AND INTERNET GOVERNANCE

Looking ahead, there are four main options to resolve these concerns, each involving uncomfortable consequences for Europeans, Americans, and citizens around the world. First, the European Commission could negotiate a new bilateral agreement with the United States, a Privacy Shield 2.0 that would address ongoing concerns and avoid disruptions to global supply chains generally, and social networking, e-commerce, and cloud service firms in particular. This option holds the potential

---

[66] *Id.*
[67] *Id.*
[68] *Id.*
[69] *Id.*
[70] *Id.*
[71] Propp & Swire, *supra* note 26.
[72] *Id.* (internal quotations omitted).
[73] *Id.* (internal quotations omitted).
[74] *Id.*

to more directly address European concerns by gaining further concessions on the part of the U.S. government on bulk data collection and EU standing to access, correct, and delete personal data. But it also calls into question the status of other EU data privacy agreements, potentially leading to further renegotiations and business disruptions.[75]

It is not atypical for U.S. and EU negotiators to take several attempts to reach a durable agreement on issues of data governance, as seen in previous sagas involving the exchange of airline passenger data and terrorist financing.[76] There is also precedent for the U.S. government taking a more flexible approach to European privacy demands, as seen in a 2016 "umbrella" agreement that required the United States to amend the Privacy Act "to grant foreign persons a right to sue equivalent to that enjoyed by U.S. persons." This step, as Peter Swire and Kenneth Propp note, has not "resulted in burdensome litigation by Europeans in U.S. courts."[77]

A durable replacement to Privacy Shield will require both: (1) a "credible fact-finding inquiry into classified surveillance activities in order to ensure protection of the individual's rights," and (2) "the possibility of appeal to an independent judicial body that can remedy any violation of rights should it occur."[78] The former may be accomplished by enlisting already existing privacy and civil liberties officers (PCLOs) spread across the intelligence community, given that they already have access to the required databases and enjoy established reporting channels along with adequate staff support.[79] Yet the European Commission and the CJEU would likely push back against this notion, given that these officers remain ultimately beholden to the executive branch, and thus cannot act as an effective independent check against U.S. intelligence bulk data collection.[80] The second needed reform may be accomplished through an appeal mechanism after the fact-finding phase of an investigation is completed to the Foreign Intelligence Surveillance Court, given that these judges fall under Article III of the U.S. Constitution and are also guaranteed life tenure.[81] Additional reforms, including those relating to standing, are also important given the higher burden placed

---

[75] *See How Will the "Safe Harbor" Arrangement for Personal Data Transfers to the US Work?*, EUR. COMM'N, https://web.archive.org/web/20151109193926/http://ec.europa.eu:80/justice/policies/privacy/thridcountries/adequacy-faq1_en.htm [https://perma.cc/S3RE-M5DX] (last visited Dec. 13, 2021).

[76] Propp & Swire, *After Schrems II*, *supra* note 53 (noting that "[i]n one instance, the Court rejected an agreement negotiated between the U.S. Department of Homeland Security and the European Commission on the transfer of airline passenger name records for flight security purposes; however, a revised version has proven durable for the past eight years. Similarly, the U.S. Treasury Department required two tries before concluding a 2010 agreement on the Terrorist Finance Tracking Program that provides U.S. authorities with a steady flow of international bank transfer data from EU territory").

[77] *Id.*

[78] *Id.*

[79] *Id.* (noting that an alternative arrangement may be to make use of the Privacy and Civil Liberties Oversight Board, but that the authority of this board is limited especially pertaining to individual complaints, and that this authority is limited to anti-terrorism).

[80] *Id.*

[81] *Id.*

on plaintiffs challenging intelligence practices in the United States as compared to Europe.[82] Swire and Propp suggest a modified version of the U.S. Freedom of Information Act (FOIA) to help bridge this gap given that this regime permits individuals to request documents without first demonstrating an injury.[83] Their suggestion leverages U.S. laws that permit individuals "to test compliance with acts that an agency is required to perform," by requiring that agencies tasked with assessing surveillance activities be required to also undertake fact-finding investigations that could be appealable to an independent federal court—and ultimately the U.S. Supreme Court.[84] This set of proposals could help raise the shields once again thereby permitting the relatively free flow of data across the Atlantic, leading to a durable Privacy Shield 2.0.

