UNC SCHOOL OF LAW

NORTH CAROLINA JOURNAL OF LAW & TECHNOLOGY

Volume 22 | Issue 4 Article 2

5-1-2021

Schrems II and TikTok: Two Sides of the Same Coin

David A. Hoffman

NORTH CAROLINA JOURNAL OF LAW & TECHNOLOGY
VOLUME 22, ISSUE 4: MAY 2021

SCHREMS II AND TIKTOK: TWO SIDES OF THE SAME COIN

David A. Hoffman*

Facebook and TikTok have both experienced considerable skepticism of whether individuals can trust the companies' privacy and data protection practices. These concerns are in part due to the potential for government agencies to access the data the companies collect and store. The European Union and the United States have both attempted to address these issues around potential government access to the companies' data by using different legal mechanisms to prohibit the international transfer of data. The Court of Justice of the European Union has ruled twice now that the United States does not provide an adequate level of protection for personal data of Europeans and therefore invalidated the legal basis that Facebook has used for its transatlantic data transfers. Similarly, the United States has attempted to use national security legal authorities to prohibit TikTok from transferring U.S. citizens' personal data to China. Both of these situations raise important questions as to how countries, companies, and individuals can evaluate whether they should trust technology that can collect personal data and transfer that data to another country. Neither the U.S approach nor China's approach to address the issue provide a scalable framework for the trust of technology. However, the Organization of Economic Coopearation and Development has begun efforts to develop such a model.

TABLE OF CONTENTS

* David A. Hoffman is the Steed Family Professor of Cybersecurity Policy at the Duke University Sanford School of Public Policy and is also Associate General Counsel and Senior Director of Data Policy Strategy at Intel Corporation.

I. INTRODUCTION: THE PROBLEM

What could teenagers creating videos of themselves dancing have to do with national security? Perhaps quite a bit. TikTok and Facebook have become fundamental components of many peoples' lives. In a press release issued in August of 2020, TikTok announced it had more than 100 million active U.S. users.[1] Industry analysts have reported that there have been 2.6 billion downloads of the TikTok app from Google Play and the Apple App Store.[2] Analysts similarly report that, as of October of 2020, Facebook has 2.7 billion active global users,[3] 410 million of whom are located in Europe.[4] Facebook's impact on privacy has been well documented,[5] including a $5 billion fine from the U.S. Federal Trade Commission ("FTC").[6] Recently, former U.S. National Security Agency ("NSA") General Counsel, Glenn Gerstel, also warned about the national security implications of Facebook.[7] Similarly, researchers are now observing

---

[1] *Why We are Suing the Administration*, TIKTOK (Aug. 24, 2020), https://newsroom.tiktok.com/en-us/tiktok-files-lawsuit [https://perma.cc/VL6E-XWH6].

[2] Stephanie Chan, *TikTok Was the Best-Rated of 2020's Top U.S. iOS Apps*, SENSORTOWER, INC. (Dec. 17, 2020), https://sensortower.com/blog/top-rated-apps-2020 [https://perma.cc/8XUR-X8P8].

[3] Salman Aslam, *Facebook by the Numbers: Stats, Demographics & Fun Facts*, OMNICORE (Jan. 6, 2021), https://www.omnicoreagency.com/facebook-statistics/ [https://perma.cc/H3JY-2XG6].

[4] H. Tankovska, *Facebook's Monthly Active Users (MAU) in Europe from 4th Quarter 2012 to 4th Quarter 2020*, STATISTA (Feb. 2, 2021), https://www.statista.com/statistics/745400/facebook-europe-mau-by-quarter/ [https://perma.cc/S7WL-A763].

[5] *See Facebook Privacy*, EPIC, https://epic.org/privacy/facebook/ [https://perma.cc/X7VE-RL34] (last visited Apr. 5, 2021).

[6] Lesley Fair, *FTC's $5 billion Facebook settlement: Record-breaking and history-making*, FTC (July 24, 2019), https://www.ftc.gov/news-events/blogs/business-blog/2019/07/ftcs-5-billion-facebook-settlement-record-breaking-history [https://perma.cc/8DRA-VPZB].

