University of Miami International and Comparative Law Review

Volume 29 | Issue 2 Article 6

5-19-2022

Big Data, Both Friend And Foe: The Intersection Of Privacy And Trade On The Transatlantic Stage

Gabrielle C. Craft
University of Miami School of Law

BIG DATA, BOTH FRIEND AND FOE: THE INTERSECTION OF PRIVACY AND TRADE ON THE TRANSATLANTIC STAGE

*Gabrielle C. Craft**

ABSTRACT

This Note analyzes the data privacy protection initiatives implemented by the European Union and the United States and their effects on international trade. As technology develops, the feasibility of data collection increases, allowing for the collecting of inconceivable amounts of data information. Consequently, this data includes personal information, thus implicating privacy concerns and the need for data privacy protection regulations. Data privacy focuses on the use and governance of personal data and how the data is gathered, collected, and stored. In 2018, the European Union enacted the General Data Protection Regulation (GDPR), which sets out highly stringent standards for how organizations conducting business with European Union citizens may handle their data. While the United States lacks an all-encompassing data-protection law similar to the GDPR, the likelihood of federal implementation of such regulation is growing. Due to the tech industry's exponential growth, data privacy regulations have had trouble keeping pace. Nevertheless, data privacy protection is more necessary than ever. The discrepancies in data privacy regulations gravely affect international business relationships governed by the different regulations. This Note discusses the affects, benefits, and possible solutions to these issues.

* J.D. Candidate, Class of 2022, University of Miami School of Law; B.S. 2017, Florida State University.

I. INTRODUCTION TO DATA PRIVACY

The Universal Declaration of Human Rights lists privacy as a fundamental human right to be achieved by all people and all nations.[1] The right to privacy is a right many nations hold to the utmost importance. However, the cherished right to privacy is under siege as the rise of big data and technological growth. To fully appreciate its significance, this topic requires an understanding of the historical development of big data and its potential benefits and costs.

Merriam-Webster dictionary defines "data" as "factual information (such as measurements or statistics) used as a basis for reasoning, discussion, or calculation."[2] In this context, data has been around since at least the creation of the cuneiform script in Mesopotamia circa 3200 BC.[3] Over time, humans' ability to develop data grew, from phonetic signs to the alphabet to the printing press. Now, technology has allowed for instant record keeping. No longer are most records kept in hard-copy format; most records are now

[1] G.A. Res. 217 (III) A, Universal Declaration of Human Rights (Dec. 10, 1948), https://www.ohchr.org/EN/UDHR/Documents/UDHR_Translations/eng.pdf.
[2] *Data*, MERRIAM-WEBSTER, https://www.merriam-webster.com/dictionary/data (last visited Jan. 14, 2021).
[3] Denise Schmandt-Besserat, *Evolution of Writing*, INT'L ENCYCLOPEDIA OF THE SOCIAL & BEHAVIORAL SCIENCES 761 (James D. Wright ed., 2d ed. 2015).

created, disseminated, and stored digitally, making data collection more effortless than ever.

Enabled by technology, the growth of data collection multiplied extraordinarily. To illustrate this growth, in 2010, data scientists estimated that the digital universe consisted of **2 exabytes**[4] (EB).[5] In 2020, data scientists estimate that the digital universe consisted of **64,200 EB** of data.[6] Further, by 2025, experts estimate the digital universe will consist of **181,000 EB**.[7] About 463 EB of data will be generated *each day* as of 2025.[8] As such, more data will be produced in *five days* than the entire amount of data that existed in 2010.[9] For a physical representation, the United States' Library of Congress contains 15 terabytes (TB).[10] One EB is the equivalent of one million TB.[11] By 2025, 463 EB of data, equivalent to about thirty-one *billion* Libraries of Congress, will be created every twenty-four hours. From this rapid growth emerged the term "big data."

Although big data poses serious privacy concerns[12], it also has significant benefits for society's social and economic development. Academic and business communities benefit from the usage of big data, which yields innovative insights, products, and services.[13] Big

---

[4] One gigabyte is around 64,782 pages of a Word document. After the GB comes the terabyte, petabyte, exabyte, zettabyte, and yottabyte. For example, 463 EB, the projected daily growth of the digital universe by 2025, converted into gigabytes (GB) would equal 463,000,000,000 GB, an unfathomable amount of data. *See How Many Pages in a Gigabyte?*, LEXISNEXIS, https://www.lexisnexis.com/applieddiscovery/lawlibrary/whitepapers/adi_fs_pagesinagigabyte.pdf.

[5] Arne Holst, *Amount of data created, consumed, and stored 2010–2025*, STATISTA (June 7, 2021), https://www.statista.com/statistics/871513/worldwide-data.

[6] *Id*.

[7] *Id*.

[8] Jacquelyn Bulao, *How Much Data Is Created Every Day in 2021?*, TECHJURY (Jan. 4, 2022), https://techjury.net/blog/how-much-data-is-created-every-day/#gref.

[9] Holst, *supra* note 5.

[10] Catherine Armitage, *Optimism shines through experts' view of the future*, SYDNEY MORNING HERALD (Mar. 24, 2012, 3:00 AM), https://www.smh.com.au/national/optimism-shines-through-experts-view-of-the-future-20120323-1vpas.html.

[11] Patrick Thomas, *Defining an Exabyte*, BACK BLAZE (Mar. 23, 2020), https://www.backblaze.com/blog/what-is-an-exabyte/.

[12] *See* discussion *infra* at 5–8.

[13] Wendy Arianne Günther et al., *Debating big data: A literature review on realizing value from big data*, 26 THE J. OF STRATEGIC INFO. SYS. 191, 191 (2017).

data has been instrumental in social improvements in education, healthcare, and public safety and security. Furthermore, the economic value of data includes employment and business growth, productivity, and consumer surplus.[14]

Based on an analysis of education literature, if schools use data sources in the same way that businesses do, public schools would have a greater understanding of their students as individuals and how best to help them succeed.[15] Data would give school districts the ability to analyze the strengths and weaknesses of each school and teacher and give them the ability to make informed decisions based on "evidence provided through the analysis of all available digitized sources."[16] Data analysis can provide schools with the opportunity to customize education and meet the needs of every student.[17] For example, studies have shown that big data can find "repetitive patterns of failure or success" which allows teachers to "solve the former and promote the latter."[18] Additionally, by analyzing "what [the students] ask, what they look for, what doubts they have, the deadlines they meet or do not meet, their normal delivery format, the way they present the information, and their learning style" data can tailor a personalized education plan to ensure academic success.[19]

Similarly, in the healthcare industry, data "hold[s] the promise of supporting a wide range of medical and healthcare functions, including among others clinical decision support, disease surveillance, and population health management."[20] For example, big data has helped to minimize the spread and aided in understanding and creation of the COVID-19 vaccine.[21] The public safety and security

---

[14] *Id*. at 191–92.
[15] Thomas G. Cech, et al., *Applying Business Analytic Methods To Improve Organizational Performance In The Public School System*, AMERICAS CONF. ON INFO. SYS. 2015 PROC. 1, 9 (June 26, 2015).
[16] *Id*. at 9.
[17] *Id*. at 10.
[18] Julio Ruiz-Palmero et al., *Big Data in Education: Perception of Training Advisors on Its Use in the Educational System*, 9 SOC. SCI. 53, 53–54 (Apr. 15, 2020).
[19] *Id*. at 55.
[20] Wullianallur Raghupathi & Viju Raghupathi, *Big data analytics in healthcare: promise and potential*, 2 HEALTH INFO. SCI. AND SYS., no. 3, Feb. 7, 2014, at 1, 1.
[21] Abid Haleem et al., *Significant Applications of Big Data in COVID-19 Pandemic*, 54 INDIAN J. OF ORTHOPEDICS 526, 526 (2020).

industry also benefits from big data. "Governments, for instance, can use big data to, 'enhance transparency, increase citizen engagement in public affairs, prevent fraud and crime, improve national security, and support the wellbeing of people through better education and healthcare.'"[22] These types of benefits not only directly affect the individual but society as a whole through "employment growth, productivity, and consumer surplus."[23]

Beyond consumer value, big data also has business and economic value "that can be measured through an organization's increase in profit, business growth, and competitive advantage resulting from big data adoption."[24] Big data increases efficiency in business by "optimizing supply chain flows; setting the most profitable price for products and services; selecting the right people for certain tasks and jobs; minimizing errors and quality problems; and improving customer relationships."[25] However, these substantial benefits come at the cost of privacy issues. Who sees all this data collected? What do they do with it? Do they share this data with others? Are they keeping this information secure from potential criminals?

