Risk and Rights in Transatlantic Data Transfers:

EU Privacy Law, U.S. Surveillance, and the Search for Common Ground

(forthcoming, Connecticut Law Review)

Ira Rubinstein[*] & Peter Margulies[**]

INTRODUCTION

After the recent decision of the Court of Justice of the European Union (CJEU) in *Data Protection Commissioner v. Facebook Ireland, Ltd. and Maximilian Schrems* (*Schrems II*),[1] the gap between European Union (EU) privacy bodies and the United States seems wider than ever. *Schrems II* invalidated the Privacy Shield agreement between the European Commission and the United States on transatlantic data transfers.[2] The *Schrems II* court's rationale tracked the reasoning in *Schrems I*, which had struck down Privacy Shield's predecessor, the Safe Harbor Agreement.[3] That gap reflects the persistent mistrust that the EU experienced in the wake of Edward Snowden's 2013 revelations about the breadth of U.S. surveillance.[4]

This gap imperils transatlantic data transfers that are necessary for modern commerce. While the CJEU's *Quadrature du Net and Others*[5] decision in October 2020 displayed a measure of deference to the national security concerns that also drive U.S. policy, finding common ground between the CJEU and the United States has been an elusive endeavor. This Article aims to fill the gap with a hybrid model that combines a risk-based approach to data transfers with substantive and institutional checks on U.S. surveillance.

---

[*] Senior Fellow, Information Law Institute, New York University School of Law. B.A., Clark University; J.D., Yale Law School.

[**] Professor of Law, Roger Williams University School of Law. B.A., Colgate University; J.D., Columbia Law School. We thank Ron Lee and Thomas Streinz for comments on a previous draft; we previously presented a version of this paper at an informal workshop sponsored by the staff of the U.S. Privacy and Civil Liberties Oversight Board (PCLOB).

[1] Case No. C-311/18 (16 July 2020).

[2] *See* Commission Implementing Decision (EU) No. 2016/1250 of 12 July 2016, 2016 O.J. (L 207) 1.

[3] For an account of the Safe Harbor principles, *see* Paul M. Schwartz, *Global Data Privacy: The EU Way*, 94 N.Y.U. L. Rev. 771, 795-98 (2019).

[4] Timothy Edgar, *Beyond Snowden: Privacy, Mass Surveillance, and the Struggle to Reform the NSA* (2017); Kenneth Propp & Peter Swire, *Geopolitical Implications of the European Court's Schrems II Decision*, Lawfare (July 17, 2020), https://www.lawfareblog.com/geopolitical-implications-european-courts-schrems-ii-decision (analyzing *Schrems II* in part as continued response to Snowden's disclosures about reach of U.S. surveillance).

[5] Case No. C-511/18, Ct. Justice Eur. Union (6 Oct. 2020).

As the CJEU explained in *Schrems II*, part of the problem is the mismatch of U.S. surveillance with EU stress on tailoring intrusive measures and providing independent recourse for persons with privacy-based complaints. According to *Schrems II*, U.S. surveillance does not meet the EU's test of necessity and proportionality. This critique of U.S. law has some merit, particularly given the breadth of surveillance permitted under the "foreign affairs" prong of § 702 of the U.S. Foreign Intelligence Surveillance Act (FISA).[6] Nevertheless, the CJEU's analysis lacks nuance. In some respects, U.S. law actually protects privacy from government intrusion more effectively than the legal systems of many EU member states.[7] Moreover, the U.S. Foreign Intelligence Surveillance Court (FISC) has more power than the CJEU acknowledges to review § 702 surveillance, although not quite enough to address all of the CJEU's concerns.[8] Snowden's disclosures have heightened the CJEU's distrust of U.S. surveillance policy, leading it to discount U.S. checks and balances.

The United States has not always helped its cause post-Snowden. In an important step forward, President Barack Obama's Presidential Policy Directive No. 28 (PPD-28) limited U.S. surveillance and required U.S. respect for the privacy of all persons around the world.[9] However, in *Schrems II* the CJEU cautioned that PPD-28 did not provide either an independent check on U.S. surveillance or "sufficiently … precise" limits on surveillance's scope.[10] For that reason, the CJEU held that PPD-28 did not cure Privacy Shield's central problem: that U.S. privacy guarantees were not adequate when compared with EU law.

In addition, when the United States has entered into data transfer agreements with EU states, the privacy work-arounds in those agreements seem more like half-hearted improvisations than permanent solutions. For example, in *Schrems II*, the CJEU considered the recourse for privacy complainants agreed to by the European Commission and the United States in Privacy Shield, the data transfer pact that succeeded Safe Harbor, an earlier pact found wanting on privacy grounds by the CJEU in the first *Schrems* decision (*Schrems I*).[11] Under Privacy Shield, a U.S State Department official served as an ombudsperson fielding EU persons' privacy grievances. According to the CJEU, the ombudsperson lacked sufficient independence. This finding contributed to Privacy Shield's invalidation in *Schrems II*.

Post-*Schrems II* EU developments have had cross-cutting effects on the prospects for future transatlantic data transfer agreements. The CJEU's decision in *Quadrature du Net* has provided a sliver of daylight for such agreements, by acknowledging that states' national security interests may justify broader government access to communications. *Quadrature du Net*

---

[6] 50 U.S.C. § 1801(e)(2)(B).

[7] For example, the U.S. Supreme Court's decision in Carpenter v. United States, 138 S. Ct. 2206 (2018), holding that law enforcement officers must obtain a warrant for cell-site location information, compares favorably with most EU member-state case law on new surveillance technology.

[8] *See infra* notes __-__ and accompanying text.

[9] *See* Presidential Policy Directive/PPD-28 (Jan. 17, 2014) [hereinafter PPD-28].

[10] *Schrems II*, ¶¶ 183-84.

[11] Schrems v. Data Protection Comm'r, Case No. 362/14 (6 October 2015).

recognized that privacy rights—while vital—are not absolute. However, the CJEU has warned that national security derogations from privacy rights must comply with the constraints of necessity, proportionality, and independent review.

In addition, *Schrems II* opened the door for companies transferring data in-house or with contractual partners to derogate under Article 49 of the GDPR.[12] Article 49 derogations do not fit every activity subject to an adequacy finding. For example, they probably would not work for Facebook users' personal data. However, this law review article argues that the *Schrems II* court's mention of Article 49 makes such derogations an option worth exploring, particularly for U.S. companies sending data about their EU employees to the United States.

Unfortunately, another important EU body, the European Data Protection Board (EDPB), has taken a de facto absolutist stance that reads *Schrems II* too broadly. The EDPB's "Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data" (the "Recommendations") require, among other things, technical measures such as encryption. Under these guidelines, encryption must preclude access to transferred data by U.S. and other third country cloud services providers as they seek to perform various operations on the data transmitting the data.

The EDPB's de facto absolutist approach pits privacy against data security. The Board's steep encryption requirements bar cloud services from checking data transfers for malware or other cyber intrusions, imperiling the security of all data users. This counterintuitive result exalts privacy rights as a matter of formal law, but sacrifices users' actual privacy in practice. In a world of persistent cyber threats, the EDPB's guidance on this score seems particularly shortsighted.

To counter the de facto absolutist approach, this paper outlines a hybrid strategy that pairs a risk-based approach with renewed attention to institutional and substantive checks on surveillance. To implement a risk-based approach, the paper looks to U.S. export control law. United States law imposes a graduated system of controls on U.S. exports of technology and other goods, depending on conditions in the receiving state. This graduated approach may also allow for more efficient safeguards on data transfer.

In the institutional realm, this Article proposes a new safeguard in U.S. law: an Algorithmic Rights Court (ARC) that will field EU persons' privacy complaints. The ARC would be staffed by life-tenured federal judges and aided by a full-time public advocate who would push back on government positions. It would provide gold-standard independent review. As a fallback position if establishing the ARC is too heavy a political lift, the Article suggests that the United States could delegate review of EU persons' privacy complaints to either the FISC or an independent multimember executive branch agency such as the Federal Trade Commission (FTC) or the Privacy and Civil Liberties Oversight Board (PCLOB), whose members have "for-cause" protections against dismissal.

[12] *Schrems II*, ¶ 202.

As a substantive check, Congress should enact a statutory presumption against collection of the communications of foreign employees of U.S. firms located abroad. Since much transatlantic data transfer concerns such foreign employees, a statutory presumption will install legal protections against unchecked surveillance of such persons. Furthermore, Congress should revise the "foreign affairs" prong of FISA § 702, to limit surveillance to actions of foreign officials, including receipt of bribes that skew international commerce.

This Article is in six Parts. Part I describes U.S. foreign surveillance, concluding that post-Snowden reforms have been significant, if not yet sufficient to blunt the CJEU's critique. Part II discusses the CJEU's jurisprudence, including both *Schrems II* and its more deferential follow-up, *Quadrature du Net*. This Part also explores the potential of Article 49 derogations. Part III unpacks the puzzling guidance of the EDPB, which claims to offer a roadmap for data transfers, but actually supplies a road to nowhere with no workable options. As a response to the EDPB's de facto absolute prohibition on data transfers, the remainder of the Article proposes a hybrid model. Part IV suggests a graduated risk assessment based on U.S. export controls. Part V outlines bilateral agreements between EU Member States and third countries. Part VI proposes substantive and institutional checks on U.S. surveillance to address *Schrems II*'s requirements.

This Article's hybrid of a graduated risk assessment with new institutional and substantive checks on surveillance will not satisfy everyone. Adherents of de facto absolutism will continue to be wary. In addition, some champions of national security may argue that the approach taken in this paper concedes too much. The hybrid model outlined here rejects the binary perspective of these contending camps. Unlike its competitors, the hybrid model will preserve privacy and security while ensuring the continued viability of transatlantic data transfers.

I. U.S. SURVEILLANCE EXPLAINED

To understand *Schrems II* and the prospects for EU-U.S. data transfers that comply with EU law, it is necessary to understand the scope of U.S. foreign surveillance law. As we shall see, the CJEU in *Schrems II* repeatedly cited U.S. surveillance law as lacking substantive, procedural, and institutional constraints. In fact, the *Schrems II* court was in part correct in large part, although the court unduly discounted checks that U.S. officials established in the wake of Edward Snowden's revelations. Understanding the CJEU's analysis requires a deeper look at U.S. foreign surveillance, centering on § 702 of FISA[13] and EO 12333.[14]

A. Surveying the Landscape of U.S. Legal Authorities

Section 702 materially expanded the coverage of the original 1978 FISA statute.[15] Under the 1978 statute, the government obtains an *ex parte* order from the Foreign Intelligence

[13] Pub. L. No. 110-261, 122 Stat. 2436 (2008) (codified as amended at 50 U.S.C. § 1881a (2020)).

[14] Exec. Order No. 12,333, 46 Fed. Reg. 59,941–42 (Dec. 4, 1981).

[15] 50 U.S.C. § 1804(a)(3)(2020).

Surveillance Court (FISC) authorizing surveillance.[16] The Chief Justice of the U.S. Supreme Court appoints judges to the FISC on a rotating basis from a pool comprised of life-tenured federal jurists.[17] To issue an order, the FISC has to find probable cause that a target was an agent of a foreign power. Courts have held that this standard is consistent with the Fourth Amendment to the U.S. Constitution, which bars "unreasonable searches and seizures."[18] In contrast, although the FISC also reviews surveillance under § 702, both substantive scope and procedural features of the newer statute give the government broader discretion.

Congress enacted § 702 in 2008 to help meet the challenge of terrorism revealed in the attacks of September 11, 2001.[19] Section 702 codified parts of the Terrorist Surveillance Program (TSP), established secretly outside of the FISA framework by President George W. Bush in 2001.[20] Section 702 has both a locational and a substantive component. Under § 702,

---

[16] *Ex parte* proceedings entail a presentation to the court by only one side—here, the government. As European courts have also recognized, this ex parte character of surveillance requests is often necessary, since tipping off a target about the possibility of surveillance would enable the target to "adapt" her behavior to hinder that targeting. *See* Big Brother Watch and Others v. United Kingdom, Eur. Ct. Hum. Rts., App. No. 58170/13, ¶ 340 (13 Sept. 2018); Kennedy v. United Kingdom, App. No. 26839/05, 52 Eur. H.R. Rep. 207, 253–54 (2010); *see also* Weber and Saravia v. Germany, 2006-XI Eur. Ct. H.R. 309 (requiring observance of principles of proportionality and necessity but extending measure of deference to state officials conducting national security surveillance); *see generally* Ashley Deeks, *An International Legal Framework for Surveillance*, 55 Va. J. Int'l L. 291 (2015) (discussing application of human rights principles to surveillance); Peter Margulies, *The NSA in Global Perspective: Surveillance, Human Rights, and International Counterterrorism*, 82 Fordham L. Rev. 2137, 2143 (2014) (same).

Ex parte proceedings can trigger issues about whether the court is deciding a "case or controversy" within the limits of Article III jurisdiction. *See* Peter Margulies, *Searching for Federal Judicial Power: Article III and the Foreign Intelligence Surveillance Court*, 85 Geo. Wash. L. Rev. 800 (2017) (contending that the FISC's role complies with Article III); Stephen I. Vladeck, *The FISA Court and Article III*, 72 Wash. & Lee L. Rev. 1161, 1170–80 (2015) (acknowledging that the FISC's role prompts tension with Article III and suggesting reforms that can ease this problem). On the other hand, *ex parte* proceedings to obtain warrants in ordinary criminal cases pre-date the Founding Era, suggesting that the Framers recognized such functions as consonant with Article III's framework. *See generally* David A. Sklansky, *The Fourth Amendment and Common Law*, 100 Colum. L. Rev. 1739, 1799 (2000) (discussing background of English cases known to the Framers); James E. Pfander & Daniel D. Birk, *Article III Judicial Power, the Adverse-Party Requirement, and Non-Contentious Jurisdiction*, 124 Yale L.J. 1346, 1375-76 (2015) (discussing Framers' understanding of *ex parte* warrants).

[17] Decisions by the FISC are subject to review by the Foreign Intelligence Court of Review (the FISCR), and a party disagreeing with a decision by the FISCR can seek review in the U.S. Supreme Court.

[18] United States v. Duggan, 743 F.2d 59 (2d Cir. 1984) (holding that 1978 statute was constitutional). Congress enacted the original FISA—sometimes called "traditional FISA" because of its requirement of a specific court order—to fill a gap in the law. When the U.S. Supreme Court held that warrantless wiretapping in domestic national security cases violated the Fourth Amendment, the Court expressly declined to address the legality of foreign surveillance. *See* United States v. United States District Court (*Keith*), 407 U.S. 297, 321-22 (1972). In enacting FISA, Congress crafted a comprehensive approach to this issue.

[19] For a historical account, *see* Peter Margulies, *Searching for Accountability Under FISA: Internal Separation of Powers and Surveillance Law*, 103 Marquette L. Rev. __ (forthcoming 2021), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3695054.

[20] See Neal Kumar Katyal & Richard Caplan, *The Surprisingly Stronger Case for the Legality of the NSA Surveillance Program: The FDR Precedent*, 60 Stan. L. Rev. 1023, 1032-34 (2008).

government can target communications of certain persons or entities "reasonably believed to be located outside the United States."[21] To collect such communications, intelligence officials designate "selectors" such as email addresses or mobile phone numbers. To be lawful, targets—even when located abroad—cannot be "United States persons," defined as either U.S. citizens or foreign nationals who are U.S. lawful permanent residents (LPRs). Targeting authority includes "one-end foreign communications" in which one party is a foreign national located abroad and one is either physically within the United States, a U.S. citizen, or an LPR.[22]

U.S. surveillance officials may target such communications to obtain "foreign intelligence information." Section 702's definition of foreign intelligence information includes attacks on the United States, espionage, sabotage, international terrorism, proliferation of weapons of mass destruction, and a more amorphous category: information "with respect to a foreign power or foreign territory that relates to … the conduct of the foreign affairs of the United States."[23] The "foreign affairs" category, in particular, suggests that § 702's targets can include a broad range of subjects.

To manage this broad coverage, it seems reasonable to infer that the United States uses automated methods such as machine learning to find patterns in the blizzard of emails, texts, social media posts, and phone calls available worldwide.[24] Artificial intelligence approaches such as machine learning can include deep-learning neural networks that rapidly sort through multiple variables in vast amounts of data.[25]

Unfortunately, despite their marked virtues, machine learning models also have significant deficits. For example, machine learning models that developers have not trained on complete or carefully selected data can make decisions that are "brittle." Brittle machine "learners" ignore context. Such naïve models pay excessive attention to trivial differences in

---

[21] 50 U.S.C. § 1881a(a).

[22] United States v. Hasbajrami, 945 F.3d 641, 649-58 (2d Cir. 2019) (describing statutory framework); David S. Kris & J. Douglas Wilson, National Security Investigations and Prosecutions § 17:17; Laura K. Donohue, The Future of Foreign Intelligence: Privacy and Surveillance in a Digital Age 69–72 (2016); Emily Berman, *When Database Queries Are Fourth Amendment Searches*, 102 Minn. L. Rev. 577, 593-94 (2017); Rachel G. Miller, *FISA Section 702: Does Querying Incidentally Collected Information Constitute a Search Under the Fourth Amendment?*, 95 Notre Dame L. Rev. 139 (2020).