[7] Glenn S. Gerstell, *The National-Security Case for Fixing Social Media*, NEW YORKER (Nov. 13, 2020), https://www.newyorker.com/tech/annals-of-technology/the-national-security-case-for-fixing-social-media [https://perma.cc/FG8C-NKJ5].

the use of TikTok not just for dancing, but also for political engagement.[8]

The U.S. government has expressed concern about the amount of data relating to U.S. citizens that TikTok may transmit back to China, which would be accessible by Chinese government authorities.[9] Similarly, European courts have ruled that the ability of U.S. government authorities to access the data of European Facebook users is a violation of those users' rights under European law.[10] Both of these concerns arise from the question of whether users of these applications can trust them.[11] A recent survey found that eighty-five percent of Americans believe that a technology company is spying on them.[12] In that survey, Facebook and TikTok were the two companies that respondents most often believed were spying on their users (sixty-eight percent and fifty-three percent, respectively).[13]

In November of 2019, TikTok U.S. General Manager Vanessa Pappas sent a letter to Congress attempting to address these concerns in which she stated:

> We know that our users want to feel secure and informed when it comes to handling their data. Recognizing the importance of this issue, we want to be as transparent as possible in order to earn the trust and confidence

---

[8] *See, e.g., How TikTok is Shaping Politics: A New York Times Q&A With TC's Ioana Literat*, TCHRS. COLL., COLUM. UNIV. (June 29, 2020), https://www.tc.columbia.edu/articles/2020/june/how-tiktok-is-shaping-politics/ [https://perma.cc/Q59A-PVJ3].

[9] *Commerce Department Prohibits WeChat and TikTok Transactions to Protect the National Security of the United States*, U.S. DEPT. OF COM. (Sept. 18, 2020), https://web.archive.org/web/20200918121401/https:/www.commerce.gov/news/press-releases/2020/09/commerce-department-prohibits-wechat-and-tiktok-transactions-protect [https://perma.cc/RPP4-KBH6].

[10] Data Protection Comissioner v. Facebook Ireland Ltd. & Schrems [2020] C-311/18 (H. Ct.) (Ir.).

[11] *See* Larry Dignan, *Facebook, TikTok Least Trusted by Americans, Google Most Trusted, Says Survey*, ZDNET (Mar. 1, 2021), https://www.zdnet.com/article/facebook-tiktok-least-trusted-by-americans-google-most-trusted-says-survey/ [https://perma.cc/6QU4-GU2A].

[12] Angelo Ilumba, *Most Americans Think Big Tech Is Spying On Them*, WHISTLEOUT (Sept. 24, 2020), https://www.whistleout.com/CellPhones/Guides/americans-think-companies-are-spying [https://perma.cc/Q48B-UBWX].

[13] *Id.*

> of our US stakeholders in this crucial area. As we have said before, and recently confirmed through an independent security audit, we store all US user data in the United States, with backup redundancy in Singapore. TikTok's data centers are located entirely outside of China. Further, we have a dedicated technical team focused on adhering to robust cybersecurity policies, and data privacy and security practices. In addition, we periodically conduct internal and external reviews of our security practices in an effort to ensure we are keeping up with current risks.[14]

However, recent reporting that TikTok has been sending U.S. job applicant data to China has created additional concerns about whether TikTok can be trusted to live up to those commitments.[15] Commentators have noted in discussions of the trustworthiness of Huawei, another Chinese technology company, that the ability of technology companies to send software updates at any time presents the risk of Chinese government access to data collected, processed, and stored by those technologies.[16]

TikTok's potential access to personal data raises privacy concerns and national security risks.[17] With advanced analytics and the potential to collect data that includes location information, social relationships, and details of the private lives of government officials and employees of critical infrastructure operators, officials express

---

[14] Vanessa Pappas, *Explaining TikTok's Approach in the US*, TIKTOK (Nov. 5, 2019), https://newsroom.tiktok.com/en-us/explaining-tiktoks-approach-in-the-us [https://perma.cc/KPZ8-464D].