One of the biggest concerns with the collection of data is the threat of identity theft. Identity theft has topped FTC's Annual Consumer Complaints for 15 years up until 2015.[26] Only recently replaced by imposter scams and debt collection, identity theft is still one of the most common issues faced by consumers today.[27] In 2020 alone, the FTC reported $3.3 billion in total fraud losses—an increase of nearly $1.5 billion over 2019.[28] "Identity theft occurs when someone

---

[22] Günther, *supra* note 13, at 191 (quoting Kim Gang-Hoon, et al., *Big-data applications in the government sector*, 57 COMMC'NS OF THE ACM 78, 81 (2014)).
[23] *Id*. (quoting Claudia Loebbecke & Arnold Picot, *Reflections on societal and business model transformation arising from digitization and big data analytics: A research agenda*, 24 J. OF STRATEGIC INFO. SYS. 149 (2015)).
[24] *Id*. at 192.
[25] *Id*.
[26] *FTC Release Annual Summary of Consumer Complaints*, FEDERAL TRADE COMMISSION (Mar. 1, 2016), https://www.ftc.gov/news-events/press-releases/2016/03/ftc-releases-annual-summary-consumer-complaints.
[27] *Id*.
[28] FEDERAL TRADE COMMISSION, CONSUMER SENTINEL NETWORK DATA BOOK 2020 (January 2020).

poses as another person by using that person's personal information without his or her permission."[29] Companies that store large amounts of data become targets for hackers seeking to steal personal and financial information. Criminals use stolen identities for a range of reasons. From using credit card information to influencing elections, identity theft is a severe problem in big data. For example, Russian operatives influenced the 2016 presidential election through stolen identities that allowed them access to United States based servers and open United States bank accounts and PayPal accounts to purchased Facebook ads and "buttons flags, and banners" for political rallies.[30] These operatives also used these stolen identities to pose as Americans on United States social media accounts.[31]

Who are these third-party companies that store data, and what do they do with all this information? As data grew, so did many organizations' need for a third-party to manage data. Enter: data brokers. Data brokers collect, store, package, and sell data to other businesses for profit.[32] The largest companies in this industry gross annual revenues in the billions.[33] Data brokers collect information and sell it to other companies that find this information helpful to their business.[34] Just one example of a data broker transaction is when a political party buys information that is statistically indicative of an individual's political affiliation in the hopes of targeting potential supportive voters. A major concern raised by data brokers' existence is that the majority of consumers have no idea that these covert companies are collecting their information.

> "In the world of data brokers, you have no idea who all has bought, acquired or harvested information about you, what they do with it, who they provide it to, whether it is right or wrong or how much money is

[29] JOHN T. SOMA, PRIVACY IN A NUTSHELL 338 (2nd ed. 2014).
[30] SUSAN ARIEL AARONSON, DATA IS DANGEROUS: COMPARING THE RISKS THAT THE UNITED STATES, CANADA AND GERMANY SEE IN DATA TROVES 6 (Ctr. for Int'l Governance Innovation (2020).
[31] *Id*.
[32] SOMA, *supra* note 29, at 369.
[33] *Id*.
[34] *Id*.

> being made on your digital identity. Nor do you have the right to demand that they delete their profile on you."[35]

Data brokers create privacy concerns because they are an easy target for criminals to acquire massive amounts of information by hacking into one data broker database. Additional privacy concerns include how these companies are collecting, using, and selling personal information.

Another prominent concern is how much control governments can assert using the information they collect from big data. When it comes to governments' use of data collection, governments' amount and access were unclear until the Snowden revelations. In 2014, Edward Snowden, a former NSA employee, blew the whistle on the United States' controversial data collection activity.[36] These disclosures exposed the NSA's unrestricted ability to target individuals, obtain and manipulate information, and control users' internet connection globally.[37] The global community was shaken by the sheer amount of control one country exercised over worldwide information. For example, the NSA collected email contact lists from Yahoo, Gmail, Facebook and Hotmail, tapped into phone calls of world leaders including German Chancellor Angela Merkel, and obtained information from communications and tech companies and forced their silence.[38] The European Court of Justice said such an approach "must be regarded as compromising the essence of the fundamental right to respect for private life, as guaranteed by Article 7 of the Charter [of Fundamental Rights of the European Union]."[39]

---

[35] Kalev Leetaru, *The Data Brokers So Powerful Even Facebook Bought Their Data—But They Got Me Wildly Wrong*, FORBES (Apr. 5, 2018, 4:08 PM), https://www.forbes.com/sites/kalevleetaru/2018/04/05/the-data-brokers-so-powerful-even-facebook-bought-their-data-but-they-got-me-wildly-wrong/#112ea6fc3107.

[36] *Edward Snowden: Leaks that exposed US spy programme*, BBC NEWS (Jan. 17, 2014), https://www.bbc.com/news/world-us-canada-23123964.

[37] *Snowden Revelations*, LAWFARE, https://www.lawfareblog.com/snowden-revelations (lasted visited on Oct. 26, 2020).

[38] *Id*.

[39] Paul M. Schwartz, *Global Data Privacy: The EU Way*, 94 N.Y.U. L. REV. 771, 800 (2019) (citing Case C-362/14, Schrems v. Data Prot. Comm'r, ECLI:EU:C:2015:650

Although this information signals a need for reform in the United States' privacy law, even the most ridged opposers of data collection do not seek to end all data collection.[40] Mainstream reform proposals "would require that the data be stored by those entities who collected it (e.g., telecommunications providers), or other non-governmental third parties, with the government only authorized to access the data upon a more specific, individualized showing of relevance."[41] The Snowden disclosures exhibited how much control just one government can have over massive amounts of information. Nevertheless, even a worst-case-scenario could not entirely negate the benefits and need for big data.

This Note will take a business-oriented approach, assessing ways in which businesses can balance big data benefits while limiting their liability under domestic and foreign privacy law. By bridging the gap between international trade law and privacy regulations, this Note will explain the interaction between these fields and what it means for international business. Specifically, this Note will address one of the most precarious relationships between the European Union and the United States. Data transfers between the United States and European Union are imperative to maintaining this $7.1 trillion economic relationship.[42] Sustaining this relationship requires a balance of adequate privacy protections that do not hinder business relations.[43]

Part II of this Note will examine the relationship between privacy and trade via cross-border data regulations and discrepancies between European Union and United States privacy regulations. Part III will discuss the historical and current issues posed by data privacy

---

¶ 94 (Oct. 6, 2015), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62014CJ0362).

[40] Stephen I. Vladeck, *Big Data Before and After Snowden*, J. NAT'L SEC. L. POL'Y 333, 335 (2014).

[41] *Id*.

[42] William Alan Reinsch & Isabella Frymoyer, *Transatlantic Data Flows: Permanently Broken or Temporarily Fractured?*, CTR. FOR STRATEGIC & INT'L STUD., (Aug. 31, 2020), https://www.csis.org/analysis/transatlantic-data-flows-permanently-broken-or-temporarily-fractured.

[43] *Letter from Deputy Assistant Secretary James Sullivan on the Schrems II Decision*, U.S. DEP'T OF COMMERCE (Sept. 28, 2020), https://www.commerce.gov/about/letter-deputy-assistant-secretary-james-sullivan-schrems-ii-decision [hereinafter White Paper Cover Letter].

regulations on transatlantic trade. Part IV will address the interpretations of the problematic *Schrems II* decision and its effects on transatlantic trade. Part V will analyze the suggested actions prescribes by both European Union and United States representatives and proposes ways United States companies can mitigate the negative effects of the *Schrems II* decision.

II. RELATIONSHIP BETWEEN TRADE AND PRIVACY

Data has become a vital part of daily life in every aspect, ranging from global trade to communicating with family. A crucial aspect of facilitating data transfers is the allowance of cross-border data flows that allow information to be shared internationally, connecting the globe to valuable information, social experiences, and economic opportunities. Cross-border commerce is estimated to have contributed hundreds of billions of dollars annually to United States' GDP.[44] Undoubtedly, data transfers are essential to growth and innovation in all sectors of life.[45]

However, the benefits of data are at risk of hinderance by restrictions on cross-border data flows. The rise of big data incited regulations, which each country imposes on cross-border data transfers to protect citizens' privacy. Different countries have taken varying legal approaches to protecting their citizens' privacy. However, the externalities of these regulations inevitably affect the economic trade relationships between countries. Regulations inherently put the burden of cost on private entities who seek to send or process their data abroad, thus affecting international economic relations.[46]

Data privacy regulations are classified by different taxonomies. One of the most popular taxonomies used to classify regulatory approaches is the "default regulatory positions" involving

---

[44] The Invalidation of the EU-US Privacy Shield and the Future of Transatlantic Data Flows: Hearing Before the U.S. Senate Comm. On Com., Sci. and Transp., 116th Cong. 2–3 (2020) (testimony of Noah J. Phillips, Comm'n Fed. Trade Comm'n.) [hereinafter Phillips Testimony].

[45] *Id*.

[46] Martina Ferracane, *Restrictions on Cross-Border data flows: a taxonomy*, 2–3 ECIPE WORKING PAPERS 2 (2017), https://ecipe.org/wp-content/uploads/2017/11/Restrictions-on-cross-border-data-flows-a-taxonomy-final1.pdf.

geographical and organizational approaches.[47] The geographical, or adequacy, approach focuses on the data protection policies of the country of import.[48] This approach analyzes the level of protection afforded by the country of import. Usually, it requires the country of import to provide the same or similar protections to the data subjects as provided by the country of export.[49] European Union regulatory laws are "prime" examples of the adequacy approach.[50] Countries that use the adequacy approach may still allow organizations from countries that do not meet adequacy standards by implementing appropriate safeguards.[51] This is where the geographical and organizational approaches intersect.