[23] 50 U.S.C. § 1801(e)(2)(B). In practice, the "foreign affairs" prong of § 702 has received a narrower meaning than its wording suggests. That meaning appears to center on activities of foreign officials in negotiating international agreements of interest to the United States, such as agreements on trade sanctions for state sponsors of terrorism. *See* Peter Margulies, *Defining "Foreign Affairs" in Section 702 of the FISA Amendments Act: The Virtues and Deficits of Post-Snowden Dialogue on U.S. Surveillance Policy*, 72 Wash. & Lee L. Rev. 1283 (2015). Neither Congress nor the FISC has imposed specific constraints on the scope of coverage under this subsection.

[24] *See* Peter Margulies, *Surveillance by Algorithm: The NSA, Computerized Intelligence Collection, and Human Rights*, 68 Fla. L. Rev. 1045 (2016); Emily Berman, *A Government of Laws and Not of Machines*, 98 B.U. L. Rev. 1277, 1298-99 (2018).

[25] PEDRO DOMINGOS, THE MASTER ALGORITHM 6-10 (2015); STUART J. RUSSELL & PETER NORVIG, ARTIFICIAL INTELLIGENCE: A MODERN APPROACH (3d ed. 2010); IAN H. WITTEN, EIBE FRANK & MARK A. HALL, DATA MINING: PRACTICAL MACHINE LEARNING TOOLS AND TECHNIQUES 232 (3d ed. 2011).

inputs that any reasonable human being would correctly discount. In the brittle world of machine learning, such trivial differences can prompt huge changes in outputs.[26] In addition, in part because of the host of variables that neural networks process, these models often reach results that are often opaque, resisting conventional verbal explanations.[27] Another machine learning flaw of special concern to surveillance is the tendency of automated methods to reflect human biases.[28] A data set used to "train" an AI model in facial recognition may have fewer images of people of color, or may fail to include the full diversity of facial traits within and across all racial and ethnic groups.[29]

Machine learning's flaws are notable precisely because of the scope of U.S. surveillance. The targeting of persons or entities abroad under § 702 results in the incidental collection of large amounts of data on both U.S. persons and persons abroad.[30] U.S. officials collect data incidentally when that collection is an unavoidable result of targeting under the locational and substantive tests described above. As a rough example, suppose the U.S. targets the communications of a foreign national located abroad whom officials reasonably believe to be planning an act of international terrorism. The target uses a "Gmail" account. Because of the architecture of the Internet and the limits of current technology, obtaining the target's emails regarding terrorism will also entail obtaining other emails to or from that individual or perhaps other individuals that the Internet's routing protocols send in the same "packet." A rough analogy would be an email "page" than a person sees when checking for recent messages. That page will have multiple items, some involving work, but some likely of a personal nature. Because of the limits of current technology, the U.S. will collect all emails on that page, even those entirely unrelated to international terrorism—e.g., emails on the health of a family member.

---

[26] Consider an example from the realm of image recognition. Seeking to classify an image in a photograph, a neural network may classify a stop sign as a yield sign, if the photograph includes a few stray white specks on the sign. *See* Bita Dervish Rouhani et al., *Safe Machine Learning and Defeating Adversarial Attacks*, 17 IEEE Security & Privacy, Mar.-Apr. 2019, at 31, 31–32, https://ieeexplore.ieee. org/document/8677311; *see generally* Paul Scharre,nPAUL SCHARRE, ARMY OF NONE: AUTONOMOUS WEAPONS AND THE FUTURE OF WAR (2018) (discussing flaws in training and implementation of machine learning systems); Peter Margulies, *Autonomous Cyber Capabilities Below and Above the Use of Force Threshold: Balancing Proportionality and the Need for Speed*, 96 Int'l L. Stud. 394 (2020) (same). Data scientists may be able to deal with this and other flaws through more discerning and inclusive training of machine learners. But training that lacks this diligent approach will merely replicate the flaws.

[27] Katherine J. Strandburg, *Rulemaking and Inscrutable Automated Decision Tools*, 119 Columbia L. Rev. 1851, 1877–78 (2019); David Lehr & Paul Ohm, *Playing with the Data: What Legal Scholars Should Learn About Machine Learning*, 51 UC Davis L. Rev. 653 (2017).

[28] Ashley Deeks, *High-Tech International Law*, 88 Geo. Wash. L. Rev. 574, 641 (2020); Margaret Hu, *Algorithmic Jim Crow*, 86 Fordham L. Rev. 633 (2017).

[29] *See* Aziz Huq, *Constitutional Rights in the Machine-Learning State*, 105 Cornell L. Rev. 1875, 1900-02 (2020); *see also* Shirin Sinnar, *Separate and Unequal: The Law of "Domestic" and "International" Terrorism*, 117 Mich. L. Rev. 1333, 1344-48 (2019) (arguing that FISA surveillance is biased against Muslims, Arabs, and South Asians).

[30] *Hasbajrami*, 945 F.3d at 661-62.

While targeting under § 702 is subject to independent review, that review is limited in scope. Under § 702, the FISC does not issue specific orders authorizing surveillance. Instead, §702 requires only annual approval by the FISC of the government's certification that procedures for gathering and using information are consistent with the statute. The FISC seems mindful of the danger that *ex parte* proceedings on certification would not subject the government's stance to appropriate levels of scrutiny. As a result, the FISC has employed *amici curiae*—friends of the court—to provide an opposing voice on legal and technical issues.[31]

B. Post-Snowden Reforms

Despite wider scope of collection under § 702 and the absence of prior specific judicial approval of targeting decisions, the FISC has imposed significant constraints.[32] First, the FISC, based on voluntary limits accepted and explained by U.S. intelligence officials, agreed that one widely used way to designate "selectors" for gathering communications violated FISA. According to both the FISC and executive branch officials, the law did not allow collection of communications that were merely "about" selectors.[33] The FISC distinguished so-called "abouts" collection from collection of communications to and from a targeted selector. Compared with this latter, more limited form of intelligence-gathering, "abouts" collection entailed acquiring of far more correspondence unrelated to the purpose of the surveillance. While the FISC barred "abouts" communication because of this method's impact on U.S. persons,[34] the bar on "abouts" communication also materially reduces the quantity of non-U.S. persons' communications that U.S. intelligence officials acquire.

In addition, the FISC has reined in the Federal Bureau of Investigation's (FBI's) use of the vast § 702 database. Concerned that the FBI was using queries unrelated to statutory purposes to search the data, the FISC cracked down.[35] It required FBI personnel to pre-clear with FBI lawyers queries that could elicit information about U.S. persons. The FISC also required that FBI personnel document their justification for such queries. Here, too, the direct beneficiaries of the FISC's review were U.S. persons. However, any reduction in U.S. person queries also

---

[31] In re Section 702 2018 Certification, For. Intell. Surv. Ct., at 85 (Oct. 18, 2018), https://www.intelligence.gov/assets/documents/702%20Documents/declassified/2018_Cert_FISC_Opin_18Oct18.pdf (recounting position of *amicus* opposing government view).

[32] *See generally* Alan Rozenshtein, *Surveillance Intermediaries*, 70 Stan. L. Rev. 99, 155 (2018) (observing that "the repeat nature of the interactions [between the executive branch and the FISC] make generating trust and credibility important; if the [government] … tries to pull a fast one in one instance, it knows to expect punishment from a skeptical court the next time it seeks authorization" for surveillance). The outcry from Snowden's disclosures was a major catalyst in the subsequent reforms. While internal oversight was present before those revelations, commentators have argued that internal oversight was too limited to provide the check that was necessary. *See* Margo Schlanger, *Intelligence Legalism and the National Security Agency's Civil Liberties Gap*, 6 Harv. Nat'l Sec. J. 112, 113 (2015).

[33] *In re Section 702 2018 Certification* at 12-19.

[34] *Id*. at 13.

[35] *Id*. at 68-75 (discussing FBI querying of § 702 data to find information about U.S. government contractors and others with no relationship to foreign intelligence information).

reduces dissemination of information about foreign persons who communicated—often innocently—with those U.S. persons. In addition, both the FISC's scrutiny and the release of such FISC opinions to the public by the U.S. Director of National Intelligence instills discipline in intelligence officials that should reduce overbroad collection across the board.[36]

In the wake of Edward Snowden's revelations, the U.S. has also become far more transparent with the public about surveillance and the rules of the road that operate in this space. An online website, "IC on the Record," contains a wealth of materials about U.S. surveillance. For example, IC on the Record recently published guidelines for a highly classified program alluded to below: EO 12333.[37] That commitment to transparency encourages public debate about the scope of surveillance and the adequacy of safeguards on government discretion. If the public and informed observers view surveillance as unduly broad or protections as insufficiently robust, they can push for legislative or executive fixes.

In addition to § 702, EO 12333 reaches non-U.S. persons' communications. Under this authority, the president authorize the collection of a range of signals intelligence (SIGINT) abroad, including communications regarding the "activities, capabilities, plans, and intentions of foreign powers."[38] To obtain communications that fit these criteria, the U.S. government can scan through automated means a vast spectrum of international communications, in a process that the U.S. government calls "bulk collection." It can then retain and inspect by both human and automated means communications that are relevant to the factors described above. To cabin this power after the Snowden revelations, President Barack Obama issued Presidential Policy Directive Number 28 (PPD-28),[39] which limited the purposes of surveillance. PPD-28 acknowledged that, "[a]ll persons should be treated with dignity and respect, regardless of their

---

[36] As discussed later in the text of this Article, the website "IC on the Record" includes a wealth of material released to the public by intelligence officials. *See, e.g.*, Opinion and Order Regarding Use and Disclosure of Information, at 1-2 (For. Intell. Surv. Ct. June 25, 2020), https://www.intelligence.gov/assets/documents/702%20Documents/declassified/June_2020_FISC_Opinion.pdf (ruling on information acquired by government through "traditional FISA" requests in the case of Carter Page, a former foreign policy advisor to the Trump 2016 election campaign; the court referred to executive branch acknowledgment that "at least some of its collection" under these requests was "unlawful" because government officials had failed to provide the FISC with information to properly weigh the allegations made in the requests); Bernard Horowitz, *FISA, the "Wall," and Crossfire Hurricane: A Contextualized Legal History*, 7 Nat'l Sec. L.J. 1 (2019) (discussing problems with Carter Page FISA request); Margulies, *Searching for Accountability Under FISA*, *supra* note __ (same).

[37] *See* Office of the Director of Nat'l Intelligence, *Intelligence Activities Approved by the Attorney General Pursuant to Executive Order 12333* (Released Jan. 14, 2021), https://www.intelligence.gov/assets/documents/702%20Documents/declassified/AGGs/ODNI%20guidelines%20as%20approved%20by%20AG%2012.23.20_OCR.pdf (hereinafter ODNI, *Attorney-General-Approved Intelligence Activities*).

[38] For a useful summary, *see* Eric Manpearl, *The Privacy Rights of Non-U.S. Persons in Signals Intelligence*, 29 Fla. J. Int'l L. 303, 318 (2018).

[39] *See* Presidential Policy Directive/PPD-28 (Jan. 17, 2014) [hereinafter PPD-28] (establishing policies for global protection of personal information).

nationality or wherever they might reside, and all persons have legitimate privacy interests in the handling of their personal information."[40]

Consistent with that acknowledgment, PPD-28 limited U.S. bulk collection under EO 12333 to a defined set of goals including acquiring data about the plans of foreign governments, espionage, sabotage, terrorism, cybersecurity, proliferation of weapons of mass destruction, and transnational criminal threats such as money laundering and evasion of U.S. sanctions.[41] The guidelines recently posted on IC on the Record track these limits.[42]

Under both § 702 and EO 12333, U.S. officials used technology not just to enhance surveillance capabilities, but also to optimize compliance with legal norms. The guidelines on EO 12333 that the Attorney General approved require regular audits of all officials' access to EO 12333 data, queries of that data for U.S. person information, and reasons for the queries.[43] Congress has also required development of technological tools to facilitate recording such information about queries of § 702 data.[44] While more has to be done to integrate technology into compliance, the U.S. is working toward this objective.[45] As with § 702, the main focus in compliance is on U.S. person queries.[46] However, that discipline also exerts both direct and indirect downward pressure on collection of data concerning foreign nationals abroad.[47]

II. *SCHREMS II* AND *QUADRATURE DU NET*: THE CJEU ON NATIONAL SECURITY SURVEILLANCE

In *Schrems II*, the CJEU struck down the Privacy Shield agreement on transatlantic data transfers. The *Schrems II* court relied on a rationale that tracked the CJEU's reasoning in *Schrems I*, which had struck down Privacy Shield's predecessor, the Safe Harbor Agreement. In both cases, the CJEU was heavily influenced by the revelations of Edward Snowden regarding the scope of U.S. surveillance.[48] Although the CJEU's October 2020 *Quadrature du Net* decision

---

[40] *Id.* at 5.

[41] Id. at 4.

[42] ODNI, *Attorney-General-Approved Intelligence Activities*, at 2.2.2(b), p, 10.

[43] *Id*. at 5.2.2.1, p. 18.

[44] 50 U.S.C. § 1881a(f)(1)(B); *cf.* Robert S. Litt, *The Fourth Amendment in the Information Age*, 126 Yale L.J. F. 8, 18 (2016) (discussing technological compliance measures such as automated alerts when queries exceed statutory limits).

[45] *In re 2018 Certification*, at 56-61. The FBI has installed such technical fixes efficiently for national security letters (NSLs) that seek information from corporations and other entities. *See* PETER STRZOK, COMPROMISED: COUNTERINTELLIGENCE AND THE THREAT OF DONALD J. TRUMP 46 (2020). The FBI could build on this success with § 702 queries.

[46] ODNI, *Attorney-General-Approved Intelligence Activities*, at 5.2.3(b), pp. 18-19.

[47] *See supra* notes __-__ and accompanying text.

[48] The *Schrems II* decision occurred against the backdrop of post-Snowden developments, including Brexit and the rise of illiberalism in the EU and in the United States under former president Donald Trump. *See* Francesca Bignami, *Schrems II: The Right to Privacy and the New Illiberalism*, Verfassungsblog (July 29, 2020).

acknowledged the importance of national security, that decision left a gap between EU privacy safeguards and U.S. law.[49]

A. Schrems II *and the Importance of Constraints on Surveillance*

In *Schrems II*, the CJEU followed in broad terms the outline that it had first used in *Schrems I*, suggesting that a company doing business in the EU had to ascertain that protections for the data were "adequate" under EU law in the country which would ultimately receive the data.[50] Under *Schrems II*, transfer of data to a third country is always appropriate if the third country "ensures an adequate level of protection" for the privacy of the data.[51] However, transfers in the absence of an adequacy finding or appropriate safeguards under GDPR Article 46 may be unlawful, unless they meet the conditions for derogation under GDPR Article 49. This subsection first discusses adequacy and appropriate safeguards, and then addresses the scope of possible Article 49 derogations.

1. Adequacy and Appropriate Safeguards Under *Schrems II*

According to the *Schrems II* court, an adequacy finding hinges on two conditions. First, the protections in the third country must be "essentially equivalent" to EU law.[52] EU law is highly protective of individual data, although those protections do not always extend to the national security surveillance conducted by EU member states.[53] In addition, the legal system of the third country must fit the factors laid out in Article 45(2), including the rule of law, independent review of government decisions affecting privacy, and "effective" recourse for persons or entities ("data subjects") who assert that the third country has wrongly obtained or used their personal data. This provision of the GDPR also considers whether the third country has entered into international agreements that further bolster privacy.[54] In the absence of an

---

[49] Scholars have long commented on differences in substance and tone between the EU and the United States on privacy issues. *See* James Q. Whitman, *The Two Western Cultures of Privacy: Dignity Versus Liberty*, 113 Yale L.J. 1151 (2004) (asserting that the United States views privacy as instrumental to liberty, while Europeans cherish dignity, defined as not imposing unwanted public scrutiny on individuals); *cf.* Francesca Bignami, *European Versus American Liberty: A Comparative Privacy Analysis of Antiterrorism Data Mining*, 48 B.C. L. Rev. 609 (2007) (suggesting that liberty is also important to EU conception of privacy); William McGeveran, *Friending the Privacy Regulators*, 58 Ariz. L. Rev. 959, 988-1003 (2016) (suggesting that in practice EU and U.S. privacy regulators are converging toward a "responsive regulation" model that encourages input from regulated entities); Ira Rubinstein, *Privacy and Regulatory Innovation: Moving Beyond Voluntary Codes*, 6 I/S: J. L. & Pol'y Info. Soc'y 355 (2011) (discussing models of co-regulation between regulators and regulated entities); Michael L. Rustad & Thomas H. Koenig, *Towards a Global Data Privacy Standard*, 71 Fla. L. Rev. 365, 387-403 (2019) (arguing that EU privacy law has become increasingly influential worldwide and in United States).

[50] *Schrems II*, ¶ 186.

[51] GDPR Art. 45(1).

[52] *Schrems II*, ¶ 105. For a valuable analysis, *see* Christopher Kuner, *Schrems II Re-Examined*, Verfassungsblog (Aug. 25, 2020), https://verfassungsblog.de/schrems-ii-re-examined/.

[53] *See* Art. 2(2), GDPR (including carve-outs for common national security and individual states' law enforcement and public security measures); *see infra* notes __-__ and accompanying text.

[54] *Schrems II*, ¶¶ 104 & 105.

adequacy decision, the company seeking to transfer data must show that appropriate safeguards ensure the data's protection once it enters the third country.