[15] @msmash, *TikTok Has Been Quietly Sending Job Applicants' Personal Data to China*, SLASHDOT (Dec. 16, 2020), https://tech.slashdot.org/story/20/12/16/1414230/tiktok-has-been-quietly-sending-job-applicants-personal-data-to-china [https://perma.cc/RGW2-ZHXA].

[16] The concerns in Huawei go well beyond just access to personal data and extend to disruption of critical infrastructure. *See* Colin Lecher & Russell Brandom, *Is Huawei a Security Threat? Seven Experts Weigh In*, VERGE (Mar. 17, 2019), https://www.theverge.com/2019/3/17/18264283/huawei-security-threat-experts-china-spying-5g [https://perma.cc/D6TQ-LEAV].

[17] *See* Bill Whitaker, *Is TikTok a Harmless App or a Threat to U.S. Security?*, CBS NEWS (Nov. 15, 2020), https://www.cbsnews.com/news/tiktok-cybersecurity-china-60-minutes-2020-11-15/ [https://perma.cc/5VPR-57GM]. S*ee also* Huileng Tan, *TikTok is 'Caught in the Middle' as the U.S. is 'Deeply Suspicious' of China, Analyst Says*, CNBC (Aug. 4, 2020), https://www.cnbc.com/2020/08/04/tiktok-is-caught-in-the-middle-as-the-us-is-deeply-suspicious-of-china-analyst-says.html [https://perma.cc/WJV3-WLVS].

concern about what the Chinese government could learn, especially when combining the data with information obtained from cybersecurity attacks on the United States, such as the attack on the U.S. Office of Personnel Management.[18] For example, it could be possible to isolate individuals who have high level U.S. government security clearances and then analyze the TikTok posts of their family members to understand their social connections, locations, schools, and videos from inside their homes. There are also concerns that the Chinese government could use TikTok to send misleading information to targeted users in an attempt to sway public opinion in the United States.[19] Other experts express reservations on the extent or likelihood of these risks, but they do not dispute that they are possible.[20]

European concerns about Facebook are similar. Beginning in 2010, Facebook began constructing data centers to manage the large amounts of data it collects and stores.[21] That first data center was in Prineville, Oregon.[22] Facebook now has a much more complicated data center infrastructure.[23] As of September of 2020, Facebook has seven data centers in the United States with plans for three more.[24] The company also operates three data centers in Europe in Sweden,

---

[18] Kevin Collier, *China Spent Years Collecting Americans' Personal Information. The U.S. Just Called It Out.*, NBC NEWS (Feb. 10, 2020), https://www.nbcnews.com/tech/security/china-spent-years-collecting-americans-personal-information-u-s-just-n1134411 [https://perma.cc/P7AV-ZBWX].

[19] *See* Brian Fung, *TikTok is a National Security Threat, US Politicians Say. Here's What Experts Think*, CNN BUS. (July 9, 2020), https://www.cnn.com/2020/07/09/tech/tiktok-security-threat/index.html [https://perma.cc/9BAS-ZHAE].

[20] *See* Justin Sherman, *Building a Better U.S. Approach to TikTok and Beyond,* LAWFARE (Dec. 28, 2020), https://www.lawfareblog.com/improving-tech-policy [https://perma.cc/3Q5D-K3FE].

[21] *The Facebook Data Center FAQ*, DATACENTER KNOWLEDGE (Sept. 27, 2010), https://www.datacenterknowledge.com/data-center-faqs/facebook-data-center-faq [https://perma.cc/6FKH-FEVH].

[22] *Id.*

[23] *See* Yevgeniy Sverdlik, *Facebook Plans Huge Expansion of Already Massive Georgia Data Center*, DATACENTER KNOWLEDGE (Sept. 17, 2020), https://www.datacenterknowledge.com/facebook/facebook-plans-huge-expansion-already-massive-georgia-data-center [https://perma.cc/6AHS-QWLR].