Second, the SCCs' regime could be updated (they still refer to the EU's Data Protection Directive and not GDPR, for example), which would be a useful next step given that, according to Hogan Lovells' Eduardo Ustartan: "The Privacy Shield has always been surrounded by a degree of uncertainty, but the SCCs have been around for nearly 20 years, so they are the bedrock of lawful data transfers."[85] The United States would be joined in this effort by the U.K., given that these legal tools are "regarded as the most obvious fix to the loss of data protection adequacy by the U.K." post-Brexit.[86] In November 2020, the European Commission released its draft Decision on Standard Contractual Clauses.[87] A final draft was not available at the time of publication, but the U.S. government did submit comments to the Commission prior to the release of the draft, which came just two months after the Swiss-U.S. Privacy Shield Framework was invalidated by the Federal Data Protection and Information Commissioner of Switzerland.[88]

Third, firms could rely on intragroup data transfers within multinationals, but such binding corporate rules (BCRs) and governance structures are time intensive and complex to create, and at any rate would be of little use to small and medium-sized businesses currently relying on Privacy Shield.[89] Further, they run into the same issues as SCCs discussed above, even as—over the long term—they may be more cost effective.[90]

---

[82] *Id.* ("Under EU law, an individual such as Max Schrems can bring a successful case without proving that he was ever under surveillance by the U.S. government.").

[83] *Id.*

[84] *Id.*

[85] Baker, *supra* note 11.

[86] *Id.*

[87] *Privacy Shield News & Events*, PRIV. SHIELD FRAMEWORK, https://www.privacyshield.gov/NewsEvents [https://perma.cc/JQ7S-MCHZ] (last visited Dec. 13, 2021).

[88] *Id.*

[89] Baker, *supra* note 11.

[90] *See* Romain Perray, *Schrems II: What Does the CJEU's Decision Mean for Transfers from the EEA to the US?*, 10 NAT'L L. REV. (July 20, 2020), https://www.natlawreview.com/article/schrems-ii-what-does-cjeu-s-decision-mean-transfers-eea-to-us [https://perma.cc/86L2-A4ZN].

Fourth, there is the much more substantial task of modernizing international privacy law to take into account data governance trends, and to create verification and enforcement mechanisms. For example, even though existing international human rights law references the right to privacy, such as in Articles 3 and 19 of the UN Declaration of Human Rights,[91] and Articles 17 and 19 of the International Covenant on Civil and Political Rights (ICCPR),[92] neither treaty framework has been updated with cyberspace in mind.[93] Yet there has been some progress, such as a 2013 UN General Assembly Resolution on the right to privacy in the digital age,[94] and a 2015 statement by the G20 that endorsed the concept of privacy, "including in the context of digital communications."[95] Given the focus by the Biden administration on finding multilateral solutions to pressing global challenges, there may well be an opportunity to build from this momentum, much of which stalled during the Trump administration.[96] "Go[ing] big," in this way, on global data governance by balancing national security concerns with privacy protections is certainly a heavy lift, but at the same time such a robust, durable international regime would avoid the bilateral band-aids like Safe Harbor and Privacy Shield that have bedeviled practitioners and policymakers alike.[97] Such an agreement would be unlikely to be agreeable to democratic and authoritarian societies alike, but even getting democracies on closer to the same page would be a huge step forward and a useful foundation from which to tackle related issues of cybersecurity, AI governance, and misinformation. Options for forums to utilize include the World Trade Organization along with the Organization for Economic Cooperation and Development, which successfully developed data governance principles in 1980.[98]

If none of these options are adopted, then costs will mount, both financial and, perhaps surprisingly, personal.[99] Beyond governmental spying—an issue extending

---

[91] G.A. Res. 217 (III) A, Universal Declaration of Human Rights (Dec. 10, 1948).

[92] International Covenant on Civil and Political Rights, *opened for signature* Dec. 19, 1966, 999 U.N.T.S. 171 (entered into force Mar. 23, 1976).

[93] *See* Scott J. Shackelford, *Should Cybersecurity Be a Human Right? Exploring the 'Shared Responsibility' of Cyber Peace*, 55 STAN. J. INT'L L. 155, 167–68 (2019).