In addressing who makes that decision about "essential equivalence" and adequacy of protection, the *Schrems II* court emphasized that ultimate authority resided with the court itself. The court is at the apex of a pyramid that includes other EU bodies and Member States. The European Commission—the EU's executive arm—has an initial, provisional role. The Commission determines whether a particular third country—such as the United States—has ensured an adequate level of protection of personal data.[55] If nationals of EU member states are dissatisfied with the Commission's stance, those individuals can file complaints with their own national data protection authority.[56] Those authorities have a mechanism for seeking CJEU review. The national authorities can bring a lawsuit in a national court, arguing that protections are not adequate in a third state. The national court may then refer a matter to the CJEU, which makes the ultimate determination.[57] The European Commission's initial decision, under both *Schrems I* and *Schrems II*, received little if any deference from the court.

The *Schrems II* court also raised questions about the use of so-called standard contractual clauses Standard Contractual Clauses (SCCs)—private agreements to supply additional safeguards for data transfer against government surveillance—as a work-around for failures in adequacy. The court did not opine definitively on such clauses.[58] In theory, parties to data transfer may be able to craft SCCs that largely obviate the risk of surveillance from the United States or other third states. For example, to use a stylized example, parties may agree to share data through shipment of a portable hard drive.[59] The hard drive containing this data is an inanimate object without an internet link or other communications capability. Upon receipt, the contents of the hard drive could then be downloaded onto a computer that was also "air-gapped" to disable all Internet connectivity.

This cumbersome process would, at least in theory, not be subject to U.S. surveillance. However, for any less elaborately contrived transfer, some risk of internet connectivity remains. In those situations, the *Schrems II* court said that the most important provision of an SCC would be a provision that requires *suspension* of the data transfer if compliance with protections is impossible.[60]

In terms of U.S. law, the *Schrems II* court stressed the importance of independent review and suggested that U.S. law was lacking both in this respect and in the proportionality of

---

[55] *Id.*, ¶¶ 117, 118.

[56] *Id.*, ¶. 120.

[57] *Id.*

[58] *Id.*, ¶¶ 143-46.

[59] We are indebted to privacy lawyer David Kessler of Norton Rose Fulbright for this example.

[60] *Schrems II*, ¶ 137.

surveillance under § 702 and EO 12333.[61] In addition, painting with too broad a brush, the *Schrems II* court stated that the FISC never addressed whether individual selectors under § 702 are "'properly targeted to acquire foreign intelligence information.'"[62] This description is unduly stark. Both the EC and the *Schrems II* court conflated the nature of the *procedures* that the FISC follows in its § 702 review and the substantive standard that the FISC employs.

The *Schrems II* court conceded that FISC review was "designed to verify whether … surveillance programmes relate to the objective of acquiring foreign intelligence information."[63] Moreover, the court was correct in its analysis of procedure, since the FISC does not review each possible selector to determine its fit with § 702's substantive criteria, such as detection of threats against the United States.

That said, the FISC has the ability to consider selectors and determine whether the criteria that U.S. intelligence agencies apply in choosing selectors are consistent with statutory purposes. FISC review is not limited to the written submissions of the U.S. Department of Justice in its certification. Indeed, as recent FISC decisions have shown, the FISC regularly reviews the querying practices of the FBI and other agencies.[64] It does so, because if implementation of the statute fails to fit the guidance that U.S. officials supply in their certification, that failure undermines the statutory scheme. Some FISC review of individual selectors is necessary to find that U.S. officials have implemented the statute correctly.

The *Schrems II* court's perception that FISA "does not indicate any limitations on the power it confers to implement government surveillance"[65] is thus a needlessly sweeping generality. The court's failure to acknowledge the actual scope of the FISC's review is problematic.[66] However, the *Schrems II* court was correct in two important respects.

The *Schrems II* court's sound descriptions outweighed its passing exaggerations. The CJEU accurately observed that the FISC does not review each and every selector which U.S. surveillance officials target. That lack of comprehensive individualized review poses a problem under EU law, although post-*Schrems II* decisions such as *Quadrature du Net* and *Privacy International* suggest that states may have a measure of flexibility in determining the targets of national security surveillance and the means of collecting data on those targets.[67] Second, the *Schrems II* court was correct in stating that neither § 702 nor EO 12333 give individual data

---

[61] *Id.*, ¶¶ 177, 178.

[62] *Id.*, ¶ 179.

[63] *Id.*

[64] *See In re Section 702 2018 Certification* at 68-75.

[65] *Schrems II*, ¶ 180.

[66] *See* Comment, *Recent Case: National Security Law—Surveillance—Court of Justice of the European Union Invalidates EU-U.S. Privacy Shield*, 134 Harv. L. Rev. 1567, 1571-73 (2021) (asserting that the *Schrems II* court painted with too broad a brush in describing U.S. surveillance).

[67] *See infra* notes __-__ and accompanying text.

subjects an avenue for seeking recourse against U.S. officials for surveillance abuses.[68] Moreover, the court found that U.S. bulk collection was not necessary or proportionate.[69]

In addition, the *Schrems II* court found that the U.S. mode of review of EU persons' complaints under Privacy Shield lacked independence from executive branch influence. Under Privacy Shield, the United States had tasked an ombudsperson at the State Department with fielding EU persons' privacy complaints. In assessing whether the State Department ombudsperson spot was a sufficient privacy fix, the *Schrems II* court found that the ombudsperson could not be sufficiently independent, since that official reported to the U.S. Secretary of State and lacked any protection against dismissal.[70] Moreover, the ombudsperson lacked binding power over U.S. intelligence agencies conducting surveillance. Fortified by this conclusion, the court found that Privacy Shield was "incompatible" with Article 45 of the GDPR.[71]

This conclusion put the onus on standard contractual clauses (SCCs) to protect data. However, as the CJEU noted, SCCs may not be a sufficient safeguard against the broad surveillance efforts of a country like the United States.[72] When a party recognizes SCCs' failure to protect data, the most drastic option under SCCs kicks in: suspension of data transfers.[73] That harsh alternative would undermine the functioning of U.S. companies with EU offices, holdings, or interests.

2. Exploring Article 49 Derogations

Despite these negative conclusions in *Schrems II* about the adequacy of protection for personal information sent to the United States and the CJEU's cautionary notes about SCCs, the court left one intriguing pathway available for data transfers. As *Schrems II* acknowledged, a possible source of flexibility for certain types of data transfers is Article 49 of the GDPR.[74] Article 49 governs certain specific exceptions—"derogations" in EU parlance—from otherwise applicable data protection provisions. Under Article 49(1)(b), a transfer to a country without adequate protections for data can still take place, even without "appropriate safeguards" such as effective SCCs. But a transfer must meet one of several conditions. As one illustration, the parties to a transfer must reasonably believe that the transfer is "necessary for the performance of

[68] *Schrems II*, ¶¶ 181, 182.

[69] *Id.*, ¶¶ 183, 184.

[70] *Id.*, ¶¶ 195-96.

[71] *Id.*, ¶ 199.

[72] *Id.*, ¶¶ 141, 142.

[73] *Id.*, ¶ 142.

[74] *Id.*, ¶ 202 (noting that Article 49 "details the conditions under which transfers of personal data to third countries may take place in the absence of" an adequacy finding or appropriate safeguards under Article 46" and thus avoids a potential "legal vacuum" regarding the fate of such transfers).

a contract between the data subject" and the transferor.[75] A U.S. company with an EU office that is transferring data about an employee may fit this criterion.[76]

Delving deeper into an derogation under Article 49(1)(b), suppose an EU employee of a U.S. firm makes a claim for health benefits. Health information is exceptionally sensitive. However, the U.S. firm may require disclosure of some data about the benefits claim in order to fulfill its accounting or cost-control duties, guard against fraud, or improve its benefits claim process. The need to disclose some data to assist the firm may be part of the employee's contract. A transfer that was strictly tailored to performance of this contract term might fit within Article 49(1)(b). That transfer would have to include use restrictions that would limit dissemination of such information. To deal with such a situation, a firm could also seek the express consent of the employee, which would justify a derogation under Article 49(1)(a).

In sum, while Article 49 is not a panacea for what ails data transfer after *Schrems II*, it is a remedy well worth further inquiry. As we shall see, Article 49 might also provide help in conjunction with the other measures recommended in this law review Article, including a risk-based approach and U.S. reforms. Article 49 derogations would not assist in every transfer. They fit the intra-firm context well; they might not fit a social media company like Facebook. But a carve-out for intra-firm transfers of data would sidestep the serious obstacle to global economic transactions that the *Schrems II* holding might otherwise represent.

3. Summary

In *Schrems II*, the CJEU coupled concrete recommendations for institutional, procedural, and substantive reform and acknowledgment of Article 49 derogations with a rejection of blanket deference on national security surveillance. As we shall see in the next subsection, more recent cases reinforce the *Schrems II* court's specific recommendations while signaling appreciation for genuine, carefully tailored national security measures.

B. The CJEU's Delicate Balance in Quadrature du Net*: Mandating Reforms While Recognizing the Need for State Flexibility*

For any court, finding the optimal accommodation between privacy and national security would be a challenging endeavor. Reflecting this truth, the CJEU's *La Quadrature du Net and Others*[77] judgment in October 2020 on legislation requiring bulk retention of communications

[75] *See* Art. 49(1)(b), GDPR.

[76] In an important discussion on the occasion of the 2021 Europe Data Protection Day, Judge Thomas Danwitz of the CJEU suggested that Article 49 derogations were worthy of exploration for companies that required a measure of flexibility. *See* Online-Meeting to the European Data Protection Day 2021, at 2:24:00 (2 February 2021), https://www.bmi.bund.de/SharedDocs/videos/EN/european-data-protection-day.html. Of course, Judge Danwitz was merely noting the value of exploring Article 49 derogations, not opining definitively on Article 49's scope.

[77] Case No. C-511/18, Ct. Justice Eur. Union (6 Oct. 2020). In a companion case decided on the same day, *Privacy International v. Secretary of State*, Case No. C-623/17, the CJEU reinforced the guidance in *Quadrature du Net*. *See id.* at ¶ 58 (recognizing that states may derogate from privacy rights in case of "necessary, appropriate and proportionate measure within a democratic society to safeguard national security, defence and public security"). While the tone of *Quadrature du Net* is more deferential to Member State interests and the tone in *Privacy*

looked in two different directions. Affirming the focus on reform in *Schrems II*, the CJEU in *Quadrature du Net* again emphasized the importance of necessity, proportionality, and independent review. However, the *Quadrature du Net* decision also acknowledged that once a state had imposed such safeguards, existential threats such as terrorism gave states more room for the exercise of discretion in the scope and duration of intelligence collection.

In assessing the mandatory bulk retention regime at issue in *Quadrature du Net*,[78] the CJEU first had to contend with the carve-out in both the Treaty of the European Union (TEU) and the GDPR for national security.[79] While European Union law is supreme in matters of commerce, member states did not relinquish their power to make individual state decisions on national security matters. Commerce influenced a state's prosperity, while national security decisions could affect a state's very existence. EU law expressly reserved these decisions for individual member states. In *Schrems II* and other cases, the CJEU had stepped into the national security space. However, it had done so for prophylactic reasons, to prevent states from making pretextual use of national security to invade privacy. In *Quadrature*, the CJEU had to reconcile that check on state pretext with the clear carve-out for national security law that EU law provided.[80]

The CJEU recognized that under the TEU the existential threats posed by national security could permit a Member State to "indiscriminately" order retention of key data on individuals' communications, subject to carefully delineated restrictions on use of such

---

International is more rights-protective, each decision balances broad privacy rights with carefully tailored exceptions for national security. In this sense, both *Quadrature du Net* and *Privacy International* modify the more absolutist rights protection in the CJEU's earlier decision, *Tele2 Sverige AB v. Post-och telestyrelsen*, Case No. C-203-15 (21 Dec. 2016). For an analysis of *Quadrature du Net* and *Privacy International*, *see* Juraj Sajfert, *Bulk Data interception/retention judgments of the CJEU – A victory and a defeat for privacy*, European Law Blog (Oct. 26, 2020), https://europeanlawblog.eu/2020/10/26/bulk-data-interception-retention-judgments-of-the-cjeu-a-victory-and-a-defeat-for-privacy/.

[78] Case No. C-511/18, Ct. Justice Eur. Union (6 Oct. 2020).

[79] *See* Art. 4(2), Consolidated Version of the Treaty of the European Union (TEU), May 2, 2008, 2008 O.J. (C 115) (TEU) (providing that EU "shall respect … essential State functions, including … safeguarding national security"); Art. 23(1)(a), GDPR (providing that EU states can restrict privacy rights when a limit "respects the essence of the fundamental rights and freedoms" established in the regulation and is necessary for and proportionate to protection of national security).

[80] The conflict between certain EU institutions and the U.S. on surveillance should not obscure the *intra-EU* conflict on the balance between privacy and national security. Some EU parties, including the center-right European People's Party—which includes Germany's Christian Democrats—have stressed national security and viewed ready data-sharing between the EU and the United States as promoting that goal. For example, the United States can share information about possible terrorist groups with EU allies and member bodies. Some government agencies in EU Member States, such as interior, security, and foreign ministries, have favored a similar balance. *See* Francesca Bignami & Giorgio Resta, *Transatlantic Privacy Regulation: Conflict and Cooperation*, 78 L. & Contemp. Probs. 231, 247 (2015).

information.[81] Acknowledging that "national security remains the sole responsibility of each Member State," the *Quadrature* court cited the danger of terrorism.[82] The court recognized that both as a matter of sovereignty and as a matter of EU law, preserving space for states' difficult national security decisions was a high priority, entailing greater deference than states' decisions about ordinary law enforcement, which lacks that existential dimension.[83]

Befitting the importance of national security, a state could retain—at least for some period and subject to use restrictions—communications data of "all users" even without portions of that data having any obvious link to the "national security of the Member State."[84] The legislature could even mandate the retention of information of users whose link was remote or nonexistent.[85] The court recognized that it would be impossible to tell *ex ante* which individuals had affiliations with terrorist groups or other existential threats. Using retained data on traffic, location, and search history, state officials could detect patterns. Moreover, to find a needle in the haystack, the state could resort to algorithms and "automated processing."[86] In this sense, the CJEU approved automated searches that easily exceed the searches that the U.S. Supreme Court currently permits of U.S. nationals' data.[87] The latter require probable cause and a court order for data such as cell-site location information.[88]

Mindful that the breadth of its authorization could prompt abuse, the CJEU insisted on safeguards that echoed the substantive, procedural, and institutional safeguards required in *Schrems II*. In the substantive realm, such collection would have to be necessary and proportionate, and tailored to a "genuine" threat.[89] The court imposed specific restraints on automated processing of retained information.

To pass muster, automated processing would have to use "models and criteria" that are "specific and reliable.[90] This requirement is vital in light of the well-documented propensity of machine learning techniques to ignore context.[91] Under *Quadrature du Net*, a country using automated processing would have to demonstrate it had substantially reduced machine learning's brittleness. In addition, according to the *Quadrature* court, automated processing would have to

---

[81] *Quadrature du Net*, ¶ 137. That information could include location and search history. *Id*.

[82] *Id*., ¶ 135.

[83] *Id*., ¶ 136.

[84] *Id*., ¶ 137.

[85] *Id*.

[86] *Id*., ¶ 178.

[87] *See* Carpenter v. United States, 138 S. Ct. 2206 (2018).

[88] *Id.* at 2219-20.

[89] *Quadrature du Net*, ¶ 137.

[90] *Id*., ¶ 180.

[91] *See* Strandburg, *supra* note __; *supra* notes __-__ and accompanying text.

be free from discrimination.[92] Presumably, the *Quadrature* court's logic would also require that machine learning models be amenable to some kind of verbal explanation.[93]

Moreover, the *Quadrature* court required that automated processing must include procedural checks that curb brittleness and bias. Although a state can use artificial intelligence (AI) to inspect retained communications data such as traffic and location, the further step of real-time surveillance of a particular suspect requires review by "non-automated means."[94] In other words, a human being would have to review an AI model's output and determine if further real-time surveillance or collection was appropriate. In addition, a state would have to conduct periodic systemic reviews of its AI surveillance models, to ensure that they were "up to date" in the range of training data provided to the model and any other inputs that ensured reliability going forward.[95]

The *Quadrature* court also reinforced an institutional check that the *Schrems II* court had stressed: independent, "effective" review of all privacy complaints. According to *Quadrature*, that review could include either a court or an "independent administrative body."[96] Without independence, surveillance officials could engage in overbroad surveillance with impunity. Independence, as in *Schrems II*, was necessary to fortify the robust safeguards against abuse that the court demanded.

That said, even the procedural checks that *Quadrature* required entailed a measure of flexibility for states conducting national security surveillance. While states would have to limit the time period covered by an order to retain communications in bulk, officials could also renew that period on a showing of necessity.[97] In addition, although officials had to notify the targets of surveillance, that notice requirement was not absolute. Rather, as in the case law of the European Court of Human Rights, notice was obligatory only when it would not jeopardize an investigation.[98] In cases where surveillance actually uncovered evidence of a national security threat, notice would allow the target to "adapt his conduct" and therefore put investigators off the scent.[99] The *Quadrature* court recognized that this was a legitimate concern.

C. The European Court of Human Rights Weighs In: Big Brother Watch

---

[92] *Quadrature du Net*, ¶ 180.

[93] *See* Sandra Wachter, Brent Mittelstadt & Chris Russell, *Counterfactual Explanations Without Opening the Black Box: Automated Decisions and the GDPR*, 31 Harv. J. L. & Tech. 841 (2018) (discussing how to fulfill GDPR requirement of "right to an explanation" of automated processing).