The organizational, or accountability, approach focuses on the policies and procedures of specific organizations importing and exporting the data and makes them accountable for the personal data they process.[52] This approach "ensures that the original collector of the personal information remains accountable for compliance with the original privacy framework that applied when and where the data was collected, regardless of the other organizations or countries to which the personal data travels subsequently."[53] Unlike the geographical approach, the country of imports' laws need not satisfy an adequate level of protection. The organizational approach only requires that the importing organization continue to apply the protections applicable under the exporting organization's law.[54] By its nature, the accountability approach is less restrictive compared to the adequacy approach. However, it imposes tremendous compliance responsibilities and potential liabilities on individual organizations. Under this approach, organizations must implement "appropriate privacy policies that are approved by senior management and implemented by a sufficient number of staff; train . . . employees to

---

[47] CHRISTOPHER KUNER, TRANSBORDER DATA FLOWS AND DATA PRIVACY LAW 76 (2013).
[48] *Id*. at 64.
[49] *Id.* at 66.
[50] *Id*.
[51] *Id*. at 71.
[52] *Id*.
[53] Malcolm Crompton, et al., *The Australian Dodo Case: An Insight for Data Protection Regulation*, BLOOMBERG BNA PRIV. & SEC. L. REP. 180 (Jan. 26, 2009).
[54] KUNER, *supra* note 47, at 71–72.

comply with these policies; adopt . . . internal oversight and external verification programmes; provide . . . transparency to individuals as to the policies and compliance with them; and adopt . . . mechanisms to enforce compliance."[55] Examples of the accountability approach include the APEC Privacy Framework and the Madrid Resolution.[56] An example of an adequacy regulation with accountability characteristics is the European Union law recognizing standard contractual agreements (SCCs) and binding corporate rules (BCRs),[57] which the next section will discuss.

III. DATA-PRIVACY REGULATIONS AND TRANSATLANTIC TRADE

A. Contrasting Historical Approaches to Data Privacy

The discrepancies between the European Union and the United States approaches regarding privacy concerns stem from history. Rather than a greater distrust of government oversight, as exhibited by the United States, the European Union focuses its privacy concerns on protecting consumers' personal information from private corporations and commercial entities.[58] Many forms of data gathering that are commonplace in the United States, the European Union restricts. For example, "employers monitoring their employees' private communications" or "checkout clerks requesting . . . addresses and telephone numbers from patrons" is allowed in the United States but prohibited in the EU.[59] The United States takes a different approach by protecting certain types of sensitive data, e.g., medical and financial information.[60] The sectoral approach greatly deviates from the EU's approach, which is a universal approach that protects all personal information.[61]

---

[55] *Id*.
[56] *Id*.
[57] *Id*. at 72–73.
[58] SOMA, *supra* note 29, at 46.
[59] *Id*. at 46–47.
[60] The Invalidation of the EU-US Privacy Shield and the Future of Transatlantic Data Flows: Hearing Before the U.S. Senate Comm. On Com., Sci. and Transp., 116th Cong. 3 (2020) (statement of James M. Sullivan, Deputy Assistant Sec'y for Int'l Trade Admin., U.S. Dep't of Commerce) [hereinafter Sullivan Testimony].
[61] *Id*.

The European Union and United States trade and privacy relationship began with the European Union Directive on Data Protections of 1995, which created explicit obligations for private entities and remedies for individuals.[62] Eventually, the European Union invalidated the Data Protection Directive of 1995, providing that United States law was still not "adequate," which spurred the creation of the Safe Harbor Framework in 2000.[63] The Safe Harbor Framework was an attempt at an accountability approach that allowed data transfers between European Union and United States organizations, even though United States law was inadequate by European Union standards.[64] The Safe Harbor framework was invalidated in 2013 by the European Court of Justice's (ECJ) decision in *Schrems v. Data Protection Commissioner* (*Schrems I*).[65] *Schrems I* provided that the Safe Harbor framework was invalid because it allowed government interferences despite the directive's protections. Overall, it failed to provide legal remedies for data subjects, and it blocked national supervisory authorities from exercising their powers.[66]

In 2016, the Privacy Shield Framework was approved and deemed by the European Commission as "adequate to enable data transfers under European Union law."[67] Similar to the Safe Harbor Framework, the Privacy Shield implemented an accountability approach to allow data transfers between organizations that implemented SCCs and BCRs.[68] This agreement became the legal basis for European Union and United States businesses to continue data transfers.[69] Since then, more than 5,300 businesses have relied on this

---

[62] SOMA, *supra* note 29, at 47.
[63] Jay Kramer & Sean Hoar *GDPR, Part I: History Of European Data Protection Law*, MONDAQ (Nov. 6, 2017), https://www.mondaq.com/unitedstates/data-protection/643052/gdpr-part-i-history-of-european-data-protection-law.
[64] *Id*.
[65] *Id*.
[66] *Id*.
[67] *Privacy Shield Overview*, Privacy Shield Framework, https://www.privacyshield.gov/Program-Overview (last visited Feb. 16, 2022).
[68] Caitlin Fennessy, *The 'Schrems II' Decision: EU-US Data Transfers in Question*, INT'L ASSOC. OF PRIV. PRO. (July 16, 2020), https://iapp.org/news/a/the-schrems-ii-decision-eu-us-data-transfers-in-question/.
[69] *Id*.

framework to conduct trade in compliance with European Union data protection rules.[70]

In 2018, the European Union implemented the GDPR. The EU's goals for creating the GDPR included unifying the regulations of the 27 nations in the EU, improving foreign data transfers, and improving data subjects' control over their identifying personal data.[71] The GDPR is a regulation that falls under the "adequacy approach" with some characteristics resembling the "accountability approach."[72] The GDPR requires European Union organizations to examine the foreign country's data protection process. If these processes do not abide by European Union laws and regulations, then the data must be returned to the exporting organization or destroyed.[73] The GDPR is known for being one of the most demanding privacy regulations imposed on cross-border transfers. Notably, the GDPR codifies additional requirements for handling data, i.e., stricter conditions for consent, "a broader definition of sensitive data, new provisions on protecting children's privacy, mandatory breach reporting obligation and the inclusions of the 'right to be forgotten.'"[74] Initially, the GDPR worked in tandem with the Privacy Shield Framework under the accountability approach.[75] However, this short-lived supplementation was ended by an ECJ decision invalidating the Privacy Shield for requiring insufficient projection under the GDPR, which will be further discussed in the subsequent section.

B. *Schrems II* Decision and Effects on Trade

Although the GDPR has created some difficulties for transatlantic data transfers, it wasn't until the ECJ's decision in *Data Protection Commissioner v. Facebook Ireland and Maximillian Schrems* ("*Schrems II*") that transatlantic trade began to feel the full force of the GDPR.[76] In July 2020, the *Schrems II* decision invalidated the Privacy

---

[70] White Paper Cover Letter, *supra* note 43.
[71] Kramer, *supra* note 63.
[72] *See supra* Part II.
[73] Fennessy, *supra* note 68; *see also Schrems II*, at ¶ 143.
[74] Kramer, *supra* note 63.
[75] *See supra* pp. 9–10.
[76] Phillips Testimony, *supra* note 44, at 6.

Shield Framework and required new obligations for mechanisms like SCCs and BJRs.[77] The ECJ invalidated the Privacy Shield for two reasons: (1) United States surveillance programs were not limited enough to abide by European Union law and (2) data subjects lack sufficient judicial redress regarding the United States surveillance programs.[78] Particularly, *Schrems II* held that neither Section 702 of the United States Foreign Intelligence Surveillance Act (FISA 702) nor the Executive Order on United States Intelligence Activities (EO 12333) meet the minimum requirement to satisfy European Union law because those regulations are not limited to what is "strictly necessary."[79] Further, the *Schrems II* decision found that the United States law fails to provide a means of individual redress that protects individuals from the prior mentioned United States regulations allowing for such broad surveillance.[80] This holding creates a considerable problem for the 70% of small and mid-sized Privacy Shield participants with minimal legal expertise and resources.[81]

Moreover, the *Schrems II* decision requires new obligations for mechanisms like SCCs and BCRs to be sufficient.[82] Under these new obligations, businesses must verify on a case-by-case basis "whether foreign legal protections concerning government access to personal data meet European Union standards."[83] If the recipient country's legal protections do not meet European Union standards, like the United States, then organizations must implement appropriate safeguards or refrain from transmitting data.[84] This puts a heavy burden on organizations and their privacy professionals to determine what constitutes "appropriate safeguards" and how to implement them. Instead of relying on the protocols under their current SCCs and BCRs, now businesses must assess their data transfers on a case-by-

---

[77] Kramer, *supra* note 63; *see also* Bradley A. Brooker, et al., *The Need for Clarity After Schrems II*, LAWFARE (Sept. 29, 2020, 11:54 AM), https://www.lawfareblog.com/need-clarity-after-schrems-ii.
[78] Fennessy, *supra* note 68; *see also Schrems II*, at ¶¶184–85, 191–93, 195–97, 201.
[79] *Schrems II*, at ¶¶184–85.
[80] *Id*. at ¶¶ 191.
[81] Brooker, *supra* note 77.
[82] *Id*.
[83] Fennessy, *supra* note 68.
[84] Brooker, *supra* note 77.

case basis and modify their current protocols to comply with European Union standards.[85]

Businesses who relied on SCCs and BCRs under the Privacy Shield Framework must now reassess and restructure their contracts and rules to comply with the new regulations, creating significant uncertainty.[86] Until the *Schrems II* decision, standardized SCCs and BCRs allowed an organizational approach to supplement the legal basis for data transfers to countries whose data protection policies do not satisfy European Union rules. However, the *Schrems II* decision invalidated standardized procedures. It now requires organizations to review SCCs and BCRs on a case-by-case basis to ensure GDPR is satisfied.[87] This case-by-case evaluation of these self-imposed clauses puts tremendous strain on small and mid-size businesses with limited legal resources. This leaves many European Union and United States businesses uncertain regarding their current protocols as well as whether they comply with European Union law. Ever since the ECJ found that protections from the United States government were lacking, the burden has fallen on companies to determine whether the ECJ's concerns apply to their specific transfers and if additional protocols can remedy these issues.[88]

The *Schrems II* decision prompted great uncertainty and polarized opinions on what the future of the transatlantic relationship would look like. For example, in May 2021, the High Court of Ireland issued a judgment suspending all Facebook data transfers finding that the *Schrems II* decision is binding and "United States law does not provide a level of protection that is essentially equivalent to that of European Union law."[89] The judgment goes even further to find that current SCCs cannot compensate for the inadequate protection provided by United States law.[90] The implications of these findings are that Facebook is forced to stop transferring European citizens'

---

[85] Fennessy, *supra* note 68.
[86] *Id*.
[87] *Id.*
[88] *Id*.
[89] Facebook Ir. Ltd. v. Data Prot. Comm'n [2020] 765 JR 2013 (H. Ct. 2021) (Ir.); *see also* Caitlin Fennessy, *The Irish High Court judgment on EU-U.S. data flows*, INT'L ASS'N. OF PRIV. PRO. (May 24, 2021), https://iapp.org/news/a/the-irish-high-court-judgment-on-eu-u-s-data-flows/.
[90] *Id*.

information to the United States[91] To survive in the EU, Facebook and other tech companies will likely be required to process European Union data within the bloc.[92] Only the absolutely "necessary" transfers can still happen between transatlantic users, otherwise the data will remain in its respective "safe" countries.[93] If this view is adopted, it will do more than damage tech and digital sectors as it will also inhibit all of the beneficial aspects of big data and information sharing, from the health sector's COVID-19 medical research to the economy as a whole currently facing uncharted economic difficulties. The High Court's interpretation of the *Schrems II* decision is a sweeping one, ultimately invalidating the use SCCs, which is vehemently opposed by parties on both sides of the Atlantic.