[24] *Id.*

Denmark, and Ireland.[25] The company also leases data center capacity in the United States, Europe, and Singapore.[26] However, even with data centers in Europe, Facebook operates its business by transferring data from the European Union ("EU") to the United States.[27] European citizens have expressed concern about these transfers of data, specifically about U.S. law allowing government agencies to be able to access that data and apply advanced analytics to infer information about individuals in the EU.[28]

The potential for government access to Facebook and TikTok data has led to legal efforts in the EU and the United States to mitigate the perceived risks. These legal mechanisms are worth reviewing in depth to compare their ability to reduce the risks and the degree to which they will have unintended consequences for innovation and the global economy. This Article will first look at the legal actions brought in the EU against Facebook under European data protection laws and will analyze the reasons given for why United States government surveillance legal authorities create a legal structure that does not provide adequate protection for the personal data of Europeans. This Article will then explore the recent actions taken against TikTok in the United States based on concerns that TikTok may transfer U.S. persons' data to China. Finally, this Article will compare the Facebook and TikTok situations and propose recommendations for a better approach.

II. FACEBOOK AND MAX SCHREMS

In 2012, University of Vienna law student Max Schrems spent a semester at Santa Clara Law School in California.[29] One of

---

[25] *Id.*

[26] *Id.*

[27] *Facebook EU Data Transfer Addendum*, FACEBOOK (Aug. 31, 2020), https://www.facebook.com/legal/EU_data_transfer_addendum [https://perma.cc/4VJ8-QPFD].

[28] Owen Bowcott, *Facebook Case may Force European Firms to Change Data Storage Practices*, GUARDIAN (Sept. 23, 2015), https://www.theguardian.com/us-news/2015/sep/23/us-intelligence-services-surveillance-privacy [https://perma.cc/D5ZZ-QR6G].

[29] Kashmir Hill, *Law Student of the Day: Max Schrems*, ABOVE THE LAW (Feb. 8, 2012), https://abovethelaw.com/2012/02/law-student-of-the-day-max-schrems/ [https://perma.cc/RC8T-6LFQ].

Schrems's law professors invited Facebook attorney Ed Palmieri to speak with the class.[30] Schrems was surprised by how little understanding the Facebook attorney had of European privacy law.[31] After writing his class paper about Facebook's lack of knowledge of European privacy law, Schrems returned to Austria and submitted a request to Facebook under the Austrian privacy law to receive the personal data Facebook held about him.[32] In response to his request, Facebook sent Schrems a 1,200-page report of all of its data relating to him.[33] Kashmir Hill, a journalist now at The New York Times, reported in Forbes that the data in Facebook's response included:

> [E]veryone he had ever friended and de-friended, every event he had ever been invited to (and how he responded), a history of every "poke" he had ever received, a record of who else signed onto Facebook on the same computers as him, email addresses that he hadn't provided for himself (but that must have been culled from his friends' contact lists) and all of his past messages and chats, including some with the notation "deleted."[34]

On June 6, 2013, Glenn Greenwald published a story in the Guardian alleging access to government documents that showed that the NSA had conducted a surveillance program to collect phone metadata records on millions of users of Verizon telecommunications services in the United States.[35] One day later, the Guardian and Washington Post both published stories describing documents that allegedly showed a program called PRISM that provided direct access for the NSA to servers at technology

---

[30] Kashmir Hill, *Max Schrems: The Austrian Thorn In Facebook's Side*, FORBES (Feb. 7, 2012), https://www.forbes.com/sites/kashmirhill/2012/02/07/the-austrian-thorn-in-facebooks-side/?sh=30b626017b0b [https://perma.cc/BT4R-3R5R].