[94] *Quadrature du Net*, ¶ 182.

[95] *Id.*

[96] *Id.*, ¶¶ 138-39, 179.

[97] *Id.*, ¶ 138.

[98] *Id.*, ¶ 190; *see also* Big Brother Watch and Others v. United Kingdom, Eur. Ct. Hum. Rts., App. No. 58170/13, ¶ 340 (13 Sept. 2018) (in decision by European Court of Human Rights, discussing situations where notice was not required).

[99] Kennedy v. United Kingdom, App. No. 26839/05, 52 Eur. H.R. Rep. 207, 253–54 (2010).

The European Court of Human Rights' (ECHR) decision in *Big Brother Watch v. United Kingdom*,[100]parallels the holding of the CJEU in *Quadrature du Net*. The ECHR recognized that countries conduct bulk collection largely for foreign intelligence purposes.[101] Because of legitimate state interests in combating terrorism and other transnational threats, the Court found that states should receive a "margin of appreciation"—a measure of deference—in the their operation of a foreign intelligence bulk collection program.[102] However, the Court recognized that the protection of privacy interests required constraints on such programs.

Officials running the program had to ensure that the "selectors" used to search for data were proportional and appropriately tailored to avoid sweeping up, storing, and retrieving personal and sensitive information unrelated to national security.[103] The operation of the program had to be subject to independent review, although review by a court was not required.[104] The reviewing body needed to authorize collection before surveillance started.[105] However, the reviewing body did not need to approve specific selectors related to particular individuals, since that might unduly disrupt intelligence efforts. But a reviewing body had to receive information about the general "types or categories" of selectors used.[106] Presumably, an independent body would need to know if bulk collection entailed gathering information from emails, phone calls, texts, and social media posts. For individual selectors, internal authorization was required; no rogue investigator could decide for herself to target a particular individual without approval by a more senior official.[107] Recourse was necessary for persons harmed by surveillance, although the Court recognized that a state's legitimate interest in maintaining the secrecy of its collection program could affect the availability and nature of recourse.[108]

With reference to the United Kingdom (UK), the court found flaws in privacy safeguards. Britain was on the right track, with an independent agency, the Investigatory Powers Tribunal (IPT), participating. However, the IPT did not have sufficient authority to conduct the required review. For example, initial authorization came from the UK Secretary of State, who as part of the government was not sufficiently independent.[109] The IPT needed to receive information

---

[100] No. 58170/13 (25 May 2021), https://www.brickcourt.co.uk/images/uploads/documents/Big_Brother_Watch_GC_Judgment_-_25-5-21.pdf.

[101] ¶ 345; *see also* Eliza Watt, *Much Ado about Mass Surveillance – the EctHR Grand Chamber 'Opens the Gates of an Electronic "Big Brother" in Europe' in* Big Brother Watch v UK, Strasbourg Observers (June 28, 2021), https://strasbourgobservers.com/2021/06/28/much-ado-about-mass-surveillance-the-ecthr-grand-chamber-opens-the-gates-of-an-electronic-big-brother-in-europe-in-big-brother-watch-v-uk/ (analyzing decision).

[102] ¶ P 338.

[103] ¶ 350.

[104] ¶ 351.

[105] ¶ 350.

[106] ¶ 354.

[107] ¶ 355.

[108] ¶ 357.

[109] ¶ 377.

about categories and types of selectors.[110] The Court did note that the provision for audits done by IPT or internal sources was important and useful.[111]

The United States' showing under the *Big Brother* standard would hinge on the measure involved: protections under § 702 of FISA are far more extensive than those under EO 12333. Generally, § 702 of FISA would stack up well in comparison with the standard that the ECHR laid down in *Big Brother Watch*. The FISC does prior authorization of collection through its annual certification process, which also entails a look back at past compliance. As part of the annual certification, the Justice Department informs the FISC of the broad outlines of the program, including the categories of selectors used. However, the United States still may not provide sufficient recourse.[112] Moreover, EO 12333 is not subject to the same safeguards as § 702. In this sense, *Big Brother Watch* produces a mixed "scorecard" for United States surveillance abroad.

D. Summary

Quadrature du Net and *Big Brother Watch* suggested that the CJEU and ECHR respectively were navigating between the perilous shoals of undue deference, on the one hand, and an impractical rights absolutism, on the other. This approach recognizes the need for institutional, procedural, and substantive checks on surveillance. However, it also recognizes that needlessly strict constraints will undermine national security and intrude too much on matters that EU law leaves to Member States. In the next section, we address whether EU regulators such as the EDPB have fully internalized the need for this careful navigation between extremes.

III. THE EDPB RECOMMENDATIONS

On November 10, 2020 the European Data Protection Board (the "Board") adopted preliminary recommendations (subject to public consultation) on the steps data exporters must take to assess whether transfer tools—including SCCs—ensure compliance with the level of data protection required by *Schrems II*.[113] Where compliance is not ensured, the recommendations also identify supplementary measures exporters may adopt to ensure that the level of protection is adequate.[114] The Board simultaneously adopted recommendations on European Essential Guarantees (EEG) that must be respected to ensure that interference with personal data by

[110] ¶ 381.

[111] ¶¶ 381, 388.

[112] *See* Clapper v. Amnesty Int'l, USA, 568 398 (2013) (holding that plaintiffs who alleged surveillance abuses lacked standing).

[113] Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data (Nov. 2020), https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2020/recommendations-012020-measures-supplement-transfer_en, (the "Draft Recommendations").

[114] *Id.*

surveillance measures does not exceed what is necessary and proportionate in a democratic society.[115]

These preliminary recommendations provided data exporters with a roadmap for applying *Schrems II* to data transfers including steps to follow to determine if supplementary measures are required, preferred sources of information for conducting an assessment, and some case studies identifying both effective (and ineffective) measures. The Board established a six-step process in which companies' data protection officers should 1) know their firm's transfers, 2) verify the relevant transfer tool, 3) assess third country laws and practices under the EEG Recommendations, 4) adopt necessary supplementary measures, 5) take any procedural steps required, and 6) re-evaluate at appropriate intervals.

On June 18, 2021, following public consultation, the Board adopted the final version of these recommendations, retaining both the six-step process and the EEG Recommendations as the reference standard for assessing foreign surveillance laws and practices.[116] But the Final Recommendations permit exporters conducting an assessment to take into account the laws *and* practices of third countries in applying surveillance laws to the specific circumstances of a particular data importer.[117] As discussed below, the Board's somewhat more flexible approach reflects the position taken by the Commission in revising the text of the standard contractual clauses in light of *Schrems II.*[118]

Both the Final Recommendations and the analysis of data protection rights in the EEG Recommendations offer very general guidance applicable to data exports to any third country using any Article 46 transfer tool. However, in spite of this lengthy guidance and the new emphasis on the application of "law in practice," serious difficulties remain regarding transfers to

---

[115] *See* Recommendations 02/2020 on the European Essential Guarantees for surveillance measures, https://edpb.europa.eu/our-work-tools/our-documents/recommendations/edpb-recommendations-022020-european-essential_en (the "EEG Recommendations"). The Board identifies four essential guarantees: basing processing on clear, precise and accessible rules; demonstrating the necessity and proportionality of legitimate objectives; independent oversight mechanisms; and effective individual remedies. *Id.* 8-15. We agree with the analysis of Theodore Christakis that in analyzing these guarantees, the Board sets a very high standard (noting that they "always 'pick and choose' the strictest requirements found in [the CJEU and the ECtHR] jurisprudence and somehow neglect elements that could be used to provide more flexibility for foreign countries' surveillance laws,") and ignores the concept of "the margin of appreciation" (noting that this concept suggest some willingness to favor member state adoption of bulk surveillance methods). *See* Theodore Christakis, *Schrems III? First Thoughts on the EDPB post-Schrems II Recommendations on International Data Transfers (Part 1)*, EUROPEAN LAW BLOG (Nov. 13, 2020), https://europeanlawblog.eu/2020/11/13/schrems-iii-first-thoughts-on-the-edpb-post-schrems-ii-recommendations-on-international-data-transfers-part-1/.

[116] Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data (June 2021), https://edpb.europa.eu/system/files/2021-06/edpb_recommendations_202001vo.2.0_supplementarymeasurestransferstools_en.pdf (the "Final Recommendations").

[117] *Id.*

[118] Commission Implementing Decision (EU) 2021/914 on standard contractual clauses for the transfer of personal data to third countries (June 2021), https://ec.europa.eu/info/law/law-topic/data-protection/international - dimension-data-protection/standard-contractual-clauses-scc_en (the "Implementing Decision").

companies in the U.S. or otherwise subject to U.S. surveillance laws, most notably § 702 but also EO 12333. After briefly describing the origin and use of SCCs for data transfers to the U.S., this Part turns to a close reading of Steps 3 and 4 of the Final Recommendations, analyzing their ambiguities and shortcomings at some length and their failure to reduce the legal uncertainty faced by multinational businesses subject to the GDPR's data transfer requirements.

A. Origin and Use of Standard Contractual Clauses

Historically, SCCs have played a central role in transborder data flows from Europe to the United States. Prior to the *Schrems* decisions, U.S. companies with EU offices seeking to transfer personal data to the United States had three options: (1) signing up for the Safe Harbor Agreement; (2) utilizing Binding Corporate Rules (BCRs) for transfers within a single company or a group of affiliated companies; or (3) using SCCs for data transfers from controllers to controllers or processors.[119] All three arrangements were treated as providing adequate protection as required by Article 45 of the GDPR and (before that) Article 25 of the Data Protection Directive.[120] But *Schrems I* invalidated the Safe Harbor Agreement while BCRs are not widely used.[121] That leaves only SCCs as a viable option for European or U.S.-owned firms in EEA countries wishing to share data with affiliates or partners in the U.S. or U.S. cloud service providers.[122]

Fortunately, SCCs are well-suited to the task. SCCs are easier to use than individual contracts or BCRs because their standardized terms avoid the need for additional drafting and cover a wide range of scenarios without having to worry about the nature of intra-company relationships.[123] Thus, SCCs have proven very popular with both EU and US controllers. With the demise of the Privacy Shield, dependence on SCCs is likely to increase, especially in view of the more flexible features of the new SCCs approved by the Commission in June 2021.[124]

---

[119] *See generally* CHRISTOPHER KUNER, EUROPEAN DATA PROTECTION LAW: CORPORATE COMPLIANCE AND REGULATION 180-207 (2nd ed. 2007).

[120] The GDPR repealed and replaced Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ 1995 L 281/31 (the "Directive").

[121] As of 2018, fewer than 100 companies used BCRs, mostly large European or U.S. multinational corporations. *See* List of companies for which the EU BCR cooperation procedure is closed (May 24, 2018), http://ec.europa.eu/newsroom/article29/document.cfm?doc_id=50116.

[122] The GDPR also permits companies to establish an adequate level of protection by adhering to an approved code of conduct or an approved certification mechanism, *see* Article 46(2)(f) and (2)(g), but neither of these new mechanisms are in wide use as of this writing.

[123] VOIGT & VON DEM BUSSCHE, *id.* at 122.

[124] These include a "modular" approach to multiple data transfer contexts (addressing all four cases of transfers between controllers and processors) and an optional "docking clause" to accommodate "complex processing operations often involving multiple data importers and exporters, long and complex processing chains, and evolving business relationships. *See* Implementing Decision, *supra* note __, at para. 6.

It is not at all clear, however, that this easy and reliable use of SCCs will survive the *Schrems II* decision, which imposes new burdens on controllers including a duty to verify, prior to transfer, that a third country offers an adequate level of protection.[125] Although the Court insists that data exporters and importers have always had a duty to verify the adequacy of third country laws, before *Schrems II* this requirement was more honored in the breach than in the observance. Consider that in 2001, when the Commission issued its earliest decision approving the use of SCCs, it allowed member state data protection agencies (DPAs) to prohibit or suspend data flows to third countries if the third country's surveillance laws permitted exceptions for national security that "go beyond the restrictions necessary in a democratic society."[126] Writing in 2007, however, Kuner identified only a single case where a DPA refused to recognize the use of SCCs as a legal basis for data transfers due to lack of adequacy.[127] Nor are we aware of any change in practices by controllers or DPAs after 2008 (when § 702 first took effect) or after 2013 (in response to the Snowden revelations), notwithstanding an Article 29 Working Party opinion proclaiming that SCCs could not serve "as a legal basis to justify the transfer of personal data to a third country authority for the purpose of massive and indiscriminate surveillance."[128]

Thus, in the years between 2001 (when SCCs were first approved) and 2015 (when *Schrems I* voided the Safe Harbor Agreement), there is scant evidence that controllers relying on SCCs for data transfers to the U.S. were aware of or acted on the duty of verification announced by the Court in *Schrems II* or that DPAs nullified the use of SCCs when controllers did not take such steps. *Schrems II* altered that welcoming landscape for SCCs, injecting fresh uncertainty into data controllers' job description. As the next subsection discusses, the EDPB's guidance compounds these quandaries.

B. Problems with the EDPB Recommendations

In this section, we analyze shortcomings with Step 3 and Step 4 of the Final Recommendations. Step 3 delegates adequacy assessments to controllers without regard for the competency of private firms to undertake these assessments. Step 4 requires controllers to adopt supplementary measures when adequacy assessments have negative outcomes without resolving a fundamental tension between two competing approaches to proportionality under Article 46. One frames the obligations of data exporters in terms of the fundamental rights character of EU data protection, while the other centers around a risk-based approach to compliance. We also briefly analyze the examples of supplementary measures in the Final Recommendations. These are divided into two categories: scenarios for which the Board suggested remedies and scenarios where the it stated that the problems were irremediable. Unfortunately, even in the former

[125] *Schrems II*, ¶ 142.

[126] Commission Decision 2001/497/EC of 15 June 2001 on standard contractual clauses for the transfer of personal data to third countries, under Directive 95/46/EC (OJ L 181, 4.7.2001, p. 19), Article 4(a).

[127] *See* KUNER, *supra* note __, at 202, n. 194.

[128] *See* Art 29 Working Party, Opinion 04/2014 on surveillance of electronic communications for intelligence and national security purposes (WP 215, April 10, 2014) 3.

situation, the Board's recommendations fail to provide practical solutions to controller's data transfer needs or to eliminate legal uncertainties.

1. Delegation.

Article 45 permits data exports to third countries on the basis of adequacy assessments undertaken by the Commission including an examination of a third country's surveillance laws. In the absence of an adequacy decision, there are alternative mechanisms for large scale data transfers; all of these mechanisms require some form of *government* review and approval. For example, the Commission must adopt SCCs[129] and a competent supervisory authority must approve binding corporate rules (BCRs).[130] Similarly, the Commission negotiated and approved both the Safe Harbor Agreement and the Privacy Shield. In contrast, the *Schrems II* decision delegates to the private sector the burden of determining appropriate safeguards including both enforceable data subject rights and effective legal remedies. Thus, data exporters relying on SCCs must "verify, on a case-by-case basis … whether the law of the third country of destination ensures adequate protections."[131]

The delegation of a governmental task to the private sector is not unprecedented in EU data protection law. The *Google Spain* decision delegated to Google the burden of operationalizing the right to be forgotten.[132] Although many have criticized this arrangement on the grounds that Google lacks democratic accountability, this delegation has benefits too "including gaining Google's administrative ability to process efficiently thousands of requests …, its technical know-how in web design and analytics, and, perhaps most important of all, the greater flexibility and experimentation Google may enjoy in developing the right than a government agency would enjoy."[133]

Unlike Google, however, few of the tens of thousands of data exporters hoping to rely on SCCs for data transfers to third countries have any special ability in assessing whether the laws of a third country provide adequate protection. Indeed, Step 3 assessments requires expertise in two arenas: First, extensive knowledge of a third country's privacy and national security laws as applied to a specific data transfer, which in turn requires familiarity with both the case law of ECHR and the CJEU and national case law of the destination country dealing with surveillance issues, reports from inter-governenmental organizations, reports by business, professional,

---

[129] GDPR, Article 46(2)(c). Alternatively, a supervisory authority may adopt SCCs with the approval of the Commission. *See* Article 46(2)(d).

[130] GDPR, Article 47(1)).

[131] *Schrems II*, ¶ 134.

[132] Case C-131/12, Google Spain SL v. Agencia Española de Protección de Datos (AEPD) (Costeja), 2014 EUR-Lex 62012CJ0131 (May 13, 2014). Under the right to be forgotten, a search engine such as Google must accommodate requests by private individuals to delete certain material from search results, if that information is personally embarrassing, remote in time, and irrelevant to current issues. This right is subject to certain exceptions, including those for information about public figures.