IV. INTERPRETATIONS OF *SCHREMS II* DECISION

Although the *Schrems II* decision invalidates the Privacy Framework, it does so on the fundamental rationale that the United States permits over-board governmental discretion of national security surveillance, citing FISA 702 and EO 12333.[94] The *Schrems* litigation is described as "a creature of distrust" by Professor Neil Richards, a privacy expert asked by the Data Protection Commissioner of Ireland to provide his independent expert testimony in the *Schrems II* litigation.[95] The Snowden Disclosures and the United States' lack of

---

[91] *See* Ryan Browne, *Facebook's EU-U.S. data flows are under threat — that may spell trouble for other tech giants*, CNBC (May 20, 2021, 4:02 AM), https://www.cnbc.com/2021/05/20/facebook-eu-us-data-flows-are-under-threat-heres-what-that-means.html.

[92] *Id*.

[93] *Id*.

[94] Alan C. Raul, Schrems II Concerns Regarding U.S. National Security Surveillance Do Not Apply to Most Companies Transferring Personal Data to the U.S. Under Standard Contractual Clauses, SIDLEY 1, 1–2 (Dec. 23, 2020), https://datamatters.sidley.com/wp-content/uploads/2020/12/Raul-Schrems-II-Concerns-Regarding-U.S.-National-Security-Surveillance-Do-Not-Apply-REVISED-12.23.20.pdf.

[95] The Invalidation of the EU-US Privacy Shield and the Future of Transatlantic Data Flows: Hearing Before the S. Comm. on Com., Sci. and Transp., 116th Cong. 2, 18 (2020) (testimony of Neil Richards, Koch Distinguished Professor in L., Dir. Cordell Inst. for Pol'y in Med. & L., Wash. Univ. in St. Louis) [hereinafter Richards Testimony].

implementation of uniform privacy laws instigated this distrust.[96] The EU, time and again, has invalidated attempts to bridge the adequacy gap of United States privacy law. However, The United States government claims that because of the limited and fragmentary rationale in *Schrems II*, many SCCs may be sufficient to comply with European Union laws regardless of *Schrems II*. United States privacy and trade experts have noted that the government surveillance concern is probably inapplicable to most data transfers to the United States and therefore should not interfere with compliance of SCCs.[97] This is because most data transfers to the United States from the European Union are unlikely to be the target of government surveillance.[98] Additionally, the United States government and some United States privacy professionals' claim that the ECJ failed to consider other United States laws protecting privacy and the limitations the United States has set for national security surveillance.

The United States argument is that since the *Schrems II* decision is only concerned about FISA 702 and EO 12333, companies who are not subject to FISA 702 and EO 12333, or "electronic communications providers," should easily satisfy the new SCCs self-assessment requirement under *Schrems II*.[99] The United States Department of Commerce's White Paper, released in response to the *Schrems II* decision therein, argues that although the ECJ finds United States law insufficient in limiting government surveillance, the United States government would not collect data in which it has no interest.[100] The White Paper concludes that United States law provides adequate

---

[96] *Id*.; The Invalidation of the EU-US Privacy Shield and the Future of Transatlantic Data Flows: Hearing Before the S. Comm. on Com., Sci. and Transp., 116th Cong. 15 (2020) (testimony of Peter Swire, Elizabeth and Tommy Holder Chair of L. and Ethics, Ga. Inst. Tech. Scheller Coll. of Bus.; Rsch. Dir., Cross-Border Data F.) [hereinafter Swire Testimony].

[97] Raul, *supra* note 94, at 2.

[98] *Id*.

[99] *Id.* at 6. (Under FISA 702, electronic communication service providers are companies in the business of transmitting or storing communications for third parties. This does not include companies who transmit their customer, employee, or business data from their bases in the European Union to bases in the United States).

[100] U.S. DEP'T OF COM., INFORMATION ON U.S. PRIVACY SAFEGUARDS RELEVANT TO SCCS AND OTHER EU LEGAL BASES FOR EU-U.S. DATA TRANSFERS AFTER SCHREMS II 2 (2020) [hereinafter White Paper].

protection and the *Schrems II* decision fails to take into account important limitations of FISA 702 and EO 12333. The White Paper addresses arguments on both FISA and EO 12333, refuting the ECJ's claims that these protocols are not sufficient to provide data subjects with adequate protections and remedies.[101] Further, the White Paper concludes that companies relying on current SCCs are in compliance with the GDPR.[102] This section will discuss both European Union and United States interpretations of the *Schrems II* decision for FISA 702 and EO 12333 and SCCs. Each discussion will first present the American arguments of each legal authority's limitations then discuss potential issues in the *Schrems II* decision rationale. In conclusion, each section will discuss the reliability of the advice given by both the United States and EU.

A. The FISA 702 Discussion

The White Paper, along with privacy experts articles, is the primary source of arguments for the purpose of this section. First, the white paper asserts that FISA 702's application is limited to electronic communications providers and foreign information. Targeting a United States citizen's data or data relating to persons located in the United States is prohibited under FISA 702.[103] FISA 702 does, however, authorize the United States to collect foreign intelligence from non-Americans located outside the United States[104] Under FISA 702, the United States government targets foreign communications via information provided by electronic communications providers; i.e., Google, Facebook, Yahoo; and direct tapping into data flows through fiber-optic cables that carry Internet traffic.[105] These techniques are required to filter out any communications that are "wholly domestic."[106] United States privacy experts argue that FISA 702 searches cannot target data transfers under SCCs because SCCs

---

[101] *Id*. at 6.
[102] *Id*. at 3.
[103] *Id*. at 6.
[104] *Decoding 702: What is Section 702?*, ELECTRONIC FRONTIER FOUNDATION, https://www.eff.org/702-spying (last visited Jan. 11, 2021).
[105] *Upstreem v. Prism*, ELECTRONIC FRONTIER FOUNDATION, https://www.eff.org/pages/upstream-prism (last visited Feb. 20, 2022).
[106] *Id*.

"necessarily entail a contract between a data exporter in Europe and a data importer in the United States"[107] Since the transfer involves a United States importer, FISA 702 cannot be the legal basis for government surveillance.[108] However, FISA 702 presents a potential loophole for domestic surveillance by allowing for "incidental" collection of domestic intelligence.[109]

Opponents of FISA 702 point out that government agencies still obtain United States persons' data by claiming the domestic information obtained was "incidental" and not "intentionally targeted."[110] Notwithstanding the potential United States constitutional violations of freedom of warrantless searches and seizures, this loophole incidentally jeopardizes international trade relations.[111] This is a critical flaw in FISA 702.

In rebuttal, the United States argues that regardless of whether FISA 702 is overbroad, domestic companies are outside of FISA 702's purpose and scope and therefore are not a target of surveillance. Thus, domestic companies protected from surveillance should not be subject to the *Schrems II* decision. The United States government assures that companies with ordinary commercial operations and ordinary personal data transfers would have no reason to "believe United States intelligence agencies would seek to collect that data."[112] Consequently, there is no threat to European Union data subjects' information. Additionally, the United States government asserts that FISA 702 has adequate supervisions ensuring proper targeting of individuals thus, it is sufficiently limited to what is necessary and essential to the public interest.[113]

"[B]efore the United States government may acquire under FISA 702 the communications data of any person (including an

---

[107] Raul, *supra* note 94, at 10.
[108] *Id*.
[109] *Decoding 702: What is Section 702?*, *supra* note 104.
[110] *'Incidental,' Not Accidental, Collection*, ELECTRONIC FRONTIER FOUNDATION, https://www.eff.org/pages/Incidental-collection (last visited Jan. 11, 2021).
[111] Comparison of Key Provisions of FISA Reauthorization Amendments Act (S. 139) and Amash/USA RIGHTS Act Amendment, Brennan Ctr. for Just., 1, Jan. 2018, https://www.brennancenter.org/sites/default/files/ChartComparingS139andUSARIGHTS11018.pdf.
[112] White Paper, *supra* note 100, at 2.
[113] *Id*. at 12.