[94] G.A. Res. 68/167, The Right to Privacy in the Digital Age (Dec. 18, 2013), https://www.unhcr.org/en-us/excom/bgares/54534c619/resolution-adopted-general-assembly-18-december-2013-[on-report-third-committee.html [https://perma.cc/PQZ4-557U].

[95] EUR. COUNCIL, G20 LEADERS' COMMUNIQUÉ, ANTALYA SUMMIT, 15–16 November, at 6 (2015), https://www.consilium.europa.eu/media/23729/g20-antalya-leaders-summit-communique.pdf [https://perma.cc/76LS-DWCA] (last visited Dec. 13, 2021).

[96] *See, e.g.*, Brian Hengesbaugh, *Why the Biden Administration Should 'Go Big' on Global Data Transfers Solution*, IAPP (Feb. 25, 2021), https://iapp.org/news/a/why-the-biden-administration-should-go-big-to-establish-a-long-term-solution-for-global-personal-data-transfers/ [https://perma.cc/E5DH-9JET].

[97] *See id.*; Meltzer, *supra* note 60 (noting that "[s]uch an outcome could be deemed an international agreement under GDPR article 45(2)(c) that would support an adequacy finding and by extension, short up access to SCC and BCRs").

[98] *Id.*

[99] *See* Jonathan Stray, *FAQ: What You Need to Know About the NSA's Surveillance*

beyond the United States to include a number of EU Member States including France, Germany, Italy, Sweden, and the Netherlands[100]—there is also the risk that the lack of a new formal agreement could embolden data black markets as well as exacerbate both cyber risk and transatlantic tensions.[101] Such an outcome could also hobble law enforcement efforts due to nations citing privacy concerns as reasons not to fulfill their obligations under Mutual Legal Assistance Treaties, making it more difficult to find, extradite, and prosecute cybercriminals.[102] The end result would be less transatlantic cybersecurity cooperation, further widening the divide on both security and privacy at a time of already heightened tensions.

The *Schrems* saga demonstrates the extent to which transatlantic privacy rights are diverging,[103] at a time of relative global convergence with more than 100 nations now having omnibus privacy laws reminiscent—if not as robust—of GDPR already enacted.[104] As Professor James Whitman has argued, and as *Schrems* demonstrates, "[i]n the law of privacy . . . the contrast between Europe and the United States is stark and is growing starker."[105] Aside from data protection, this trend may be seen in differing conceptions over what counts as "news" and the "public interest," as well as who "public figures" are and what privacy rights they should enjoy.[106] Part of the reason for this divide is that, despite the United States' and Europe's shared fascination with celebrity, differences in legal cultures permeate transatlantic privacy law. For example, some have criticized European jurists as "elitist" given their stance on the

---

Programs, PROPUBLICA (Aug. 5, 2013, 3:20 PM), http://www.propublica.org/article/nsa-data-collection-faq [https://perma.cc/N7RM-MFTC].

[100] *See* Russell, *supra* note 14. For more on the broadening French approach to surveillance, see Laura Smith-Spark, Jim Bittermann, & Saskya Vandoorne, *Report: France Runs Surveillance Program like PRISM*, CNN (July 5, 2013, 11:38 AM), http://www.cnn.com/2013/07/05/world/europe/france-surveillance-claims/ [https://perma.cc/7RWW-2J2P].

[101] The cybersecurity angle could be especially problematic given that it could require the replication of data centers, some of which may not be as secure as their U.S. counterparts. *See, e.g.*, David Linthicum, *IT Pros Agree: Security Is Better in the Cloud*, INFO. WORLD (Mar. 31, 2017, 3:00 AM), https://www.infoworld.com/article/3185757/it-pros-agree-security-is-better-in-the-cloud.html [https://perma.cc/X9ZG-SDZX].

[102] *See* Katie Bo Williams, *Safe Harbor Ruling May Hamper US Law Enforcement Overseas*, THE HILL (Oct. 11, 2015, 7:30 AM), http://thehill.com/policy/cybersecurity/256575-safe-harbor-ruling-may-hamper-us-law-enforcement-overseas [https://perma.cc/KB83-UT7W].