[133] Edward Lee, *Recognizing Rights in Real Time: The Role of Google in the EU Right to Be Forgotten*, 49 UC DAVIS L. REV. 1017, 1026 (2016).

academic civil society organizations, and transparency reports from firms processing data in the same industry as the importer;[134] and, second, the ability to analyze these elements holistically and determine whether they constitute an adequate level of protection under the GDPR read in light of the EEG Recommendations.[135]

Foreign law assessments are difficult, complex, ambiguous and costly in their own right. Indeed, one of us co-authored a comparative analysis of international bulk data collection laws and practices[136] based on papers commissioned from leading experts (and native speakers) in twelve countries in Europe and the Middle East, the Americas, and Asia and the Pacific.[137] Among its most prominent findings: in many countries, both the legal basis for bulk access and the underlying surveillance practices were hidden from public view; relevant laws were "vague and ambiguous, and government interpretations of them are often hidden or even classified"; and published law and actual practice were often inconsistent.[138]

Despite these practical difficulties faced even by experts in the field, the Board requires data exporters and importers to shoulder the burden of conducting (and fully documenting) assessments based on information that is "relevant, objective, reliable, verifiable and publicly available."[139] The Board itself offers no geopolitical analysis of which countries surveillance laws are problematic in various scenarios. Thus, thousands of firms must master both European and foreign surveillance laws and practices and related judicial procedures in multiple countries (and languages) and then analyze these laws against the evolving requirements of EU data protection law. This is a substantial burden, especially for small and medium-sized enterprises (SMEs) engaged in routine data transfers. In addition, it will inevitably result in a lack of certainty and uniformity regarding the propriety of data transfers to the same country by different exporters.[140] Mistakes are unavoidable.[141]

---

[134] *See* Final Recommendations, Annex 3.

[135] Final Recommendations, ⁋⁋ 40-42.

[136] Ira Rubinstein, Gregory Nojeim and Ronald Lee, *Systematic Government Access to Personal Data: A Comparative Analysis*, 4 INT'L DATA PRIVACY L. 96, 97 (2014). Revised and reprinted in BULK COLLECTION: SYSTEMATIC GOVERNMENT ACCESS TO PRIVATE-SECTOR DATA (F. Cate & J. Dempsey, eds., 2017).

[137] See generally BULK COLLECTION, *id.* at 49-306.

[138] Rubinstein, et al., *supra* note __ at 97.

[139] Final Recommendations, ⁋ 46.

[140] *See* Peter Swire, *"*Schrems II*" backs the EU legal regime into a corner—how can it get out?*, Int'l Ass'n of Privacy Professionals (IAPP) Blog (July 16, 2020).

[141] This is obvious from the outcome of the two *Schrems* decisions rejecting the Commission's own adequacy assessments approving the Safe Harbor Arrangement and the Privacy Shield Decision. If the Commission erred, it follows that many private firms are also bound to fail, absent more practical guidance regarding how the Board and the DPAs view specific scenarios arising under specific foreign laws in specific destination countries. Some might object that these agencies only disclose their thinking about such matters in the course of issuing formal adequacy decisions. But formal adequacy decisions occupy the far end of a very wide continuum of useful guidance the government might offer. There is ample room on the continuum for the government to provide practical assistance beyond the generalities and abstractions of the Final Recommendations and EEG Recommendations.

2. Does the Six-Step Process Require a Risk-Based or a Rights-Based Approach to Proportionality Under Article 46?

The adoption of a risk-based approach to data protection constitutes one of the main regulatory innovations of the GDPR. Risk-assessment and risk-management are both central to the accountability principle in Article 24, data protection by design and default in Article 25, security of processing in Article 32, and the requirement to conduct "data protection impact assessments" (DPIAs) of high-risk processing operations in Article 35 and to seek prior consultations per Article 36.

Article 24's accountability principle provides a general framework for the risk-based approach by requiring the implementation of appropriate technical and organizational measures that take into account "the nature, scope, context and purposes of processing as well as the risks of varying *likelihood and severity* for the rights and freedoms of natural persons" (emphasis added).[142] Many have questioned whether this risk-based approach applies not only to the accountability provisions in Chapter IV of the GDPR but also to the data protection principles in Chapter II (including data minimization and lawful processing) and the rights granted to data subjects in Chapter III (including transparency, access, rectification and the right to be free of automated decision-making and profiling). Furthermore, critics have voiced concerns that adoption of a risk-based approach makes fundamental rights far too dependent on calculating the costs and benefits of a processing operation, with the likely result of increasing the discretion of controllers and diminishing the rights of data subjects.[143]

Commentators have sought in various ways to resolve the tensions between the risk-based approach to compliance and the GDPR's fundamental rights character. Hustinx insists that the notion of a risk-based approach "should be carefully distinguished from the notion of 'risk' as a threshold condition for any protection to apply, and even more from an approach in which protection would only apply to the most risky processing operations." Rather, "more detailed obligations should apply where the risk is higher and less burdensome obligations where it is lower."[144] As Lynskey correctly observes,[145] this is in keeping with the Article 29 Working Party's insistence that the risk-based approach is not an alternative to well-established data protection rights and principles, but rather is "a scalable and proportionate approach to compliance."[146] Thus, a graduated risk-based approach to legal obligations implies "that a data

[142] GDPR, Article 24; *see also* Recitals 74-77.

[143] *See* Raphaël Gellert, *We Have Always Managed Risks in Data Protection Law: Understanding the Similarities and Differences Between the Rights-Based and the Risk-Based Approaches to Data Protection*, 4 EUROPEAN DATA PROTECTION L. 481, 482-83 (2016).

[144] Peter Hustinx, EU Data Protection Law: The Review of Directive 95/46/EC and the Proposed General Data Protection Regulation, 38 (Sept. 2014), https://edps.europa.eu/data-protection/our-work/publications/speeches-articles/eu-data-protection-law-review-directive_en.

[145] ORLA LYNSKEY, THE FOUNDATIONS OF EU DATA PROTECTION LAW 85 (2014).

[146] Art 29 WP, "Statement on the Role of a Risk- Based Approach in Data Protection Legal Frameworks" 2 (2014), https://www.huntonprivacyblog.com/wp-content/uploads/sites/18/2014/06/wp218_en.pdf.

controller whose processing is relatively low risk may not have to do as much to comply with its legal obligations as a data controller whose processing is high-risk."[147]

Gellert goes one step further by suggesting that a risk-based approach to compliance and adherence to GDPR legal obligation are "twin practices" insofar as both rely on very similar balancing tests.[148] Quelle takes a different tack by arguing that the risk-based approach both "supplements and alters" data protection obligations but in different ways depending on the nature of the obligation.[149] Thus, the risk-based approach fits well with the GDPR's accountability provisions, somewhat less so with data protection principles requiring a risk-oriented result (such as processing for a compatible purpose) or a risk-oriented effort (such as maintaining integrity and confidentiality), and much less with the control rights of data subjects.[150]

The logic of the risk-based approach frames appropriate safeguards for Article 46 data transfers. A risk-based approach entails balancing the need for certain supplementary measures against various risk factors (including the "likelihood and severity [of government intrusions] for certain rights and freedoms") in order to set appropriate safeguards. Controllers can adopt less burdensome measures where the likelihood of foreign government access to transferred data is very low and/or the impact of such access on rights and freedoms is not very severe.

Alternatively, a strict rights-based approach considers the laws of a third country in more universal terms in order to determine whether or not they satisfy the essential guarantees (by imposing limitations on surveillance powers that respect the principles of necessity and proportionality as a general matter). Foreign laws that fail this test require appropriate supplementary measures. This implies that measures allowing any level of interference with fundamental rights, no matter how unlikely this occurrence, cannot be tolerated. As the analysis below suggests, the Final Recommendations move back and forth between these two ways of framing Article 46 obligations (and hence Step 3 assessments and Step 4 supplementary measures) without successfully resolving the underlying tension between them.

3. The Final Recommendations: Clear Guidance or More Uncertainty?

As noted above, Step 3 in the data transfer roadmap requires a data exporter to determine if there is anything in the law or practices of the third country that may impinge on the effectiveness of the appropriate safeguards of SCCs (or other transfer tools) in the context of a

[147] *Id.*

[148] Gellert, *supra* note __. *See generally* RAPHEL GELLERT, THE RISK-BASED APPROACH TO DATA PROTECTION (2020) (arguing that the principle of proportionality is the "missing link" between data protection regulation and risk).

[149] Claudia Quelle, *The 'risk revolution' in EU data protection law: We can't have our cake and eat it, too, in* DATA PROTECTION AND PRIVACY: THE AGE OF INTELLIGENT MACHINES (R Leenes, R van Brakel, S Gutwirth and P De Hert, eds., 2017).

[150] *Id.* at __.

specific transfer.[151] The Board identifies a list of factors for analyzing the relevant context including the purposes of the transfer, the types of entities involved in the processing, the sector in which the transfer occurs, the categories of personal data transferred, where the data is stored and/or accessed, data format, and the possibility of onward transfers.[152] This may sound like a risk-based approach—that is, one that allows firms to adopt appropriate safeguards based on the *likelihood* of risk and the *severity* of the applicable factors. In fact, Step 3 diverges from a risk-based approach in several ways.

To begin with, the Final Recommendations fail to cross-reference any of the familiar risk-based assessment techniques that permeate the GDPR.[153] Rather, the Board demands a binary, up or down verdict on whether or not a third country's surveillance laws and practices satisfy the European Essential Guarantees, thereby ensuring that data exporters and importers comply with their obligations under Article 46.[154] The Board's demand for a binary assessment is especially prominent in its treatment of US law and practices. For example, in the Draft Recommendations, the Board cites *Schrems II* for the conclusion that § 702 "does not respect the minimum safeguards resulting from the principle of proportionality under EU law" further stating that if a data transfer falls within the scope of § 702, data exporters may not rely on SCCs unless they adopt supplemental technical measures.[155] Indeed, firms that fall within the scope of § 702 may as well dispense with any further analysis of the applicable legal context or the specific circumstances of the transfer based on the factors identified above because the outcome of the analysis is predetermined.

Firms may seek to rebut this conclusion by embracing the position taken by the U.S. government ("USG") in a November 2020 White Paper.[156] The White Paper—which was co-authored by the ODNI, a senior-level agency that provides oversight to the U.S. Intelligence Community—states: "Most U.S. companies do not deal in data that is of any interest to U.S. intelligence agencies, and have no grounds to believe they do. They are not engaged in data transfers that present the type of risks to privacy that appear to have concerned the CJEU in Schrems II."[157] Moreover, companies whose EU operations involve ordinary commercial products or services, and whose EU-U.S. transfers of personal data involve ordinary commercial information like employee, customer, or sales records, "would have no basis to believe U.S.

---

[151] *See* Final Recommendations, ⁋ 30.

[152] *Id.*, ⁋ 33.

[153] For a discussion, s*ee supra* III.B.2.

[154] *Id.*, ⁋ 49. Similarly, the language used in describing the standards that technical measures must satisfy to ensure equivalence is also binary (measures are effective or ineffective) rather than scalable and proportionate to the risk. *See id.*, ⁋ __

[155] Draft Recommendations, text box under ⁋ 44; *see also* Final Recommendations, text box under ⁋ 49.

[156] U.S. Dep't of Comm., U.S. Dep't of Justice, and Office Dir. Nat'l Intelligence (ODNI), Information on U.S. Privacy Safeguards Relevant to SCCs and Other EU Legal Bases for EU-U.S. Data Transfers after Schrems II (Sept. 28, 2020), https://www.commerce.gov/sites/default/files/2020-09/SCCsWhitePaperFORMATTEDFINAL508COMPLIANT.PDF at 1.

[157] *Id.*

intelligence agencies would seek to collect that data."[158] But the Board (at least in the Draft Recommendations) heavily discounts these declarations, stating that "the likelihood of public authorities' access to your data in a manner not in line with EU standards" is merely a "subjective" factor and Step 3 assessments may only consider "objective factors."[159]

In spite of this stance, the USG's argument seems compelling. After all, § 702 is not universal in scope and there is nothing "subjective" about its statutory limitations. For example, § 702 by its terms does not permit the U.S. government to "intentionally target a United States person reasonably believed to be located outside the United States."[160] It follows that a U.S. firm in Paris, all of whose employees are U.S. persons, might rely on SCCs to transfer data about them to the U.S. with almost no likelihood of running afoul of § 702. And this is an objective reading of the statute, not a subjective assessment.Think tanks like the Center on Information Privacy Law,[161] as well as various European trade associations like Bitkom,[162] and Digital Europe,[163] have urged EU officials to recognize the limited scope of § 702 but it is too soon to say how much the Board (or the DPAs) will take these suggestions to heart in enforcement actions.

Almost seven months after the Board adopted the Draft Recommendations, the Commission published an Implementing Decision in which it sought to re-establish a risk-based approach to SCCs.[164] In contrast to the Board, the Commission treats the likelihood of foreign government access to data under the specific circumstances of a data transfer as a legitimate factor that parties may consider in their assessments.[165] In the Final Recommendations, the Board revised its position accordingly by dropping any reference to subjective versus objective factors and allowing firms to take into account the practical experiences of the importer,[166] including "the practical scope of application" of § 702.[167]

---

[158] *Id.*

[159] Draft Recommendations, ⁋ 42.

[160] 50 U.S.C. § 1881a(b)(2).

[161] *See* Centre for Information Policy Leadership, Comments on the European Data Protection Board's Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data (21 Dec. 2020).

[162] *See* Bitkom, Position Paper: EDPB Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data (21 Dec. 2020).

[163] *See* Digital Europe, Response to draft EDPB Recommendations on supplementary measures for personal data transfers 21 Dec. (2020).

[164] Implementing Decision, *supra* note __,

[165] *Id.* at ⁋ 20 (noting that "different elements may be considered as part of an overall assessment, including reliable information on the application of the law in practice (such as case law and reports by independent oversight bodies), the existence or absence of requests in the same sector and, under strict conditions, the documented practical experience of the data exporter and/or data importer").

[166] *Id.*, ⁋ 47.

[167] *Id.*, text box under ⁋ 49.

This represents an important concession by the Board, especially for firms that can point to a legal prohibition on § 702 requests (such as our hypothetical U.S. firm in Paris or a manufacturer that offers no electronic communication services). But the size of this concession largely depends on how EU data protection authorities treat firms that might be subject to § 702 but have not (so far) received any requests for access to data from U.S. public authorities. Consider the thousands of privately owned firms (including insurance firms) that offer telephone or email services to their employees but not the to the general public. Do they fall within the scope of § 702 as "electronic communication service providers" (ECSPs)? In his report to the Irish High Court in the *Schrems II* litigation, privacy expert Peter Swire referred to a Third Circuit case that treated an insurance firm offering email services to its employees as meeting the definition of an "electronic communication service" (ECS) under the Electronic Communication Privacy Act (ECPA), thereby raising the possibility that such firms may indeed fall within the scope of § 702 (because an ECS is one of the sub-categories of ECSPs).[168] Suppose further that an insurance firm wishes to transfer data from its European offices to the U.S and reports no prior instances of § 702 (or any other FISA) requests. Does this suffice to demonstrate that the firms are not subject to § 702? In the Final Recommendations, the Board is ambivalent at best, discounting "the absence of prior instances" and instead demanding that firms take on the difficult if not impossible task of proving a negative.[169]

Nor is § 702 the only obstacle firms face in seeking to transfer data from the EU to the U.S. by means of SCCs. In *Schrems II*, the CJEU raised concerns with intelligence activities under both § 702 (which authorizes the USG to compel ECSPs to disclose communication data in response to a court order) and EO 12333 (which does not authorize compulsory orders to private firms but instead permits direct access to transmission networks located outside the U.S. for specified intelligence purposes). In the Final Recommendations, the Board alludes to EO 12333 when it states that the essential guarantees apply "during the *transit of data* from the exporter to the importer's country."[170] And EO 12333 poses a far more serious obstacle to data

[168] Peter Swire, Irish High Court Testimony (Nov. 2, 2016), at 9-2, https://www.alston.com/en/resources/peter-swire-irish-high-court-case-testimony.

[169] As noted by the Board, "the absence of prior instances of requests received by the importer can never be considered, by itself, as a decisive factor on the effectiveness of the Article 46 GDPR transfer tool that allows the transfer to proceed without supplementary measures" and "should be corroborated and not contradicted by relevant, objective, reliable, verifiable and publicly available or otherwise accessible information on the practical application of the relevant law." Final Recommendations, ¶ 47.

[170] *Id.*, ¶ 29 (emphasis added); *see also* note 40, which refers to a discussion in *Schrems II* of the legal deficiencies of data access under EO 12333. The USG argues that foreign surveillance via direct access to transmission networks on the basis of EO 12333 should be treated as outside the bounds of any adequacy assessments. *See* United States Mission to the European Union, Comments on Proposed SCC Decisions, (Dec. 10, 2020) 5-8, https://edpb.europa.eu/sites/default/files/webform/public_consultation_reply/2020.12.21_-_us_comments_on_edpb_supp_measures_final.pdf The EDPB appears to reject this argument in view of *Schrems II* and the Final Recommendations. For a thorough discussion of the opposing arguments, *see* Theodore Christakis, Squaring the Circle? International Surveillance, Underwater Cables and EU-US Adequacy Negotiations (Part 1), EUROPEAN LAW BLOG (April 12, 2021), https://europeanlawblog.eu/2021/04/12/squaring-the-circle-international-surveillance-underwater-cables-and-eu-us-adequacy-negotiations-part1/ and Theodore Christakis, Squaring the Circle? International Surveillance, Underwater Cables and EU-US Adequacy Negotiations (Part 2), EUROPEAN LAW BLOG (April 13, 2021), https://europeanlawblog.eu/2021/04/13/squaring-the-circle-international-surveillance-underwater-cables-and-eu-us-adequacy-negotiations-part2/.

transfers than § 702 for at least two reasons. First, unlike § 702, EO 12333 has no provision limiting its scope. Thus, overseas clandestine intelligence gathering may occur with respect to any data transfer by any company. Furthermore, no company has any basis for proving that it is beyond the scope of EO 12333. Second, while the U.S. government regulates overseas intelligence gathering under EO 12333, PPD-28 and various other authorities,[171] the operational details about specific locations or targets of interception are confidential and classified. They are certainly not publicly available to data exporters or importers. And this makes it impossible for U.S. firms to conduct a satisfactory Step 3 assessment related to the circumstances of a given data transfer because they have no way of determining whether U.S law and practice relating to direct access of transmission networks meets EU legal standards. As the U.S. government mordantly observes in its White Paper:

> Were the lawfulness of data transfers outside the EU to depend on an assessment of intelligence agencies' clandestine access to data outside a given destination country while in transit, no data transfers could be found lawful under EU standards because intelligence agencies worldwide potentially could access the data as it travels over global networks.[172]

4. The Board's Case Studies

To summarize the argument so far: In Step 3, the Board purportedly adopts a risk-based approach to assessing the laws and practices of third countries. But in the case of assessments undertaken in support of data transfers from the EU to the U.S., this approach turns into a binary review of the scope of § 702 and EO 12333 with limited regard for a firm's specific circumstances. As a practical matter, uncertainty over the scope of these provisions will result in a large number of firms reaching a negative outcome in their Step 3 assessments, forcing them to adopt supplementary technical measures under Step 4 or forego entirely data transfers relying on SCCs.