European Union citizen or resident) meeting certain targeting restrictions, the Foreign Intelligence Surveillance Court ("FISC") must … approve a written certification submitted by the Attorney General and the Director of National Intelligence jointly authorizing the collection activities for up to one year."[114]

FISA 702 authorization requests are required to define how the government determined which specific persons' communications are to be acquired, be limited to a specific type of purpose, and specify how the agency will use it to acquire the type of foreign intelligence specified in the certification.[115] Independent intelligence oversight attorneys with the Department of Justice (DOJ) review every targeting assessment made by the NSA for compliance.[116] The White Paper further outlines the limitations of FISA 702 and independent departments' supervisory roles that protect from overbroad data collection.

Further privacy safeguards were added to FISA 702 in 2017, including:

> "(1) requiring that with each annual FISA 702 certification, the government must submit and the FISC must approve querying procedures, in addition to targeting procedures and minimization procedures;
> (2) requiring additional steps including notification to Congress before the government may resume acquisition of "about" collection under FISA 702;
> (3) amending the enabling statute for the PCLOB to allow it to better exercise its advisory and oversight functions;
> (4) adding the Federal Bureau of Investigation and NSA to the list of agencies required to maintain their own Privacy and Civil Liberties Officers, instead of being subject only to their parent department-level officers, to advise their agencies on privacy issues and ensure there are adequate procedures to receive, investigate, and redress complaints from individuals

[114] *Id*. at 8.
[115] *Id*.
[116] *Id*. at 9.

> who allege that the agency violated their privacy or civil liberties;
> (5) extending whistleblower protections to contract employees at intelligence agencies; and
> (6) imposing several additional disclosure and reporting requirements on the government, including to provide annual good faith estimates of the number of FISA 702 targets."[117]

Moreover, according to the White Paper, the *Schrems II* decision failed to address that United States law does provide redress for FISA 702 violations.[118] The FISA statute itself provides a cause of action for individuals, both United States and non-United States citizens, for violations of FISA 702.[119] The White Paper contends that the *Schrems II* court did not sufficiently evaluate United States law, as it failed to acknowledge that FISA 702 provides both United States citizens foreign individuals who are subject to United States surveillance. If any individual, United States citizen or not, is unlawfully targeted and whose communications are used or disclosed may seek compensatory and punitive damages, as well as attorney's fees.[120] Even beyond the FISA statute, the Electronic Communications Privacy Act, provides another separate cause of action for FISA violations.[121] The Administrative Procedure Act is another means in which an individual may challenge unlawful government access to personal data.[122]

These arguments, however, have been unsuccessful in persuading European Union entities. The *Schrems II* court altogether declined to consider these assertions. In applying the newly decided precedent from *Schrems II*, the High Court of Ireland also refused to consider these arguments, although they were brought to the attention

---

[117] *Id*. at 15.
[118] *Id*. at 13.
[119] *Id*.; 50 U.S.C. § 1810 (2018).
[120] *Id*. at 12.; 50 U.S.C. § 1810 (2018).
[121] *Id*. at 13.
[122] *Id*.

of the court.[123] Whilst, this is no surprise, as these arguments would require the European Union to trust that the United States government abides by the FISA 702 limitations when there is evidence to suggest that the United States does not.[124] Thus, United States companies relying on SCCs are in danger of losing trade relations with European Union partners because of the loophole in FISA 702.[125] Unless the United States entity can sufficiently prove that it is not a target of government surveillance, which cannot be definitively known by a company, there is no way for companies, on their own, to satisfy their self-assessment obligation under *Schrems II*.

Whether the United States' arguments are considered or not, the *Schrems II* decision is final and binding, which makes these *ex post facto* arguments ineffective in protecting trade between European Union and United States organizations, as we now know it. In order to maintain stable trade relations with the EU, Congress or individual states must enact further legislation.

B. The EO 12333 Discussion

The EO 12333 guides intelligence agencies on conducting overseas surveillance in situations where the United States Constitution does not apply.[126] The United States assures that EO 12333 provides full protection of United States persons' privacy rights, thus EO 12333 does not provide a legal basis for which the government may target data transmissions "to or from the United States by United States companies under SCCs."[127] The United States emphasizes that safeguards are in place to protect from government overreach regarding EO 12333, including the Presidential Policy Directive (PPD-28) and the National Intelligence Priorities Framework (NIPF).[128] Based on these policies and laws, United States privacy experts argue

---

[123] Facebook Ireland Ltd. v. Data Protection Commission [2020] 617 JR 2013 (H. Ct. 2021).
[124] Raul, *supra* note 94, at 6.
[125] *Id*. at 6.
[126] *Id.*
[127] *Id.* at 11.
[128] White Paper, *supra* note 100, at 20.

that the ECJ's concerns about overbroad government surveillance are irrelevant for many companies who rely on SCCs.[129]

First, presidential directives are a specific type of executive order that "carry the force and effect of law."[130] For example, one notable and effective presidential directive is George H.W. Bush's NSPM-4: Organization of the National Security Council and the Homeland Security Council.[131] President Barack Obama's PPD-28, ("PPD-28") limits the use of bulk collections to only six categories: (1) espionage and other threats from foreign powers; (2) terrorism; (3) threats from weapons of mass destruction; (4) cybersecurity threats; (5) threats to United States or allied forces; and (6) transnational criminal threats.[132] PPD-28 also requires that intelligence agencies treat foreign personal information as protected United States citizens' personal information. PPD-28 forces intelligence agencies to intelligence agencies to protect foreign citizens' rights as they would for a United States citizen and to adopt procedures to protect personal information, regardless of nationality.[133] PPD-28 only allows for the retention or dissemination of a foreign persons' personal information if "comparable information concerning United States persons would be permitted."[134]

Another safeguard to limit United States government surveillance to national security purposes is the NIPF.[135] The NIPF has both statutory and executive order authority via EO 12333.[136] The NIPF is the oversight body for EO 12333, which applies objective criteria to limit "bulk collections," which is the collection and storage of massive amounts of data that includes United States citizen information to specific national intelligence priorities and reviews agency requests for collection to ensure each request is consistent with the specific criteria

---

[129] Raul, *supra* note 94, at 7.
[130] *Presidential Directives*, SAFETY SCI. SEC. (Feb. 15, 2018), https://www.phe.gov/s3/law/Pages/Directives.aspx#:~:text=Presidential%20Directives%20are%20a%20specific,requirements%20for%20the%20Executive%20Branch.
[131] *Id*.
[132] White Paper, *supra* note 100, at 19.
[133] Richards Testimony, *supra* note 95, at 4, 6.
[134] *Id*.
[135] *Id*.
[136] *Id*.

set forth.[137] Irrespective of these safeguards, the ECJ is not convinced the NIPF is sufficient to protect against these bulk collections. The *Schrems II* decision takes issue with the mere *potential* the EO 12333 provides for bulk collection.[138]

However, bulk collection is "expressly prohibited" under FISA and National Security Letters statutes.[139] "Bulk data collection is permitted only in other contexts, such as clandestine intelligence activities involving overseas access to data."[140] Even the European Union permits this type of foreign surveillance by its member states.[141] The fact that the United States conducts global intelligence collection should not interfere with transatlantic trade relations. There is a limited expectation of privacy on global networks because any country or individual who has the means obtain access to data transfers can do so.

> "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."[142]

The European Union requires "essentially equivalent" protection from the United States government.[143] Since the ECJ has never ruled on an European Union member state's overseas access to foreign data, it follows that the United States need not be subject to

---

[137] *Id*. at 19–20.
[138] White Paper, *supra* note 100, at 17; *see also* AMOS TOH ET.AL., OVERSEAS SURVEILLANCE IN AN INTERCONNECTED WORLD 15 (2016), https://www.brennancenter.org/our-work/research-reports/overseas-surveillance-interconnected-world.
[139] *Id*. at 17.
[140] *Id*.
[141] *Id*. (citing EU FRA Intel. Rep't Vol. II at 42 (2017)) (some Member States "might allow for general surveillance of communications–but they do not regulate it in detail").
[142] *Id*.
[143] *Id*. at 15.

additional scrutiny but *equal* scrutiny.[144] It is widely agreed that gathering intelligence on both foreign and domestic transfers is extremely important to public safety and security, as we will discuss in the next subsection.[145]

Because EO 12333 is substantially different in its data collection scope than FISA 702, it has a more favorable chance of passing the GDPR's standards with some slight modifications. EO 12333 is a purely foreign intelligence collection that falls outside the GDPR's jurisdiction, unlike FISA 702 and its problematic loopholes. Since the European Union does not have strict regulation for what its member states may collect on the foreign front, the *Schrems II* decision should not have passed judgment on a United States policy that falls outside the EU's regulations.

V. NAVIGATING THE UNCHARTED WATERS POST-*SCHREMS II*: SUGGESTED ACTIONS TO SATISFY GDPR COMPLIANCE

This section discusses who the GDPR affects and what difficulties they face based on their circumstances. Both United States and European Union approaches to GDPR compliance will be discussed, with advice from both government agencies and independent privacy experts with an emphasis on the European Data Protection Board's ("EDPB") final recommendations on supplementary measures in the context of international transfer safeguards, such as SCCs.

Schrems II follows a pattern of invalidation of privacy agreements between the European Union and the United States, which is likely to continue absent legislative intervention.[146] The United States Congress votes on a federal privacy law proposal almost every legislative session in recent years but has yet to pass any legislation on a federal privacy policy since 1974, leaving up to the individual states. Thus far, four states—California, Colorado, Nevada, Virginia—have

---

[144] *Id*. at 15, 18.
[145] *See infra* Section IV.C.
[146] Richards Testimony, *supra* note 95, at 8–9.

enacted comprehensive privacy laws.[147] State legislative session has begun in most states, twelve of which have proposed privacy bills circulating in committees.[148] Waiting on state legislatures to decide the fate of businesses and private entities profitability and liability is not recommended. Whether these bills become law is unknown and out of private entitles' control. Suppose these bills even become law, they must be comprehensive enough to satisfy the GDPR for private entities to rely on them. Businesses should intervene in what they can control, their own privacy protocols.