[103] *See generally* Daniel J. Solove, *Conceptualizing Privacy*, 90 CALIF. L. REV. 1087 (2002) (advocating a pragmatic approach to conceptualizing privacy); Scott J. Shackelford, *Fragile Merchandise: A Comparative Analysis of the Privacy Rights for Public Figures*, 49 AM. BUS. L.J. 125, 132 (2012) (discussing varying privacy rights in the context of public figures).

[104] *See* THE STATE OF DATA PROTECTION RULES AROUND THE WORLD: A BRIEFING FOR CONSUMER ORGANIZATIONS, CONSUMERS INT'L 3 (2018), https://www.consumersinternational.org/media/155133/gdpr-briefing.pdf [https://perma.cc/8Q7N-YJMA].

[105] James Q. Whitman, *The Neo-Romantic Turn*, *in* COMPARATIVE LEGAL STUDIES: TRADITIONS AND TRANSITIONS 312, 330 (Pierre Legrand & Robert Munday eds., 2003).

[106] *See generally* Shackelford, *supra* note 103, at 130.

public's right to know.[107] This may be seen in cases like *Von Hannover v. Germany*, in which Princess Caroline of Monaco recovered for breach of privacy against German publishers, which would likely have had a very different outcome in a U.S. court given First Amendment preferences for freedom of expression over individual privacy rights.[108]

As with privacy, the *Schrems* saga also highlights contrasting EU and U.S. views on Internet governance generally, particularly with regard to cyber sovereignty.[109] The EU, for example, has sought to keep data on EU citizens within its territorial borders. Similarly, GDPR goes even further, asserting the EU's ability to regulate all data related to EU persons, regardless of its storage location or place of origination.[110] Following from other EU precedent, such as the right to be forgotten and the EU antitrust cases,[111] the EU is, in some ways, pushing a view of privacy that is quickly becoming the default global standard. Various nations, including some with already relatively strong privacy regimes such as Canada, Australia, and Japan, are in the process of updating their laws to comply with GDPR and ease data transfers, as was discussed in Part II.[112] More multinational firms, including U.S. behemoths like the pharmaceutical giant Eli Lilly, are complying with GDPR for their global operations.[113]

At a higher level, as was referenced in Part II, there are positive network effects to encouraging robust information sharing. Indeed, it has been described as a core confidence building measure (CBM), according to Professor Deborah Housen-Couriel, "by the OSCE,[114] the UN's 2015 GGE,[115] the 2018 Paris Call for Trust and

---

[107] *See* Lawrence M. Friedman & Nina-Louisa Arold, *Cannibal Rights: A Note on the Modern Law of Privacy*, 4 NW. INTERDISC. L. REV. 235, 242 (2011).

[108] Von Hannover v. Germany, 2004-VI Eur. Ct. H.R. 41.

[109] *See* Rita Heimes, *Top 10 Operational Impacts of the GDPR: Part 9—Codes of Conduct and Certifications*, PRIVACY ADVISOR (Feb. 24, 2016), https://iapp.org/news/a/top-10-operational-impacts-of-the-gdpr-part-9-codes-of-conduct-and-certifications/ [https://perma.cc/68DU-L972].

[110] *See id.*

[111] *See, e.g.*, Farhod Manjoo, *'Right to Be Forgotten' Online Could Spread*, N.Y. TIMES (Aug. 5, 2015), http://www.nytimes.com/2015/08/06/technology/personaltech/right-to-be-forgotten-online-is-poised-to-spread.html?_r=0 [https://perma.cc/YTS5-MEYY].

[112] Laurent Barthelemy, *One Year On, EU's GDPR Sets Global Standard for Data Protection*, PHYS.ORG (May 24, 2019), https://phys.org/news/2019-05-year-eu-gdpr-global-standard.html [https://perma.cc/NM9F-VMAR].

[113] *See* Oksana Sokolovsky, *Is GDPR The New Standard?*, FORBES (July 16, 2018, 8:00 AM), https://www.forbes.com/sites/forbesnycouncil/2018/07/16/is-gdpr-the-new-standard/#226a3e0b3313 [https://perma.cc/AXV4-NL6M].

[114] *OSCE Expands Its List of Confidence-Building Measures for Cyberspace: Common Ground on Critical Infrastructure Protection*, NATO COOP. CYBER DEF. CTR. EXCELLENCE (Mar. 10, 2016), https://ccdcoe.org/incyder-articles/osce-expands-its-list-of-confidence-building-measures-for-cyberspace-common-ground-on-critical-infrastructure-protection/ [https://perma.cc/7R22-QB27].