---

[171] *See supra* note __.

[172] *See supra* note ___, at 17-18. The White Paper offers a second reason that companies may find it impractical to conduct Step 3 assessments: the CJEU has never ruled on the lawfulness of foreign surveillance by EU Member States (i.e., surveillance of communications outside of a state's territorial jurisdiction) and may lack the jurisdiction to do so, while the ECtHR has only ruled on domestic surveillance by Member States and never on foreign surveillance. Thus, it is impossible to assess whether access under EO 12333 meets EU standards because "there is no discernable comparator in EU law." *Id.* at 18.

One likely counterargument to these objections is that the Board has already identified a supplementary technical measure to protect data during transit, namely, end-to-end encryption, and in Use Cases 3 and 4, declares that end-to-end encryption "provides an effective supplementary measure," *See* Final Recommendations, *supra* note __, at note 54 and 33. Thus, even if a firm fails to prove the negative (that is, to establish that it is not the target of international surveillance authorized by EO 12333), it may overcome this problem by resorting to a readily available technical measure for protecting data in transit. This is a compelling retort provided the Board extends this blanket treatment of end-to-end encryption as an "effective" measure to all data transfers potentially subject to EO 12333. On the other hand, if the Board or DPAs were to require a case-by-case analysis of a firm's use of end-to-end encryption for specific data transfers—and hence an assessment of whether the NSA can bypass end-to-end encryption in a given case—then firms are back to square one, having to conduct an assessment even though they lack access to any relevant information.

Step 4 in the data transfer roadmap requires a determination of the effectiveness of supplementary measures in guaranteeing the required level of protection on a case-by-case basis. As in Step 3, the Board provides a list of relevant factors along with some examples of supplementary measures in Annex 2. The factors include data format (i.e., is the data in plain text, pseudonymized or encrypted), the nature of the data, the length and complexity of data processing workflow, and the possibility that the data may be subject to onward transfers. These sound like the elements of a risk-based assessment of data processing and the technical, organizational and contractual measures needed to address such risks. But once again the Board backs away from a truly risk-based approach.

In the Draft Recommendations, the Board takes a narrow view of supplementary measures in the context of EU-U.S. data transfers: Due to the possibility of § 702 and EO 12333 access, data exporters may rely on SCCs only "if additional supplementary *technical* measures make access to transferred data impossible or ineffective."[173] This is a high standard. It sets aside less burdensome contractual or organizational measures and instead requires technical measures that guarantee essential equivalence. But ensuring that data access is "impossible" is beyond the capability of any risk-based assessment. Neither qualitative nor quantitative risk-assessments can absolutely preclude a given outcome. Rather, all they can do is identify potential hazards that could cause harm and determine countermeasures that may reduce the likelihood and severity of such harms.[174] If Step 4 were truly risk-based, it would describe a process for determining likelihood of data access by US spy agencies and the countermeasures for reducing the probability of access or mitigating any resulting harm. By setting an impossibility standard and insisting that technical measures achieve a guarantee of essential equivalence, the Board in the Draft Recommendations abandoned any pretense of finding practical solutions. Granted, in the Final Recommendations, the Board replaced the terms "impossible or ineffective" with the terms "impede or render ineffective."[175] While this language is friendlier to a risk-based approach—to "impede or render ineffective" is a matter of degree whereas impossibility only permits binary outcomes—the Use Cases reveal that the Board is unwilling to endorse supplementary technical measures unless they guarantee a predetermined outcome.

Step 4 identifies five risk-based factors for assessing supplementary measures: (1) the format of the data to be transferred (i.e. in plain text/pseudonymised or encrypted); (2) the nature of the data (i.e., its sensitivity); (3) the length and complexity of data processing workflow (such as the number of actors involved in the processing); (4) the technique or parameters of practical application of the third country law concluded in Step 3; and (5) the possibility that the data may be subject to onward transfers within the same third country or even to other third countries.[176]

---

[173] Final Recommendations, text box under § 44 (emphasis added); *see also* para 48.

[174] *See generally*, Cheryl A. Wilhelmsen and Lee T. Ostrom, RISK ASSESSMENT: TOOLS, TECHNIQUES, AND THEIR APPLICATIONS (2nd ed., 2019).

[175] Final Recommendations, § 53.

[176] Final Recommendations, § 54.

However, only the first factor (data format) truly matters because it trumps the other factosr. This is obvious from thinking through the implications of resorting to encryption as a technical measure. Encryption converts plain text into unreadable cipher text, making it unintelligible to anyone other than an intended recipient who holds a decryption key for converting the cipher text back into readable plain text.[177] The primary purpose of such encryption is to protect the confidentiality of both stored data or data transmitted over the internet or any other computer network. This also protects stored or transmitted data against access by unauthorized parties—including U.S. intelligence agencies engaged in intelligence activities under § 702 or EO 12333. Imagine a data transfer to the U.S. that is very low-risk in terms of factors 2, 3, and 5, (i.e., the data is not sensitive; the data processing workflow is limited to a single corporate entity; and there is no onward transfer). If the data is not encrypted, thereby allowing possible access by U.S. spy agencies, these other factors are irrelevant. Only data format—in this case, the use of encryption—prevents foreign government intrusion. It alone makes access impossible or ineffective. Of course, a necessary consequence of relying on encryption for these pruposes is that it also prevents the parties to a data transfer from reading the encrypted data unless they have access to the key.

The seven Use Cases include five scenarios featuring effective technical measures (three involving encryption, one involving pseudonymization, and one involving secure multiparty computing) and two depicting ineffective steps (one involving encryption and the other remote access).The encryption scenarios are the most important to data exporters (because they involve data storage and transmission and the use of cloud services) but also the most telling in terms of revealing how the Board's preference for absolutes, not probabilities.

Consider Use Case 1, which endorses encrypted data storage as a supplementary measure but with several caveats. One caveat cautions that the data exporter (or a trustee in a third country whose laws have been deemed adequate under Article 45) must retain sole control over the encryption/decryption keys. This sounds like a practical option for data exporters except that it completely ignores the disadvantages to cloud customers of using cloud service providers who must be denied access to the keys and hence to unencrypted data. This not only prevents cloud providers from performing such useful tasks as scanning the data for malware or other security threats but also disrupts value-added functionalities such as search and other forms of data analysis (including real-time analytics and machine learning). Moreover, the encrypted data storage scenario ignores the ready availability of data localization solutions using dedicated local data centers to enable customers to store data in their own region. In short, the Board permits a company holding European citizen data to store this data in the U.S. if and only if it encrypts the data and retains sole control of the keys, thereby foregoing many of the additional benefits of cloud services. But few European firms are likely to embrace this option when the entire gamut of cloud services is available to them in Europe from both European firms and major U.S.

[177] This is referred to as "symmetric encryption." *See* William Stallings, NETWORK SECURITY ESSENTIALS: APPLICATIONS AND STANDARDS 46 (6th ed. 2019).

providers utilizing the data localization model.[178] In this sense, the Board's recommendations are simply a recipe for data localization in the EU—a solution with its own set of issues.[179]

Use Case No. 2 enables a data exporter to pseudonymize data prior to transfers to a third country for analysis. This might be useful for purposes of statistical research provided many additional conditions are met.[180] However, it does not serve the needs of many ordinary commercial transfers requiring access to personal data (notably for Human Resources (HR) purposes).

Use Case No. 3 continues the Board's rigid approach. It endorses encrypted data merely transiting a third country provided certain conditions are met. To pass muster, the encryption protocols employed must be state-of-the art and provide "effective protection against active and passive attacks with resources known to be available to the public authorities of the third country," employ tests for software vulnerabilities and possible back doors, and the encryption algorithm must conform to the state-of-the-art and be considered "robust against cryptanalysis performed by the public authorities when data is transiting to this third country taking into account the resources and technical capabilities" of the third country and be properly implemented.[181] Of course, it is no small task for the parties to satisfy these conditions. Indeed, it may be impossible for businesses to determine definitively the resources and capabilities for attacking encryption protocols or undertaking cryptanalysis of an intelligence agency such as the NSA when this information is confidential and classified.

The remaining examples exhibit different problems. For example, Use Case No. 4 allows transfers "to a data importer in a third country specifically protected by that country's law, e.g., for the purpose to jointly provide medical treatment for a patient, or legal services to a client" if the laws of the country fully exempt the data from government access, the data exporter encrypts the data in transit, and the data importer retains sole custody of the encryption keys. But this use case is inconsistent with Step 3: if local law fully protects the transferred data against access, Step 3 should result in a positive assessment of foreign surveillance law as achieving equivalence, making the supplementary technical measures superfluous.[182] Use Case 5 relies on secure multiparty processing, but we will skip over it for simplicity's sake.

Use Case 6 rejects as ineffective one of the most common scenarios for cloud computing, namely, data processing in the clear by cloud service providers (i.e., unencrypted processing).[183]

---

[178] *See* Paul M. Schwartz, *Legal Access to the Global Cloud*, 118 COL. L. REV. 1681, 1694-97 (2018).

[179] *See* Anapum Chander, *Is Data Localization a Solution for Schrems II?* 23 J. INT'L ECON. L. 771 (2020).

[180] *See* Final Recommendations, ⁋⁋ 86-88.

[181] *Id*., ⁋ 90.

[182] See Digital Europe, Response to draft EDPB Recommendations on supplementary measures for personal data transfers 21 Dec. (2020), note 10.

[183] Cloud services providers typically encrypt data in transmission and at rest. In order to perform most arithmetic operations on encrypted data, however, they must convert it back to its unencrypted form. Although

The Board's position in Use Case 6 also bars direct data transfer from EU firms to their U.S. affiliates or customers (i.e., transfers not involving cloud providers) if they permit access to data in the clear. Now add to this Use Case 7, in which the Board rejects remote access and use of data in the clear by a data importer in a third country. Remote access is appealing for various business purposes including a European parent company allowing its U.S. subsidiary to access a unified HR database that includes European employee data. But Use Case 7 rejects this scenario, even though the data never leaves the EU and is accessible only for brief periods under the control of the data exporter, which can revoke access at the first sign of trouble (such as any indication of U.S. government interest in accessing the data).

The inescapable conclusion is that the supplementary technical measures the Board considers effective not only stigmatize most routine data transfers between Europe and the U.S. but render them pointless.[184] What sense does it make to advise data exporters to adopt supplementary measures like encryption in order to ensure an essential equivalent level of protection to that guaranteed by EU law, when these measures make it impossible for data importers to even read the transferred data? Furthermore, this outcome is unnecessarily strict. It treats high-risk transfers (e.g., by communication providers falling squarely within the scope of § 702) in the same manner as low-risk transfers (e.g., ordinary businesses that transfer ordinary commercial data which is of no interest to U.S. intelligence agencies per the USG White Paper). It also squanders the enormous investment in time and resources that U.S. firms have devoted to GDPR compliance. As a result, data transfers by thousands of firms will be disrupted notwithstanding the low-risk nature of the transfers. These firms will have to await the negotiation of a new Privacy Shield agreement, which may not succeed. There has to be a better way.

5. The Illusory Appeal of Easy Solutions

This grim conclusion has led some commentators to look for "magic bullet" solutions that define U.S. surveillance power narrowly to justify U.S. firms' reliance on SCCs. Thus, Alan Raul, a former Vice Chairman of the U.S. Privacy and Civil Liberties Oversight Board (PCLOB), has argued that *Schrems II* is less of a problem for EU-U.S. data transfers than one might think.[185] He suggests that there are categorical bars in §702 and E.O. 12333 against certain types of data collection. According to Raul, "[d]ata transfers pursuant to SCCs between an American company in Europe to its American headquarters in the U.S. are exactly the types of communications that may not be targeted under those authorities."

Raul's argument is highly appealing because it enables firms to avoid the need for burdensome supplementary measures (as discussed above). But his rationale is unduly optimistic and overbroad. It conflates the *probability* that the U.S. intelligence agencies will

researchers have demonstrated the feasibility of processing encrypted data using "homomorphic encryption" and other new approaches, at this point in time these are more experimental than practical.

[184] See Christakis, *supra* note __.

[185] Alan Charles Raul, *Why Schrems II Might Not Be a Problem for EU-U.S. Data Transfers*, LAWFARE (Dec. 21, 2020), https://www.lawfareblog.com/why-schrems-ii-might-not-be-problem-eu-us-data-transfers.

seek access to certain transferred data—a risk-based assessment—with the existence of categorical bars preventing such access as a matter of law. Raul's risk assessment is persuasive. Indeed, it parallels our own. But his categorical legal argument fails.

Under § 702, the U.S. government can target any person "reasonably believed to be located outside the United States" who is not a U.S. person (i.e., neither a U.S. citizen nor an LPR).[186] It makes no difference whether such persons happen to work for U.S. companies or subsidiaries of U.S. companies: officials can target persons who fall within § 702's targeting criteria, including espionage, sabotage, attacks on the U.S., sanctions evasion, and U.S. "foreign affairs." Communications from such individuals may be collected directly or incidentally, even if they happen to work for U.S. companies. Moreover, such communications may involve personal information of EU individuals.

As a practical matter, most employees of U.S. companies abroad may well not be targeted. But that's a *risk-based* calculation—one that the EDPB rejects. It is not a categorical *legal* protection. Legal protection might inure in the rare case of a U.S. company with offices in the EU that only employs U.S. persons and only transfers their employee data to the U.S. The mere fact that the firm is a U.S. company does not immunize it from § 702 targeting procedures affecting foreign national employees located abroad.

Furthermore, Raul's proposal excludes EU companies that provide goods or services to the U.S. and use SCCs to transfer personal data about EU employees or customers to U.S. firms for various purposes. Nothing in § 702 prevents the U.S. government from scanning or collecting EU vendors' communications if they meet the relevant targeting criteria. Raul's omission of EU firms is glaring in view of a recent estimate that "85 per cent of companies operating in Europe use SCCs" and "the vast majority (75 per cent) [are] headquartered in the EU."[187] That telling statistic indicates the need for a more comprehensive response to the EDPB.

IV. AN ALTERNATIVE MODEL: EXPORT CONTROL LAW

For the reasons indicated above, the six-step roadmap described in the Final Recommendations solves few problems for data exporters seeking to rely on SCCs. But this roadmap is not the only possible model for delegating compliance tasks to data exporters. In this section, we highlight the problems with the roadmap and (in the next section) offer some ideas for improvements by comparing the data export process sketched out above with the U.S. export control regime. This requires a short digression that we think will yield some useful insights. We focus on U.S. export controls due to our familiarity with them while noting that European controls on "dual-use items" (i.e., goods, technology, or software having both civilian and military applications) are very similar in most relevant respects due to European and U.S. participation in multilateral exports regimes as discussed below.

---

[186] 50 U.S.C. § 1881a(a); *see supra* notes __-__ and accompanying text.

[187] Digital Europe et al., Schrems II: Impact Survey Report (2020) (implying that Raul's analysis ignores 64% of all firms using SCCs)..

A. Overview of U.S. Export Control Law

There are multiple reasons for imposing export controls on dual-use items including national security, non-proliferation of weapons of mass destruction, and foreign policy. We are mainly interested in national security controls, which seek to limit foreign access to the most sensitive U.S. weapons and technology. These controls reflect the Cold War assumptions of the Coordinating Committee (CoCom), a multilateral organization formed at the end of World War II by the U.S. and other NATO members to stem the flow of Western technology to the former U.S.S.R., its Warsaw Pact allies, and China.

In the 1990s, CoCom transitioned to the more complex Wassenaar Arrangement (WA), a voluntary export control regime approved in 1996 and currently consisting of 42 members. Its participants agree to control exports and retransfers of items on a list of dual-use goods and technologies and the Munitions List.[188] Although the scope of export controls in participating states is determined by the two WA lists, practical implementation varies from country to country in accordance with national laws and procedures. The WA operates by consensus and therefore tolerates more national discretion among member states than did CoCom, which has lead to conflicts over exports policy to some countries including China. [189] For example, the U.S. recently enacted a law imposing greater restrictions on exports to China of certain "emerging and foundational technologies" (including cybersecurity) considered critical to U.S. national security, even though no consensus on these controls has been reached by the WA countries.[190]

Three government agencies in the U.S, are mainly responsible for overseeing export controls. The Department of Commerce's Bureau of Industry and Security (BIS) controls the export and re-export (to a third country) of dual-use items and less sensitive defense articles under the Export Administration Regulations (EAR) through a system of general licenses and individual validated licenses (IVLs).[191] A general licenses is a self-administered grant of authority to all exporters for certain categories of less sensitive products (including technology and software) to all or most destination, subject to some additional requirements and accountability measures.