The GDPR has perforce altered the future of the transatlantic trade and will require stricter privacy protection measures. Despite the inconvenience of change, the GDPR protocols provide many benefits. Most importantly, the protection of privacy, which should already be of the highest priority to businesses who mainly transact over the internet. Part I established that, due to the growth of internet transactions, it is of extreme consequence to create company initiatives that protect consumers' privacy and personal information from cyber-attacks and other unauthorized usage. To determine the most effective way to adapt, United States business must first understand who is affected by the GDPR and what actions will ensure compliance.

A. United States Approach to Compliance Post-*Schrems II*

As discussed previously,[149] the White Paper instructs companies to take the stance that most companies are not subject to FISA 702 of EO 12333.[150] The basis of this rationale is that these data transfers of no interest to the United States government and adequate safeguards ensure that government agencies properly target individuals and data collection is limited to what is necessary.[151] Under this theory, there are two groups of companies: (1) companies

---

[147] Taylor Kay Lively, *US State Privacy Legislation Tracker*, INT'L ASS'N. OF PRIV. PRO. (Mar. 31, 2022), https://iapp.org/resources/article/us-state-privacy-legislation-tracker/.
[148] *Id*.
[149] *See* discussion, *supra* Part IV.A-B.
[150] White Paper, *supra* note 100, at 6.
[151] *Id*.

that received order(s) to disclose information under FISA 702; and (2) companies relying on SCCs, including companies that are and are not electronic service providers. Companies should act according with each group it belongs to. Regardless of group, all companies should articulate that their data transfers are directed to persons (or organizations) located in the United States, which falls outside of FISA 702 and EO 12333 authority; thus, making their SCCs adequate.[152] Companies should also consider stating in public, corporate privacy policies that data transfers to the United States pursuant to SCCs are United States person communications.

i. Companies Ordered to Disclose Information Under FISA 702: GDPR's Public Interest Derogation

First, the United States suggests that companies ordered to disclose information under FISA 702 may rely on Article 49 of the GDPR's "public interest" derogation. The European Union continues to recognize the public interest derogation as an exception to data collection and sharing "in the spirit of reciprocity for international cooperation" and because it serves an "important public interest."[153] In the *Schrems II* decision, the ECJ upheld these derogations to maintain a cooperative relationship between United States and European Union intelligence agencies for public safety and security.[154] The information obtained through FISA 702 requests helps "counter a variety of threats, including international terrorism, the proliferation of weapons of mass destruction, and the activities of hostile foreign cyber actors."[155] The information obtained through FISA 702 requests has proven to be vital in investigating international crimes involving citizens of foreign nations.[156] The United States government insists that

---

[152] *Id*. at 7, 16–17; Raul, *supra* note 94, at 12.
[153] *Id*. at 3; *see also* EDPB, Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679 at 2.4 (May 25, 2018).
[154] *Id*.
[155] *Id*. at 4.
[156] *Id*. ("In 2014 the United States Privacy and Civil Liberties Oversight Board ("PCLOB"), an independent oversight entity, conducted an extensive review of FISA 702, including assessing its efficacy. After reviewing fifty-four cases in which FISA 702 information was used in intelligence matters, the PCLOB found that "approximately forty cases exclusively involved operatives and plots in foreign

FISA 702's international public safety benefits outweigh its privacy concerns, and abolishing this data collection could create serious public safety issues.[157]

Suppose a company has received a FISA 702 order, in that case, it may apply this approach by articulating this to the EDPB while conducting the newly required assessments of SCCs compliance.[158] Companies should also thoroughly document and assess FISA 702 requests to ensure the requests are sufficiently limited and non-incidental to report to the EDPB.[159] Companies should consider including information on "whether or not they have ever received national security intelligence collection demands under 702 or 12333 with respect to European Union data transferred to the United States under any Article 46 mechanism (i.e., SCCs, Privacy Shield, binding corporate rules, etc.)" in their EDPB assessments and public privacy statements.[160] This disclosure conveys a sense of transparency and compliance that is a core goal of the GDPR.[161] Transparency reports and internal records and statements have been deemed a possible source of information to assess an importer's compliance.[162] Also, if

---

countries." As an example of such a case, on December 31, 2016, a gunman killed 39 people and injured 69 others at a Turkish nightclub before fleeing the scene. Public reporting indicates the wounded and dead included European Union citizens from France, Germany, and Bulgaria. Almost immediately, Turkish law enforcement and United States intelligence officials began cooperating to identify and locate the shooter. Part of that effort included intelligence collection under FISA 702. The information derived from FISA 702 collection ultimately led police to an apartment in Istanbul where an Uzbek national was arrested, and firearms, ammunition, drones, and over $200,000 in cash were seized. This individual was tried and convicted, and in September 2020 was sentenced to life imprisonment.") For more examples, *see* White Paper, *supra* note 100, at 4–5.

[157] *Id*. at 5.

[158] Raul, *supra* note 94, at 13.

[159] *Id*.

[160] *Id.* at 14.

[161] Rania El-Gazzar & Karen Stendal, *Examining How GDPR Challenges Emerging Technologies*, 10 J. of Info. Poly, 238, 244 (2020) ("Lawfulness, fairness, transparency" is the first key principle of GDPR's seven principles EU organizations processing personal data must abide by.).

[162] *Recommendations*, *infra* note 177, at 47. ("Transparency reports, on the condition that they expressly mention the fact that no access requests were received." "Internal statements or records of the importer expressly indicating that no access requests were received for a sufficiently long period; and with a preference for statements and

applicable, a company should establish that it is not a communications service provider for the purposes of FISA 702.[163] Finally, companies who receive demands under FISA 702 should "[c]ommit to challenging any 702 directive it in good faith believes is unauthorized."[164]

ii. Companies Relying on SCCs

Companies relying on SCCs should first determine whether they are an electronic services provider under FISA 702. FISA statute defines electronic communication service providers as "telecom carriers, ISPs, email providers, cloud services, and 'any other communication service provider who has access to wire or electronic communications either as such communications are transmitted or as such communications are stored.'"[165] The majority of organizations engaging in transatlantic data transfers are not electronic service providers.[166]

If an organization is *not* an electronic communications service provider, then it would be beneficial to articulate to both United States intelligence agencies and EDPB that the organization is not an electronic service provider for purposes of FISA 702. Therefore it should not be targeted or issued any directives under FISA 702.[167] Organizations should include this information in their self-assessments of their SCCs. Since the company is not an electronic

---

records engaging the liability of the importer and/or issued by internal positions with some autonomy such as internal auditors, DPOs, etc.").

[163] Raul, *supra* note 94, at 14.

[164] *Id*.

[165] *Id*. at 7 (quoting 50 U.S.C. 1881b(4)); *see also* Evidence in Criminal Investigations, DEP'T OF JUSTICE (2009), at 117–118, available at https://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/01/14/ssmanual2009.pdf (However, the Stored Communications Act provides that agencies may not construe corporate email systems to constitute an electronic service provider. See Searching and Seizing Computers and Obtaining Electronic.).

[166] *Id*. at 6 ("i.e., the discrete set of companies in the business of transmitting (or storing) communications for third parties – as opposed to the vast number of companies transferring their own customer, employee or business data from their bases in Europe to their bases in the U.S.").

[167] *Id*. at 14.

service provider and not at risk of being targeted under FISA 702, the company will be able to adhere to their contractual obligations under the SCCs, and these transfers "will provide adequate protections for the privacy rights of individuals whose personal data is transferred pursuant to the SCCs."[168]

Suppose an organization is an electronic communications service provider, in that case, it may be helpful to note that:

> "[the] majority of companies have never received orders to disclose data under FISA 702 and have never otherwise provided personal data to United States intelligence agencies. Neither would such companies have any indication that a United States intelligence agency has sought to obtain their data unilaterally outside the United States under the authority of EO 12333."[169]

It remains crucial, however, to inform the EDPB of the organization's commitment to challenging any 702 directive it believes is unauthorized.[170] Further, organizations that share data with communications service providers should inform the communications service providers upon commencement of service with them, "and periodically thereafter, that communications emanating from the company's domain to a recipient in the United States is a United States person communication to a person located in the United States"[171] Additionally, the organization should assert that it will challenge any FISA 702 directive that is issued to collect a service provider's "United States-bound communications from the [European Economic Area], and request that the service provider provide meaningful advance notice of any such attempted collection to the full extent permitted by law."[172]

---

[168] Pulina Whitaker et al., *The End of the US-EU Privacy Shield, But Standard Contractual Clauses Remain Valid*, Morgan Lewis Publications (July 17, 2020), https://www.morganlewis.com/pubs/2020/07/the-end-of-the-us-eu-privacy-shield-but-standard-contractual-clauses-remain-valid.
[169] White Paper, *supra* note 100, at 2–3; *see also* Raul, *supra* note 94, at 6.
[170] Raul, *supra* note 94, at 14.
[171] *Id*.
[172] *Id*.

The United States Department of Commerce, via the White Paper, and United States privacy experts argue that companies may use this information to satisfy their self-assessment obligations under *Schrems II*.[173]

B. EU Approach to *Schrems II*

It is unlikely that the United States approach alone will satisfy the EU's strict data protection regulations, although it may have some persuasive influence.[174] The United States approach seems to treat the symptoms of the *Schrems II* decision rather than the underlying disease. To treat the transatlantic problem, the United States will need comprehensive consumer privacy reform implemented by Congress as well as the federal surveillance reform.[175] However, this reform may be too little, too late for United States businesses currently in danger of losing trade relations with the EU. This section will address how United States businesses may independently adopt GDPR protocols to help them achieve compliance with European Union standards that will protect them from both domestic and international liability and risk.