[115] U.N. Gen. Assembly, Rep. of the Group of Governmental Experts on Developments

Security in Cyberspace[116] and other organizations."[117] Robust information sharing is a vital component in the building of institutions to manage various knowledge commons, and more generally to aid coordination, and promote trust,[118] which as noted by Nobel Laureate Elinor Ostrom, "is the most important resource."[119] One mechanism to conceptualize this type of approach to networked, distributed data governance is polycentric governance.[120] As noted by Professor Dan Cole:

> Decades of work conducted by researchers associated with the Vincent and Elinor Ostrom Workshop in Political Theory and Policy Analysis at Indiana University have emphasized two chief advantages of polycentric approaches over monocentric ones: they provide more opportunities for experimentation and learning to improve policies over time, and they increase communications and interactions—formal and informal, bilateral and multilateral—among parties to help build the mutual trust needed for increased cooperation.[121]

Polycentricity is no panacea given the extent to which it can lead to gridlock and other systemic failures,[122] but it can be a pragmatic path forward that the Biden administration in particular could pursue given the rich array of cyber norm building efforts underway through the UN, EU, and otherwise.[123]

---

in the Field of Information and Telecommunications in the Context of International Security, U.N. Doc. A/70/174 (July 22, 2015), https://documents-dds-ny.un.org/doc/UNDOC/GEN/N15/228/35/PDF/N1522835.pdf?OpenElement [https://perma.cc/ZZD8-886X].

[116] *See The Nine Principles*, PARIS CALL, https://pariscall.international/en/principles [https://perma.cc/W6J6-UF59].

[117] Deborah Housen-Couriel, *Information Sharing as a Critical Best Practice for the Sustainability of Cyber Peace*, *in* CYBER PEACE: CHARTING A PATH TOWARD A SUSTAINABLE, STABLE, AND SECURE CYBERSPACE (Scott Shackelford, Frederick Douzet & Chris Ankersen eds., Cambridge University Press, 2021).

[118] *See, e.g.*, George V. Hulme, *Tackling Cybersecurity Threat Information Sharing Challenges*, CSO (Jan. 17, 2017, 6:29 AM), https://www.csoonline.com/article/3157540/security/tackling-cybersecurity-threat-information-sharing-challenges.html [https://perma.cc/LM7R-M2EK].

[119] *Interview with Nobel Laureate Elinor Ostrom*, ESCOTET FOUND., http://escotet.org/2010/11/interview-with-nobel-laureate-elinor-ostrom/ [https://perma.cc/9CB5-X5P5] (last visited Dec. 13, 2021).

[120] Paul D. Aligica & Vlad Tarko, *Polycentricity: From Polanyi to Ostrom, and Beyond*, 25 GOVERNANCE 237, 245 (2012).

[121] Daniel H. Cole, *Advantages of a Polycentric Approach to Climate Change Policy*, 5 NATURE CLIMATE CHANGE 114, 114 (2015).

[122] *See* L. Caldwell, *The Geopolitics of Environmental Policy: Transnational Modification of National Sovereignty*, 59 REV. JUR. U.P.R. 693, 700 (1990).

[123] *See, e.g.*, Josh Gold, *The First Ever Global Meeting on Cyber Norms Holds Promise,*

The ability of cyber powers to reshape the global regulatory environment is an important, if often underappreciated, element of Internet governance.[124] Is cyberspace, then, a "global networked commons,"[125] as maintained by former Secretary of State Hillary Clinton, an extension of national territory, as France and the CJEU seems to maintain, or something in between: an "imperfect" or pseudo commons as argued by Professor Joseph Nye, Jr.?[126] Fissures seem to be deepening with concerns over the "Splinternet," or what had previously been called "Internet Balkanization" or a "New Digital Divide" again reaching a fever pitch in the wake of the race to dominate 5G globally.[127] Indeed, there is some evidence that the Trump administration favored the historically European perspective on Internet governance as seen by the fact that neither the 2018 U.S. National Cyber Strategies does not, nor did the 2017 Trump Administration cybersecurity executive order, refer to cyberspace as a global commons.[128] Whether a system of Internet governance practicing John Herz's notion of "neoterritorality," whereby sovereign states recognize their common interests—such as the public goods of privacy and cybersecurity—while also mutually respecting one another's independence in the face of more decisions like *Schrems* remains to be seen.