Most commercial U.S. exports are shipped abroad under general export licenses, which require no application or prior approval for their use. By contrast, an IVL is a specific grant of authority in the form of a licensing document issued to a particular exporter, authorizing exports of specific items to a particular country of destination and specific end-users and end-uses. Unlike general licenses, IVLs are not self-certifying—BIS must approve and issue a license before any exports are permitted. In addition, the EAR contain ten "General Prohibitions" such

---

[188] *See* The Wassenaar Arrangement, Frequently Asked Questions, https://www.wassenaar.org/about-us/#faq.

[189] *See* Cindy Whang, *Undermining the Consensus-Building and List-Based Standards in Export Controls: What the US Export Controls Act Means to the Global Export Control Regime*, 22 J. INT'L ECON. L. 579 (2019).

[190] *Id.*

[191] *See generally* Part 734 of the EAR.

as exporting or re-exporting a controlled item requiring a license without first obtaining an applicable license; exporting or re-exporting virtually any product to an embargoed country; or proceeding with any transaction with knowledge that an export violation has occurred or is about to occur.

The Department of State regulates the export of items specifically designed for military purposes ("munitions") under a far more restrictive regime requiring firms to register as arms exporters and obtain individual license for all destinations.[192] Many more countries are restricted as compared with Commerce licensing and there are fewer exemptions. Finally, the Department of Treasury administers foreign asset controls or embargoes, which prohibit all financial and trade transactions to embargoed countries, subject to very limited exceptions for humanitarian aid and informational materials.[193]

The licensing requirements for technology subject to BIS controls appear on the Commerce Control List (CCL), which identifies and classifies sensitive dual-use or civilian items as well as some less sensitive defense articles not subject to the State munitions controls that BIS controls for export or re-export. The CCL lists hundreds of commercial items and classifies each of them using a an identifier that indicates various kinds of information such as industrial sector, type of product, and the reason for control. After determining if an item is listed on the CCL and the reasons for control, an exporter must check the Commerce Country Chart (which has entries for about 200 countries) to see if a license is required for exports to that destination.[194]

BIS also organizes countries into four country groups (A, B, D and E) based on particular reasons for control. For example, Country Group A is the least restrictive group and includes key US allies and members of NATO, among others; Country Group B is a catch-all for more restrictive controls; Country Group D covers about 40 countries (including China, Russia and Yemen) that raise national security, nuclear, chemical-biological or missile technology concerns; while Country Group E is the most restrictive and includes countries subject to comprehensive embargoes (Cuba, Iran, North Korea, Sudan, and Syria).[195]

Less sensitive items that are subject to export controls but not specifically listed on the CCL are covered by a catch-all classification known as EAR99. In general, EAR99 items may be exported to most destinations without a license unless a General Prohibition applies. Exporters typically determine for themselves the classifications of dual-use items they wish to export, but they remain responsible for any exports of controlled products without a required license if their classification is in error. If they are uncertain about the proper classification of an

---

[192] *See generally* the International Traffic in Arms Regulations (ITAR), 22 C.F.R. 120 et seq., implementing the Arms Export Control Act of 1976.

[193] The Office of Foreign Assets Controls within the Treasury Department administers various embargo and sanctions regulations (31 C.F.R. Part 500 et seq.) under the International Emergency Economic Powers Act, the Trading with the Enemy Act and a number of laws targeting specific countries.

[194] *See generally* Part 738 of the EAR.

[195] *See generally* Supp. 1 to Part 740 of the EAR.

item, and wish to avoid liability for an erroneous classification, they may apply to BIS for a formal classification. The Steps for using the EAR may be found in Part 732 of the EAR.

In sum, for any given export transaction, firms must determine, 1) which U.S. export controls apply; 2) whether these controls require a license such as an IVL or permit export under a general license, license exception, or other exemption (and if so any applicable conditions or procedures for compliance); 3) prepare and submit appropriate applications for items requiring a license; and, 4) make shipments as authorized by the license while maintaining any required documentation.

B. Comparison of Data Exports and Dual-Use Exports

This oversimplified summary of U.S. export controls[196] allows us to compare the main similarities and differences between the data export regime as developed in the EDPB Recommendations and U.S. dual-use export controls. There are a number of striking similarities. First, like the GDPR, which serves the dual objectives of safeguarding fundamental rights to data protection and the free flow of personal data within the EU, export controls also serve two goals: limiting access to strategic goods and technologies by potentially hostile countries without unduly burdening international trade.[197]

Second, also like the GDPR, which permits data exports to countries that have not received an adequacy determination subject to appropriate safeguards and without requiring any specific authorization from supervisory authorities, BIS controls establish general licenses for exports to many countries without the need for a license application and for which no governmental approval document is issued. Moreover, the notion of "onward transfer" to a third country is mirrored under U.S. export law by the concept of "re-exports" to a third country. Finally, just as the EDPB Recommendations requires data exporter to "assess whether the GDPR transfer tool you are relying on is effective in light of all circumstances of the transfer," so too must exporters determine for themselves whether a proposed export of a dual-use item is eligible for a general license to some or all destinations or requires an IVL. Exporters are responsible for understanding the specific conditions and restrictions of the various general licenses, how they apply to the proposed export, and when the use of such licenses is prohibited.

There are also important differences between the two regimes. To begin with, the adequacy requirement represents a form of unilateral EU law-making,[198] whereas dual-use exports controls arose within a multilateral regime that now covers 41-member states under the

[196] For a comprehensive overview, *see* Benjamin H. Flowe, Jr., Compliance with U.S. Export and Reexport Controls (Nov. 2013), https://bcr.tv/ExportandReexportComplianceGuide_Master_Version_November_2013.pdf.

[197] Of course, there is never (in theory) any conflict between the free flow of data *within* the EU and the protection of fundamental rights since the GDPR ensures an equally high level of data protection in all EU Member States. Rather, conflicts like those that arise in export law only occur when data subjects or DPAs take issue with the adequate safeguards established by a data exporter seeking to legitimize personal data transfers to third countries outside of the European Economic Area.

[198] *See* Anu Bradford, *The Brussels Effect,* 107 NW. U. L. REV. 1 (2012). The GDPR jurisdictions provisions add to this trend. *See* Lynskey, *supra* note __.

WA. Second, the GDPR weighs the free movement of data against a fundamental right, while export controls balance international trade against important government objectives like national security and foreign policy that do not necessarily implicate fundamental rights. Finally, the EDPB Recommendations calls upon data exporters to determine whether public authorities in a *third country* may unjustifiably interfere with the data being transferred. In contrast, dual-use items exporters must determine their obligations under their own *national* laws based on an item's classification, ultimate destination, end-user, and end-use. So this analogy between the two export regimes is by no means perfect.

Nonetheless, for present purposes, the most important difference between the two sets of procedures is that Commerce has designed a licensing system that actually works. It allows exporters to determine their licensing obligations by following prescribed steps and thereby reach a reliable outcome. It takes some effort to learn how to read the CCL but companies that export sensitive dual-use items usually possess the technical expertise to master CCL classifications and utilize the Country Chart to see if the item qualifies for a general license or requires an IVL.

Thus, dual-use export controls are quite practical. They permit self-classification, which promotes efficiency. But they avoid delegating governmental tasks to private firms such as policy decisions about which items are sensitive or which countries raise national security or foreign policy concerns. Governments makes these decisions (as participants In the WA or by applying national discretion) and only delegate to companies the task of applying these policy s to specific export scenarios. Thus, exporters determine their licensing obligations by applying their own expertise to information in their own possession.

The Final Recommendations fail to offer similarly concrete guidance for data exporters. Instead, it requires them to assess foreign surveillance laws, policies, and practices against the abstract terms of the essential guarantees, without identifying more specific factors for deciding if SCCs are appropriate in a given situation. Dual-use export controls provide a risk-based and highly granular assessment methodology for determining whether an export qualifies for a general license. In general, controls classify an export is low-risk if it does not contribute significantly to the military potential of another country or undermine U.S. foreign policy objectives.

In contrast, the Final Recommendations remain ambivalent about the risk-based approach. Where dual-use export controls adopt a permissive licensing approach for exports to allies and other nations, concentrating regulatory resources on exports to restricted and embargoed countries, the Final Recommendations make little effort to differentiate countries on a geopolitical basis. Granted, the Recommendations reference GDPR Article 45(2), which identifies general factors such as "the rule of law, respect for human right and fundamental freedoms" as part of the assessment process. But the naming and shaming of U.S. surveillance law (§ 702 of FISA and EO 12333) suggest that the Board considers data exports to the U.S. as on par with those to Russia or China—countries that maintain surveillance programs manifestly lacking in respect for the rule of law or accountability.

The Board's recommendations are lacking in several other nuances of export control law. Where dual-use export controls draw obvious distinctions among different end-users/end-uses, the Board treats all data importers as similarly situated. Under Step 3 of the Final Recommendations, a data transfer to the U.S. must be analyzed in the same fashion whether it is undertaken by a Google or Facebook or a U.S. firm engaged in a much more modest and mundane business. As already noted, a U.S. manufacturing that operates a sales offices in Europe with mostly U.S. person employees and a single European employee must be treated in an identical fashion to Google when it transfers data to the U.S. because that lone European employee might be targeted under § 702. While the Final Recommendations identify risk-based factors for evaluating foreign law and the effectiveness of supplementary measures, in the end these factors reduce to the binary decision of whether or not the essential equivalency standards are satisfied. That rigid, binary standard conflates firms with fundamentally different business models and radically disparate risks of eliciting U.S. surveillance.

The U.S. export controls capture such nuances, instead of ignoring them. The Commerce Department's dual-use export controls are *permissive*. They allow the export of most ordinary commercial items without a formal approval, while restricting or prohibiting exports of strategic goods and technology based on reasonably clear risk-factors as determined in advance by the government. The State Department's arms controls regime is *restrictive*, requiring a license for all controlled items to any destination, and many license applications are denied. The Treasury Department's asset controls are *prohibitive* and block almost all financial and trade transactions with embargoed countries. Although the Final Recommendations purport to describe a permissive regime that many data exporters may rely upon to transfer data to third countries using SCCs, in fact the Final Recommendations describe a highly restrictive regime that would effectively prohibit or render pointless data transfers to the U.S. in a vast number of cases.

V. BILATERAL COOPERATION

Since the Board has adopted a de facto absolutist stance that provides little or no effective guidance for data transfers to the United States, alternatives are essential. This section and Part VI take up the challenge with a hybrid model. The subject of this section is bilateral cooperation between the EU and third countries. The following section describes new substantive and institutional checks on surveillance in third countries, including the United States.

Bilateral cooperation builds on the insights in the preceding section on U.S. export controls. The export control process permits private firms to determine the propriety of third-country data transfers through multilateral standards embodied in national law. With this in mind, we propose that the Board give due consideration to the practical wisdom of dual-use export controls and revise its own guidance on SCCs and other transfer tools accordingly. Rather than setting out abstract criteria and expecting firms to reach binary decisions about the adequacy of a third country's laws and practices, the EU should offer more concrete guidance. For example, it should create a simple matrix identifying the risks of different classes of data exports. This matrix could utilize the same structure as the CCL—items (data) characteristics, destination, end-user, and end-use—but on a much scaled-back basis.

To move this process along, EU officials—ideally accompanied by member state representatives[199]—should initiate a series of bilateral meetings with officials of importing countries (including the United States). Officials at the meetings would conduct comprehensive reviews of foreign surveillance laws and practices. They would also assess judicial oversight and international commitments.

The meetings would take on several specific tasks to achieve these goals. Officials should, 1) identify the full gamut of an importing country's surveillance laws that permit government access to transferred data; 2) determine what if any categorical legal protections exempt specific end-users/end-use scenarios from the reach of these laws; 3) share information about the actual practices of intelligence agencies, together with company disclosures of various statistics related to government requests for user data, records, or content;[200] and, 4) discuss related issues such as the impact of a wider array of supplementary measures and the role of notification procedures.

For example, imagine an agreement on protocols in which any data exporter that relies on a risk-based assessment of third country access as the basis for data transfers would (except in cases barred by law) receive a notice when a data importer (or service provider) becomes subject to a foreign government access request.[201] This would allow the entity to revoke encryption keys and/or suspend immediately such transfers pending the outcome of the request and a re-assessment of the relevant risks of relying on SCCs to accomplish such transfers. That agreement on protocols would make compliance far more manageable and user-friendly.

An EU-U.S. summit meeting might review a range of surveillance authorities including the Electronic Communications Privacy Act, FISA, statutes authorizing National Security Letters, and administration laws and procedural rules governing subpoenas. This would yield useful information about the likelihood of government access to transferred data depending in part on the nature of the data (electronic communications, financial data, customer information, other business records), the end-user (communications services, financial institutions, manufacturers, medical firms, and so on) and the end-use (private communications vs. commercial transactions).

A more ambitious approach would entail convening a multilateral group of countries to identify and agree upon criteria for understanding "the rule of law" and "respect for human rights

---

[199] Inviting member state officials to participate would help address certain anomalies associated with the EU's mixed authority over national security issues and its unwillingness to factor into its thinking about cross-border data transfers either (1) the actual practices of member state intelligence agencies or (2) U.S. sharing with member states some of the data collected under § 702. See Dep't of Comm. White Paper, *supra* note __.

[200] For a good overview of the information available in transparency reports from ten major U.S. internet firms, *see* Eleni Kosta and Magdalena Brewczyńska, *Government Access to User Data in* TOWARDS MORE MEANINGFUL TRANSPARENCY REPORTS IN REGULATING INDUSTRIAL INTERNET THROUGH IPR, DATA PROTECTION AND COMPETITION LAW (R. Ballardini, P. Kuoppamäki & O. Pitkänen, eds., 2019).

[201] In the Implementing Decision, the Commission addresses the obligations of the data importer in case of access by public authorities including notification of the data exporter by the data importer. *See* Implementing Decision, *supra* note __, at Clause 15.

and fundamental freedoms" in the context of surveillance law.[202] Reaching consensus on these criteria would in turn facilitate reviews of third country foreign surveillance laws as discussed above and possibly incentivize legal reforms in countries that fall short of these multilateral standards. A multilateral approach would also enable the EU (or any participant acting on its own authority) to create a listing of countries analogous to the BIS's Country Groups.

An EU country list classifying destinations using risk-based criteria would both resolve the delegation problem as discussed above and facilitate risk-based assessments of data transfers. One possible classification might look like this: Country Group A (the twelve countries that have received favorable adequacy determinations and temporarily (pending a future decision) the UK[203]); Country Group B (the dozen or so countries seeking adequacy decisions or that have enacted strong data protection laws premised on the GDPR—e.g., South Korea (in "Tier 1" because adequacy talks are ongoing) and Argentina, Brazil, Chile, Hong Kong, India, the Philippines, Singapore, South Africa and Taiwan (in "Tier 2"); Country Group D (including the U.S. and other countries with divergent privacy laws but a strong commitment to the rule of law and respect for human rights and fundamental freedoms, with various tiers as appropriate); and Country Group E (including China, Iran, North Korea, Russia, and other countries with weak privacy laws under EU standards and/or a weak commitment to the rule of law and respect for human rights and fundamental freedoms).

With this geopolitical mapping in place, the EU might then consider adopting policies under which data exporters transferring data in low- or medium-risk scenarios to importers in Country Group A would enjoy a "presumption of compliance" and ditto for transfers in low-risk scenarios only to the highest tiers of Country Group D, while all transfers to importers in Country Group E would operate under a "presumption of denial" barring an extraordinary showing of additional positive factors. Ideally, a simple matrix modeled on the CCL Country Charts and combining all of the factors discussed above would then allow data exporters to determine the risk level of a data export based on the various risk factors and the country of destination. Again, this approach would make compliance far more straightforward.

VI. NEW U.S. INSTITUTIONAL AND SUBSTANTIVE CHECKS

This section proposes U.S. statutory and administrative measures that could address the *Schrems II* court's concerns as a complement to the risk assessment described above. The first subsection discusses the CJEU's demand for independent review of EU persons' privacy complaints, proposing a new Algorithmic Rights Court (ARC). Following that discussion, this Part argues for amendment of § 702's "foreign affairs" surveillance authority, a statutory

[202] For one attempt at identifying such criteria, *see* Rubinstein et al., *supra* note __, Table 1.3 (identifying fourteen normative factors).

[203] The Brexit Trade and Cooperation Agreement allows data transfers from the EEA to the UK to continue without the use of SCCs or additional restrictions until May 1, 2021 (which, barring objections, will automatically extend until July 2021), or until the European Commission makes a final ruling on the matter of data transfers between the UK and EEA.)

presumption against surveillance of foreign employees of U.S. companies working abroad, and codification of PPD-28.

A. Independent Review

Under the CJEU's jurisprudence, independent review is crucial. Independent review, as the U.S. Supreme Court noted in *Keith*, keeps the executive branch honest.[204] It ensures that review will not be perfunctory or pro forma; rather, it will be serious and substantive. In its *Keith* decision requiring a warrant for domestic national security searches, the Supreme Court found that nothing less than judicial review would suffice in domestic national security surveillance. *Schrems II* requires a robust review for EU persons' privacy complaints. That in turn requires a reviewer who is impervious to the pressures of the political arena.