Unlike the High Court of Ireland, the EDPB found that the EJC upheld the use of SCCs on the condition that data controllers or data processors relying on SCCs:

> "verify, on a case-by-case basis and, where appropriate, in collaboration with the recipient of the data, whether the law of the third country of destination ensures adequate protection, under European Union law, of personal data transferred pursuant to standard data protection clauses, by providing, where necessary, additional safeguards to those offered by those clauses."[176]

---

[173] White Paper, *supra* note 100, at 1; Raul, *supra* note 94, at 14.
[174] Richards Testimony, *supra* note 95, at 8–9.
[175] *Id*. at 9.
[176] *Schrems II*, at ¶ 134.

On June 18, 2021, the EDPB adopted its final recommendations ("Recommendation") on how European Union data exporters and third-country importers can ensure compliance with *Schrems II* holdings.[177] The Recommendation provides guidance for how European Union exporters should assess third-party countries' laws or practices which "impinges on the effectiveness of the appropriate safeguards contained in the Article 46 GDPR transfer tools," i.e. SCCs, and "[identify] appropriate supplementary measures where needed."[178] The Recommendation advises that exporters, while conducting the required case-by-case verification of GDPR compliance of the third country importer, should collaborate with third country importers to ensure the appropriate safeguards are in place for the transfers.[179] This Note will expand on the role of importers pursuant to the Recommendation.

The Recommendation outlines a six-step roadmap ("EDPB Roadmap") to assist in the assessment of third countries and the measures that can be taken to safeguard the transfer of personal data:[180]

1. Know your transfers

2. Identify the transfer tools you are relying on

- Adequacy decisions
- Article 46 GDPR transfer tools (including SCCs and BCRs)
- Derogations

3. Assess whether the Article 46 GDPR transfer tool you are relying on is effective in light of all circumstances of the transfer

- Transfer factors
- Assessing laws

---

[177] Eur. Data Prot. Bd., Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data 1 (June 18, 2021), https://edpb.europa.eu/system/files/2021-06/edpb_recommendations_202001vo.2.0_supplementarymeasurestransferstools_en.pdf [hereinafter Recommendation].

[178] *Id*. at 3.

[179] *Id*.

[180] *Id*.; *see also* ONETRUST DATAGUIDANCE, THE DEFINITIVE GUIDE TO SCHREMS II 7 (2021) (eBook).

- Assessment outcomes

4. Adopt supplementary measures

5. Take procedural steps if you have identified effective supplementary measures Re-evaluate at appropriate intervals.[181]

The first step of the EDPB Roadmap advises exporters to "know [their] transfers."[182] Exporters are required to know where the personal data they export ends up in order to ensure that it is afforded the "essentially equivalent level of protection wherever it is processed."[183] As importers, it is your best interest to aide exporters in understanding where the personal data imported will be processed, stored, and the procedures used in this process. Importers should inform the exporters of the rationale and purpose for the adequacy, relevancy, and extent of the data that is being transferred. To maintain full awareness of the data imported, organizations must record and "map" all transfers. One crucial protocol that the GDPR requires to record and map data is the Record of Processing Activities (ROPA).[184] Implementing a ROPA would help to ensure that an organization's SCC is adequate and complies with protecting personal data.

"[T]he ROPA describes the exact usage of the data, the technical and organisational measures, that you have in place for the protection of the data, it shows you who is affected by a processing and it also shows you the recipient of a processing and possible data processors are also listed there. A fundamental risk analysis should also be included in a ROPA."[185]

The GDPR requires a ROPA from every organization or individual processing personal data, also known as "data controllers."[186] First, an organization must establish whether it is a controller or a processor. A processor is an organization or individual

---

[181] *Id*.
[182] *Id*.
[183] *Id*.
[184] Patty P. Tehrani, *International Data Privacy Compliance, Checklist - GDPR Data Portability Data Mapping Steps*, BLOOMBERG LAW.
[185] Easy GDPR Governance Platform, *FAQ*, https://easygdpr.eu/gdpr/faq/ (last visited Jan. 18, 2022).
[186] *Id*.

who processes personal data on behalf of the controller.[187] A controller "determines the purposes and means of the processing of personal data."[188] In other words, the controller is the entity collecting and using the data, and the processor is how the controller synthesizes the data. The controller's ROPA information should be more extensive than a processor's and must include purposes of processing, whose data is processed, what data is processed, etc.[189] The processor mainly needs to include the controller's processing information, the type of processing being done, if the information will be sent outside of the EU, and technical and organizational measures taken.[190] "The controller is responsible for implementing appropriate technical and organizational measures to ensure and demonstrate that processing is compliant with GDPR; the controller shall implement data protection policies and adhere to approved codes of conduct to demonstrate its compliance."[191]

Organizations with fewer than 250 employees are not required to maintain a ROPA unless they partake in systematic processing.[192] Systematic processing includes monthly processing of customer or employee data—e.g., payroll, or anything that would not be considered "occasional."[193] "[T]he only organizations that really might not have to keep a very extensive ROPA are organizations that don't have a lot of employees and that don't process any personal data other than that either."[194] These types of entities are unique, and it is unlikely

---

[187] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), art. 4(8), 2016 O.J. (L 119) 1, 33; *see also* El-Gazzar, *supra* note 161, at 242.

[188] Regulation (EU) 2016/679, art. 4(7), 2016 O.J. (L 119) 1, 33; *see also* El-Gazzar, *supra* note 161, at 242.

[189] Data Privacy Podcast, *How to Create a GDPR Records of Processing Activities*, at 15:54 (Nov. 18, 2020), https://dataprivacypod.com/laura-de-vries-how-to-create-a-gdpr-records-of-processing-activities/ (transcript available at link cited).

[190] *Id.*

[191] El- Gazzar, *supra* note 161, at 243.

[192] Data Privacy Podcast, *supra* note 189, at 18:27.

[193] *Id.*; *see also* Regulation (EU) 2016/679, art. 30, 2016 O.J. (L 119) 1, 50–51.

[194] *Id.* at 18:27; *see also* Regulation (EU) 2016/679, art. 30, 2016 O.J. (L 119) 1, 50–51.

that many entities will fit into this exception.[195] Further, the GDPR only applies to data controllers outside of the European Union if these entities are processing European Union data subjects' personal information regularly, including by offering goods and services and marketing to European Union data subjects.[196] A monetary transaction need not occur to be subject to the GDPR; the outside entity only needs to be observing and processing the behavior of data subjects within the EU.[197]

Although completing a ROPA will require time and resources, it is likely that many organizations already have some of the information needed to begin their ROPA at hand via their data inventory. A data inventory is an organized record of information an organization creates, acquires, and stores. If an organization already has a data inventory, it will make it much easier to create a ROPA. Since knowing and effectively using data is a vital part of a successful business, it is likely that most organizations already have some type of data inventory established. Nevertheless, if an organization does not have a data inventory, creating a ROPA will help begin the process of creating a data inventory. Beyond limiting organizations' liability, this is another benefit of creating and maintaining a ROPA. Creating a ROPA can help organizations in whatever stage their data inventory is in. Data inventories improve efficiency, increase internal accountability, and reduce risk. Failing to take advantage of an organizations' data can increase liability and financial risks.[198] There is also the risk that the organization is losing potential value by failing to understand their data.[199] Data helps to look at how companies generate leads, make sales, how companies operate, how staff is being

---

[195] *Id*. at 19:38.
[196] *Id*. at 37:22.
[197] Easy GDPR Governance Platform, *supra* note 186 ("An example: An US organisation that is selling online classes with no visible relation to the EU, is not subject to the GDPR—even if the online classes can be bought from inside the EU. If the organisation prices the classes also in EUR, then it is also subject to the GDPR.").
[198] Data Privacy Podcast, *supra* note 189, at 25:45; Steve Boston, Data Inventory: What Do You Have?, GBQ (Sept. 24, 2019), https://gbq.com/data-inventory-what-do-you-have/.
[199] *Id*.

trained, and how invoices are being processed.[200] This is the vital information that leads organizations to success.

When creating an organization ROPA, the first step is to determine the entity's ambitions for its data collection and what goals it would like to achieve from creating its data inventory.[201] It is important to set up an understandable overview that will be used as an internal guide that explains the goals and the tasks needed to achieve them.[202] This overview should include instructions for completing the ROPA tasks, descriptions of the information required, explanations for what the information is for, and how it will be used.[203] A detailed guide is the foundation for an accurate and valuable tool because when the people who are assembling the ROPA understand their work's legal basis, they can more accurately complete their tasks.[204]

After creating an internal guide, an organization should assemble an internal team with its most knowledgeable people on data privacy and those who are doing work with the personal data.[205] The people within the organization that are actually handling the personal data should be the individuals filling out the activity information.[206] Another suggestion is to include an individual who is familiar with the mechanisms from each department—someone who "knows what kind of systems they use, what kind of data they process, how they process this data, so they can help you fill in the details."[207] A legal representative and IT representative would also be helpful additions to the team.[208]

The second step is to "verify the transfer tool your transfer relies on."[209] The transfer tools are listed under Chapter V of the GDPR. The European Commission ("EC") allows third countries to obtain compliance in three ways: (1) adequacy decisions, (2) Article 46 GDPR

---

[200] *Id*. at 27:40.
[201] *Id*. at 20:52.
[202] *Id*.
[203] *Id*.
[204] *Id*.
[205] *Id*. at 30:53.
[206] *Id*.
[207] *Id*.
[208] *Id*.
[209] Recommendation, *supra* note 177, at 3.

transfer tools, and (3) derogations. Depending on the country, region or sector importing the data, some importers deemed adequate under the EC's adequacy decisions need not take any additional action described herein.[210] This, however, is not the case for the United States, as *Schrems II* makes clear that United States law is insufficient for GDPR compliance. Countries like the United States may rely on one of the transfer tools listed under Articles 46 of the GDPR.