CONCLUSION

Even if successful, negotiating Privacy Shield 2.0 may well just be another temporary band-aid for a widening transatlantic data governance wound. What is needed is a rekindled multi-stakeholder dialogue to help clarify global privacy

---

But Broader Challenges Remain, COUNCIL ON FOREIGN REL. (Sept. 30, 2019, 12:06 PM), https://www.cfr.org/blog/first-global-meeting-cyber-norms [https://perma.cc/Y5WJ-8RRG].

[124] For more on this topic, see Chapters 1 and 2 of SCOTT J. SHACKELFORD, MANAGING CYBER ATTACKS IN INTERNATIONAL LAW, BUSINESS, AND RELATIONS: IN SEARCH OF CYBER PEACE (2014).

[125] Hillary Rodham Clinton, U.S. Sec'y of State, Remarks on Internet Freedom (Jan. 21, 2010), https://2009-2017.state.gov/secretary/20092013clinton/rm/2010/01/135519.htm [https://perma.cc/WQ93-H3K4] (emphasizing the need for behavioral norms and respect among states to encourage the free flow of information and protect against cyber attacks).

[126] JOSEPH S. NYE, JR., CYBER POWER, HARV. KENNEDY SCH. 15 (May 2010) (referring to cyberspace as an "imperfect commons").

[127] *See, e.g.*, Scott J. Shackelford & Amanda Craig, *Beyond the New 'Digital Divide': Analyzing the Evolving Role of Governments in Internet Governance and Enhancing Cybersecurity*, 50 STAN. J. INT'L L. 119 (2014).

[128] *See* NATIONAL CYBER STRATEGY OF THE UNITED STATES OF AMERICA (2018), https://trumpwhitehouse.archives.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf [https://perma.cc/23CM-CGKG]; U.S. DEP'T OF DEFENSE, THE DOD CYBER STRATEGY (2015), https://www.hsdl.org/?view&did=764848 [https://perma.cc/3Y29-3AY2]; Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure, Exec. Order No. 13,800, 82 Fed. Reg. 22,391 (May 11, 2017).

standards and flesh out the right to privacy mentioned in both the Universal Declaration of Human Rights and ICCPR. Elements of the private sector, including Apple, Microsoft, and Google, have been calling for global privacy norms for years.[129] There is evidence that policymakers are also coming to this conclusion with growing support for an additional protocol to ICCPR,[130] and even the United States is moving away from a sector-specific approach to privacy protection and toward a GDPR-type privacy regime. Such efforts could help narrow the widening transatlantic rift and build a common vision of privacy rights in the digital age across democracies, perhaps eliminating the need for *Schrems III* in the process.

---

[129] *See* Liam Tung, *GDPR, USA? Microsoft Says US Should Match the EU's Digital Privacy Law*, ZDNET (Sept. 26, 2021), https://www.zdnet.com/article/gdpr-usa-microsoft-says-us-should-match-the-eus-digital-privacy-law/ [https://perma.cc/M4X9-CE4E]; *Google Backs Calls for Global Privacy Standards*, IT PRO PORTAL (Oct. 28, 2010), https://www.itproportal.com/2010/10/28/google-backs-calls-global-privacy-standards/ [https://perma.cc/8KA4-ETVD] (following on the heels of the backlash against Google's Street View site).

[130] This gathering included "a diverse selection of privacy and data protection officials from across the world . . . including Japan, New Zealand, France, Slovenia, Uruguay, Belgium, Ireland, Finland, Spain, Australia, Germany, Burkina Faso, Canada, the United States, and the United Kingdom." Ryan Gallagher, *After Snowden Leaks, Countries Want Digital Privacy Enshrined in Human Rights Treaty*, SLATE (Sept. 26, 2013, 2:16 PM), http://www.slate.com/blogs/future_tense/2013/09/26/article_17_surveillance_update_countries_want_digital_privacy_in_the_iccpr.html [https://perma.cc/RR3R-PN5M].