In the U.S. system, ensuring that level of independence entails review by one of two possible tribunals. Review can be available from a federal court presided over by a judge with lifetime tenure under Article III of the U.S. Constitution.[205] In the alternative, review can be available through a multimember bipartisan administrative body whose members can be dismissed only "for cause."

1. Creating an Algorithmic Rights Court

To address institutional concerns about the adequacy of U.S. privacy protections raised in *Schrems II*, Congress should create a new court, the Algorithmic Rights Court (ARC). The ARC would hear individual complaints about privacy, as the *Schrems II* court required. In that connection, the ARC could review search criteria under both FISA § 702 and EO 12333. The ARC could also field complaints on related issues, including the brittleness, bias, and lack of intelligibility of many current algorithms used in credit, employment, government benefits, and housing.

The ARC, like the FISC, would be a federal court comprised of Article III judges with lifetime tenure. That would guarantee the ARC's independence from political pressure. In addition, the FISC would have staff that would supply legal and technical expertise.

As an added check on government, the ARC would have a full-time public advocate. The public advocate would expand on the role that *amici curiae* currently play with the FISC. Like *amici*, the public advocate could push back against the government's legal and technical claims. In addition, Congress would empower the public advocate to bring its own cases on the public's behalf against excessive, erroneous, or biased surveillance.[206]

---

[204] United States v. United States District Court, 407 U.S. 297 (1972).

[205] *See* U.S. Const., art. III, § 1.

[206] *See* Andrew Weissman, *The Need for Increased Amicus Role in the FISA Process*, Just Security (Jan. 14, 2020), https://www.justsecurity.org/68047/the-need-for-increased-amicus-role-in-the-fisa-process/; *see also* Marty Lederman & Steve Vladeck, *The Constitutionality of a FISA "Special Advocate"* (Nov. 4, 2013), available at http://justsecurity.org/2013/11/04/fisa-special-advocate-constitution/ (asserting that public advocate would be

To see how the ARC would work in practice, consider a case in which an EU resident—who we'll call Josef M.—filed a complaint about erroneous surveillance under § 702. In a classified proceeding, the ARC and the public advocate would require the government to submit any and all selectors relevant to Josef M.'s emails, texts, social media posts, and phone calls. With the public advocate's help, the ARC would analyze the selectors to determine if they were adequately tailored to provide foreign intelligence information, such as evidence of espionage, sabotage, or international terrorism. If the selectors were not so tailored, the ARC would impose a remedy, requiring the government to modify its selectors. In addition, the ARC could require the government to submit all selectors—or a random sample thereof—to both the ARC and the public advocate for a specified period. The ARC would then communicate to Josef M. that it had resolved his complaint. The court's opinion could include a statement of reasons, although a public accounting might be both general and heavily redacted to avoid disclosure of intelligence sources and methods.

Of course, the ARC could also reach a different result in Josef M.'s case. Having examined submissions by the government, the court could determine that selectors were adequately tailored to produce foreign intelligence information. Alternatively, the court could determine that Josef M. was unduly concerned about U.S. surveillance, since in fact the government was not using selectors that collected Josef M.'s communications. Here, the ARC's statement to Josef M. might have to be even more terse than in the situation described above, in which the ARC found Josef M.'s complaint to be meritorious. To avoid tacitly or actively giving away intelligence sources and methods that might be useful to U.S. adversaries, the court might simply say that it had not found in Josef M.'s favor, without providing further explanation.[207]

The ARC might encounter constitutional issues, but it would have sound responses. One problem here might be the courts' view that foreign surveillance with no U.S. link is a purely executive function linked to the President's role as commander in chief. This would be particular problem for a tribunal addressing privacy complaints prompted by EO 12333. However, Congress can regulate foreign surveillance under the commerce power, given the effects that transatlantic mistrust would have on international business and trade. In addition, Congress could probably resort to the war power and to Congress's power to regulate "captures," which might extend beyond persons and tangible things to collection of data. Moreover, a legislative framework on foreign surveillance also would have a prophylactic effect on surveillance of U.S. persons. Congress could plausibly argue that some check on foreign surveillance was necessary to prevent the executive from using foreign surveillance pretextually to target U.S. citizens and LPRs. The ARC would be vigilant about such pretexts and impose relief to preclude their growth or recurrence.

---

constitutional). On reform efforts generally, see Julian Sanchez, *A Chance to Fix FISA*, Just Security (March 27, 2020).

[207] The United Kingdom's Investigatory Powers Tribunal (IPT) makes a similar determination. *See Kennedy v. United Kingdom*, App. No. 26839/05, 52 Eur. Ct. H.R. 207, 232 (2010). The European Court of Human Rights has upheld this procedure. *Id*. (noting when it finds that a complaint is not meritorious, the IPT informs the complainant that "no determination has been made in his favour").

Another problem arises with Article III of the Constitution, which regulates federal courts. Under Article III, courts can only adjudicate particular cases or controversies. The Supreme Court has held that fears of intrusive surveillance—even those held by U.S. persons—lack the concreteness and particularity that are necessary to allege an "injury in fact." Without an injury in fact, a complaint would not allege a case or controversy necessary to support federal jurisdiction. However, there are answers to the Article III concern. The Supreme Court has signaled that Congress should receive a measure of deference in determining that certain statutory claims supply the requisite injury in fact.[208] Moreover, courts even before the Constitution's enactment acknowledged that law enforcement could apply *ex parte* for a warrant authorizing surveillance. Providing recourse to private parties who feared surveillance would merely balance out that long-established tradition. In addition, courts could reasonably require that a complainant show some articulable basis for a belief that she had been subject to abusive surveillance. That showing, if required in legislation enacted by Congress, might well be sufficient to overcome Article III concerns. Participation by the government on the other side, arguing that surveillance was appropriate, would also blunt Article III arguments.

The ARC's proceedings would address the *Schrems II* court's institutional and procedural concerns. Judges of the ARC would be independent. In addition, the *Schrems II* court's concern about fair procedures would be vindicated by the creation of a public advocate who would counter the government's arguments. The government's legitimate security concerns would be protected by a requirement that both ARC personnel and the public advocate have the requisite security clearance. Creating a tribunal like the ARC would entail a political commitment from both the Congress and the executive branch. But that commitment would have substantial pay-off in the good will of EU bodies.

2. An Independent Executive Branch Agency

If the political will for such a bold move was lacking, the United States could address independence through an executive branch agency. To hear EU persons' privacy complaints, Congress could establish a multimember bipartisan administrative body whose members can be dismissed only "for cause."

The Supreme Court has recently limited Congress's power to protect heads of executive branch agencies from presidential dismissal.[209] According to the Supreme Court, the President's power to dismiss senior executive branch officials reinforced the Framers' plan for an "energetic executive" who would balance out the power that the Framers feared in the legislative branch.[210] However, Chief Justice Roberts, writing for the Court, observed that historical practice has

[208] Spokeo, Inc. v. Robins, 578 U.S. 330 (2016).

[209] Seila Law LLC v. CFPB, 140 S. Ct. 2183 (2020) (citing Article II grounds in striking down a portion of the legislation creating the Consumer Financial Protection Bureau with a single director whom the President could only dismiss "for cause").

[210] *Id.* at 2203 (citing The Federalist No. 70 (Alexander Hamilton) at 471).

created an exception for a bipartisan "body of experts" within the executive branch such as the Federal Trade Commission (FTC) exercising quasi-judicial or quasi-legislative powers.[211]

Buttressed by historical practice, a multimember body may decide contested factual and legal questions raised by implementation of federal regulatory statutes and also provide reports to Congress. Such bodies typically feature staggered terms exceeding four years that allowed members to gain expertise and permit each successive president of either political party to nominate members of the body. The "for cause" protection from dismissal extended to members—which requires some showing of specific transgressions by the official—gives the heads of such multi-member entities a modicum of shelter from the gusts swirling in the political arena.[212]

A future agreement may require legislation that will set up a new multi-member body to ensure adequate levels of independence. Alternatively, Congress could establish such review within an existing multi-member body such as the FTC. The FTC already regulates privacy through settlements with U.S. firms whose negligence has led to massive data breaches.[213] The FTC has also played a role in Privacy Shield and its predecessor, Safe Harbor, by vetting the procedures of U.S. firms participating in transatlantic data transfer agreements. Because of this experience, the FTC would be a logical place for EU privacy complaints.

Alternatively, the U.S. Privacy and Civil Liberties Oversight Board (PCLOB) could take on this task.[214] The PCLOB has produced exceptionally comprehensive and insightful reports on U.S. surveillance, including reports on the U.S.A. Freedom Act and § 702. The skill-set of its members and staff certainly equip it for performing independent review. Indeed, EU bodies regularly cite the PCLOB as an example of accountability within the U.S. surveillance system—accountability that EU entities otherwise often find lacking in the United States. In addition, the PCLOB already has a structure that would be acceptable under Article II of the U.S. Constitution. It is an independent agency whose bipartisan complement of members serve staggered terms and are removable only for cause. Moreover, the Board also has clearance to receive sensitive information about U.S. surveillance.

However, there would also be down-sides to the PCLOB's assumption of this new role. The Board would need to scale up its staffing considerably to cope with the expected volume of EU persons' privacy complaints. In addition, the PCLOB would probably need statutory and regulatory changes to set up a formal adjudicative process. This juristic turn might not fit well the Board's current reporting duties. For example, members who had staked out particular positions on U.S. surveillance in reports might not be ideal adjudicators for complaints raising

---

[211] *Cf. id.* at 2199.

[212] *See also id*. at 2204 (implying that multi-member body with officers having staggered terms mitigates harm to executive functions of permitting removal of officers only for cause).

[213] *See* FTC v. Wyndham Worldwide Corp., 799 F.3d 236 (3d Cir. 2015).

[214] *See* Kenneth Propp & Peter Swire, *After Schrems II: A Proposal to Meet the Individual Redress Challenge*, Lawfare, Aug. 13, 2020 (suggesting that the PCLOB undertake to review EU privacy complaints, or that privacy and civil liberties officers within U.S. intelligence agencies perform this function).

similar issues. Members with preexisting positions might—rightly or wrongly—be perceived as lacking the objectivity and detachment necessary for impartial adjudication. This perceived conflict might rekindle the mistrust that already plagues EU views of the U.S. system.

3. Summary

As an independent court, the ARC would most effectively accommodate the CJEU's concerns. The FISC could also handle this role. An independent executive branch agency would be useful, although it would lack the gold standard of lifetime tenure that only the federal judiciary can provide. The PCLOB might fit the bill in this respect, although that transformation would have significant opportunity costs for the PCLOB's other important work.

B. Substantive Statutory Moves

The institutional pivot toward independence should accompany substantive changes. These would include codification of PPD-28, a presumption against collection of the communications of U.S. firms' EU employees located abroad, and revision of FISA's "foreign affairs" prong.

1. Codification of PPD-28

PPD-28 is a useful constraint that limits U.S. surveillance to certain discrete areas, including espionage, sabotage, and terrorism. However, a subsequent president can revoke the measure, leaving U.S. surveillance unconstrained. As a practical matter, PPD-28 has shown surprising resilience. It is notable that President Trump, despite all of his departures from his predecessors, left PPD-28 intact. However, to ensure PPD-28's permanence, Congress should codify its protections.

2. A Statutory Presumption Protecting U.S. Firms' EU Employees

Congress should codify the practical protections for U.S. firms abroad that now exist in risk-based analysis. At the moment, as we have discussed, it is highly unlikely as a practical matter that U.S. intelligence capabilities will reach the kind of intra-company transfers that comprise the range of processes covered by transatlantic agreements such as Privacy Shield. As we have explained, targeting of a U.S. company's communications would be unlawful under § 702, just as targeting a U.S. person would be unlawful.[215] Congress can underscore this practical protection by expressly codifying a statutory presumption against targeting of any foreign national *employee* of a U.S. company abroad.

This presumption would dovetail with U.S. security. U.S. companies carefully vet their own employees both here and abroad. The risk that such employees would be engaged in activities that would present a danger to the United States or its allies seems small. Furthermore,

[215] *See* Raul, *supra* note __.

as part of the statutory presumption against targeting such employees, Congress could provide for overriding that presumption upon a showing to the FISC or another independent decisionmaker that probable cause existed to believe that the individual in question was engaged in activities that imperiled U.S. security. That individualized showing of probable cause would meet the *Schrems II* requirements of necessity and proportionality.

3. Revising the FISA "Foreign Affairs" Prong

Congress should also modify the "foreign affairs" prong of § 702. That provision allows the U.S. to conduct surveillance "with respect to a foreign power or foreign territory" of any matter concerning the foreign affairs of the United States.[216] Critics of U.S. surveillance have long pointed to the foreign affairs prong of § 702 as giving U.S. surveillance officials wide discretion in their choice of targets. In practice, the foreign affairs prong probably has a narrower scope, focusing on foreign companies that have engaged in anticompetitive practices against U.S. firms and on foreign diplomats advancing positions in international bodies such as the United Nations. The intelligence that the U.S. has collected in such situations has sometimes been useful. However, Congress should have a candid and robust debate about whether such intelligence is worth the harm to overall U.S. interests engendered by the distrust that the foreign affairs prong of § 702 has triggered.

After such a debate, Congress could fashion a more precise substitute to the foreign affairs prong that would focus on collecting intelligence regarding foreign nationals' evasion of U.S. sanctions—an area already flagged in PPD-28—or by foreign officials' engaging in corrupt practices such as taking bribes from U.S. or other firms. This change would limit U.S. surveillance, and perhaps hinder acquisition of some useful intelligence. However, the change would be a powerful signal that the U.S. officials are prepared to make sacrifices for the greater good served by preserving cooperation with the EU. The trade-off seems eminently worthwhile.

C. A Reprise on Article 49 Derogations

Adding to the elements in this hybrid approach, consider the combination of the risk-based assessment, U.S. statutory reforms, and Article 49 derogations. Particularly in the intra-firm space, Article 49 derogations based on consent or performance of a contract might derive additional credibility from the hybrid approach suggested in this law review Article. A company would be both unwise and irresponsible in relying solely on Article 49, even for an intra-firm transfer. However, in tandem with reasonable safeguards on privacy—albeit safeguards that are not absolutely foolproof—such a transfer might withstand scrutiny. The risk-based approach in this law review Article could also be helpful.

An example illustrates the point. Suppose a reasonable data controller—the chief privacy officer of a firm— views a particular transfer for contractual purposes as unlikely to attract intelligence community scrutiny. That assessment might also weigh in favor of permitting the

[216] 50 U.S.C. § 1801(e)(2).

transfer. As this law review Article notes in recommending U.S. reforms, a statutory presumption against surveillance of a foreign national employee of a U.S. firm abroad would also help with compliance. Perhaps none of these factors alone would meet with favor. However, a hybrid of all of these elements might constitute the practical safeguard against intrusion that the GDPR requires.

CONCLUSION

The CJEU's decision in *Schrems II* poses significant challenges for transatlantic data transfers. In finding that transfers to the United States did not provide adequate privacy safeguards, *Schrems II* cited the lack of necessity and proportionality in U.S. surveillance—particularly surveillance under EO 12333 and FISA § 702—and the lack of independence of mechanisms for reviewing EU persons' privacy complaints. The principal task for stakeholders in transatlantic data transfers is addressing the CJEU's concerns in a constructive manner.

Based on the current state of debate, it is easy to identify flaws in current responses to *Schrems II*, but it is more difficult to find a way forward. Some in the United States have focused either on critique or denial. They have found fault with the CJEU's ruling, suggesting with some basis that the court did not fully acknowledge checks and balance within U.S. law, including the more robust role of the FISC in the wake of Edward Snowden's revelations. Others have resorted to the definitional games that lawyers like to play, denying that entities in the EU transferring data to the United States are even *subject* to U.S. surveillance. Neither critique nor denial constitutes an adequate response to the CJEU's landmark decision.

At the same time, some EU entities, such as the EDPB, have issued absolutist pronouncements that would effectively ban transatlantic data transfers. Considering the future of SCCs, the EDPB's guidelines took a rigid, binary approach. Under the rubric of technological safeguards, the EDPB's recommendations require encryption that would preclude cloud providers from monitoring data transfers for cyber threats. This highly restrictive approach would sacrifice data security and long-term privacy goals on the altar of formal privacy protections.

Navigating between the shoals of critique, denial, and absolutism, this paper outlines a hybrid model that weds a concrete risk-based approach to proposals for new institutional and substantive checks on U.S. surveillance. Borrowing from the graduated structure of U.S. export controls, the paper suggests a graduated model of risk analysis for data transfers. In addition, the paper proposes lodging independent review of EU persons' privacy complaints in a new independent court—the ARC—or an independent executive agency whose members have "for cause" protection against dismissal. On the substantive front, the paper argues for codification of PPD-28, a presumption against collecting the communications of EU persons working for U.S. firms abroad, and revising FISA's "foreign affairs" prong. Article 49 derogations can also play a role, both standing alone and even more persuasively in combination with the other elements of the hybrid model.

The hybrid model may not satisfy all audiences for the continuing drama of transatlantic data transfers. Denial and absolutism will always have acolytes. But the hybrid model

acknowledges the core insights in *Schrems II* while enabling essential economic activity. That is a scenario worth pursuing on both sides of the Atlantic.