Article 46 GDPR transfer tools include the following: standard data protection clauses (SCCs); binding corporate rules (BCRs); codes of conduct; certification mechanisms; and ad hoc contractual clauses.[211] These tools must ensure that the personal data transferred will benefit from an "essentially equivalent level of protection.[212] If the tools used are not sufficient to provide this level of protection, additional measures, such as supplementary measures, may be implemented. On July 4, 2021, the EC released a new set of SCCs for the transfer of personal data to third countries, including an explanation of the SCCs and a form document for SCCs.[213]

> "[The] revised SCCs have a broader scope to reflect the GDPR's extraterritorial reach as well as more flexibility to facilitate the use of SCCs in complex and constantly evolving relationships. The revised SCCs also reflect a strengthened data protection framework under the GDPR and specific clauses to accommodate concerns brought about by the *Schrems II* decision."[214]

United States data importers should use these forms when creating or updating their SCCs with the European Union exporter.

---

[210] *Id.* at 12.
[211] *Id*. at 13.
[212] *Id*.
[213] Commission Implementing Decision 2021/914 of 4 June 2021on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council, 2021 O.J. (L 199) 31, https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc/standard-contractual-clauses-international-transfers_en.
[214] ONETRUST DATAGUIDANCE, *supra* note 180, at 10.

Organizations must update their SCCs pursuant to the newly adopted SCCs within eighteen months beginning June 2021.[215]

Beyond transfer tools, Article 49 provides for derogations are unique and limited to specific situations. "[D]erogations . . . are exemptions from the general principle that personal data may only be transferred to third countries if an adequate level of protection is provided for in the third country or if appropriate safeguards have been adduced[.]"[216] Organizations may use derogations, but the use of these derogations may not contradict the rule that an adequate level of protection be afforded to the data being transferred.

Once the transfer tool has been verified, Step Three advises that the importer should assess whether the transfer tool being relied on is "effective in light of all circumstances of the transfer."[217] This assessment begins with determining if there is any law or practice in the import country that impinges on the appropriate safeguards of the transfer tool. In the United States, these laws or practices would be FISA 702 and EO 12333.[218] United States importers should incorporate the United States guidance on GDPR compliance discussed in the previous section.[219] The White Paper provides guidance on asserting that United States public authorities' limited ability to access data from a majority of United States importers.

Further, the importer should assess the characteristics of their transfers to identify the specific laws and practices that apply to their organization and type of transfers. For example, electronic service providers may be subject to a greater likelihood of surveillance by the United States government pursuant to United States law.[220] Some other factors to consider are the purpose for transfer, the types of entities involved in processing, the sector where transfer occurs, the categories of personal data, the location data that will be stored, the

---

[215] *Id*.
[216] Eur. Data Prot. Bd., *Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679*, at 4 (May 25, 2018), https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_2_2018_derogations_en.pdf.
[217] Recommendations, *supra* note 177, at 14.
[218] *See Schrems II*, at ¶ 60.
[219] *See supra* Part V.B.
[220] *See supra* Part V.A.ii.

availability of remote access by third countries, the format of the transferred data, and the possibility of subsequent transfers.[221]

The ROPA, or data mapping, will benefit this assessment, as it will identify all actors participating in the transfer. The laws or practices of the importing country will be considered incompatible with the transfer tool if they: (1) "[do] not respect the essence of the fundamental rights and freedoms of the European Union Charter of Fundamental Rights, or" (2) "[e]xceed what is necessary and proportionate in a democratic society to safeguard one of the important objectives as also recognised in Union or member state law such as those listed in Article 23(1) GDPR."[222] In short, if the importer restricts the data subjects from enabling their rights, i.e. access corrections and deletion requests for transferred data, judicial redress, then the transfer tool is effectively applied. The Recommendation specifically explains the FISA 702 situation:

"If your assessment of the relevant U. S. legislation leads you to consider that your transfer might fall within the scope of Section 702 FISA, but you are unsure if it falls within its practical scope of application, you may decide either:

> 1. To stop the transfer;
> 2. To adopt appropriate supplementary measures that ensure effectively a level of protection of the data transferred essentially equivalent to that guaranteed in the EEA; or
> 3. To look at other objective, reliable, relevant, verifiable and preferably publicly available information (which may include information provided to you by your data importer) to clarify the scope of application in practice of Section 702 FISA to your particular transfer."[223]The Recommendation allows the importer the ability to persuade their exporter that FISA 702 does not apply to their particular transfer. Importers should provide persuasive documentation

[221] Recommendations, *supra* note 177, at 15.
[222] *Id*. at 16.
[223] *Id*. at 20.

> to the exporter that shows FISA 702's inapplicability.[224] An importer may find that conducting a System and Organization Control (SOC) 2 privacy audit may be helpful in persuading the exporter of GDPR compliance.[225] If the exporter finds that FISA 702 does not apply, then no supplementary measures are necessary. If the exporter finds that FISA 702 *does* apply, then supplementary measures must be taken, or the data may not be transferred.

Step Four discusses the available supplementary measures. Supplementary measures must be implemented on a case-by-case basis unless the repeat transfers are of the same specific type to the same third country.[226] Supplementary measures may have a contractual, technical or organizational nature. The Recommendation finds that, generally, contractual and organizational measures alone will not overcome problems arising from import countries' legislation and practices.[227] Contractual and organizational measures can, however, strengthen technical measures to rise to the level of protection required. Annex 2 of the Recommendation lists examples of the types of supplementary measures and circumstances in which they may apply.[228]

Step Five advises on the procedure necessary for supplementary measures in addition to different contractual transfer tools, i.e., SCCs, BCRs, and ad hoc contractual clauses. For example,

---

[224] *Id.* at 21 (this information can be found in "Provisions of Section 702 FISA; Rules of Procedure of the Foreign Intelligence Surveillance Court (FISC), declassified FISC opinions and decisions, case law of U.S. courts; reports and hearing transcripts of the Privacy and Civil Liberties Oversight Board (PCLOB); reports by the Office of the Inspector General[,] U.S. Department of Justice; reports by the NSA Director of Civil Liberties and Privacy Office; reports prepared by the Congressional Research Service; reports by the American Civil Liberties Union Foundation (ACLU).")

[225] Timothy Dickens, *Understanding Data Processors' ISO and SOC 2 Credentials for GDPR Compliance*, INT'L ASSOC. OF PRIV. PRO. (May 22, 2018), https://iapp.org/news/a/understanding-data-processors-iso-and-soc-2-credentials-for-gdpr-compliance/.

[226] Recommendation, *supra* note 177, at 21.

[227] *Id*. at 22 (FISA 702 and EO 12333 falls within problematic legislation).

[228] *See id*. at 28.

SCCs require that the supplementary measures not contradict the SCCs and ensure the "protection guaranteed by the GDPR is not undermined."[229] If the supplementary measure and SCC contradict each other, then authorization from the competent supervisory authority in accordance with Article 46(3)(a) of the GDPR is required.

Step Six is simply the requirement to re-evaluate transfer compliance on an ongoing basis.[230] Importers must watch their country's legislative developments to act accordingly to maintain compliance. Currently, the best means of limiting liability and maintain compliance with international privacy regulations would be following advice set forth in the Recommendation.

C. New Transatlantic Privacy Framework

On March 25, 2022, the White House issued a statement announcing that the United States and European Union have "committed to a new Trans-Atlantic Data Privacy Framework, which addresses the concerns raised by the [*Schrems II* decisions]."[231] In its press release, the White House confirms that new policies will be implemented by the federal government to ensure that the United States adheres to a reliable legal basis for continued data flows with the European Union. Further, the press release confirms that companies and organizations may continue to utilize the Privacy Shield Principles to maintain compliance with the GDPR. It is the United States' position that President Biden's Executive Order will form the basis of the United States' legal adequacy for GDPR compliance.[232] This Executive Order could have substantial effects on data transfers and the requirements for how businesses maintain their data.

---

[229] *Id*. at 24.
[230] *Id*. at 25.
[231] Press Release, The White House, Fact Sheet: United States and European Commission Announce Trans-Atlantic Data Privacy Framework (Mar. 25, 2022) (on file with author).
[232] *Id*.

VI. CONCLUSION

Even with the united promise of the new Trans-Atlantic Data Privacy Framework, the future of the transatlantic trade relationship remains unclear. The *Schrems II* decision puts the pressure on Congress to enact privacy legislation that will further negotiations towards a privacy agreement. Some unique characteristics may allow the current Congress to enact this legislation.[233] However, until they do, United States organizations may use the guidance set out in this Note as a means to limit their liabilities and to continue their trade with the EU. This Note urges United States businesses to create a data inventory, not only to comply with the inevitable future of privacy protection, but also to increase their business' profitability and efficiency. Further, United States businesses should implement a privacy-conscious approach to their data handling, due to the inevitability of increased regulations on data handling. United States lawmakers and businesses must adjust with the changing technologies, as they have the obligation to protect their citizens' and customers' right to privacy.

[233] Swire Testimony, *supra* note 96, at 16.