[31] *Id.*

[32] *Id.*

[33] *Id.*

[34] *Id.*

[35] Glenn Greenwald, *NSA Collecting Phone Records of Millions of Verizon Customers Daily*, GUARDIAN (June 6, 2013), https://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order [https://perma.cc/R57E-XGZW].

companies including Facebook.[36] On June 8, 2013, U.S. Director of National Intelligence James Clapper released a fact sheet about PRISM.[37] The fact sheet asserted that the U.S. government did not have direct access to technology company servers.[38] Instead, Clapper described PRISM as a program under Section 702 of the Foreign Intelligence Surveillance Act ("FISA") that provides requests for information to the technology companies:

> With FISA Court approval and with the knowledge of the provider based upon a written directive from the Attorney General and the Director of National Intelligence. In short, Section 702 facilitates the targeted acquisition of foreign intelligence information concerning foreign targets located outside the United States under court oversight. Service providers supply information to the Government when they are lawfully required to do so.[39]

It was soon revealed that the documents referenced in the Guardian and Washington Post stories had been leaked by former government contractor Edward Snowden.[40] Max Schrems has stated that the Snowden disclosures made a significant impact on him, as

---

[36] Glenn Greenwald & Ewen MacAskill, *NSA Prism Program Taps in to User Data of Apple, Google and Others*, GUARDIAN (June 7, 2013), https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data [https://perma.cc/FX39-GQP5]; Barton Gellman, *U.S., British Intelligence Mining Data from Nine U.S. Internet Companies in Broad Secret Program*, WASH. POST (June 7, 2013), https://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html [https://perma.cc/7GR5-3NXK].

[37] OFF. OF THE DIR. OF NAT'L INTEL., FACTS ON THE COLLECTION OF INTELLIGENCE PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT, 1–3 (June 8, 2013), https://www.dni.gov/files/documents/Facts%20on%20the%20Collection%20of%20Intelligence%20Pursuant%20to%20Section%20702.pdf [https://perma.cc/X9EH-FLN6].

[38] *Id.* at 1.

[39] *Id.*

[40] Glenn Greenwalk et al., *Edward Snowden: The Whistleblower Behind the NSA Surveillance Revelations*, GUARDIAN (June 11, 2013, 9:00 AM), https://www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance [https://perma.cc/72VR-WU4F].

he realized that the information Facebook had about him and others in the EU was accessible by the NSA.[41]

With inspiration from Edward Snowden, Schrems soon focused his complaints about Facebook on whether Facebook's transfers of personal data to the United States were legitimate under the then existing law in Europe, *The 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* ("the Directive").[42]

Article I of the Directive provides the dual objectives of the law as:

> 1. In accordance with this Directive, Member States shall protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data.
>
> 2. Member States shall neither restrict nor prohibit the free flow of personal data between Member States for reasons connected with the protection afforded under paragraph 1.[43]

As noted in the second objective, the Directive provides for the free flow of data within EU member states. One mechanism it uses to accomplish the first objective is to restrict the transfer of personal data to other countries. Article 25, Section 1 of the Directive provides that companies can only transfer personal data when "the third country in question ensures an adequate level of protection."[44] Section 2 of Article 25 then provides criteria for how the Commission should determine whether the other country's protection is adequate.[45]

---

[41]Hannah Kuchler, *Max Schrems: The Man Who Took on Facebook — and Won*, FIN. TIMES (Apr. 5, 2018), https://www.ft.com/content/86d1ce50-3799-11e8-8eee-e06bde01c544 [https://perma.cc/8VSC-4ET5].

[42] *Id.*

[43] 2000 O.J. (L 215) at Article I. The Directive has not been superseded by the E.U. General Data Protection Regulation, but the objectives and restrictions on international data transfers have been incorporated into the regulation.

[44] *Id.* at Article 25, Section 1.

[45] *Id.* at Article 25, Section 2. In Article 26, the Directive also provides a number of derogations to the adequacy requirement including consent of the individual and the necessity of transfer to the performance of a contract. However, an adequacy decision was and is under the current General Data Protection

The Directive was designed to come into effect in October 1998, at which time member states were required to incorporate at least the minimum standards of the Directive into their country-specific data protection and privacy laws.[46] Shortly thereafter, the United States began negotiations with the European Commission to put in place a framework to allow the Commission to find whether United States was providing an adequate level of protection of the privacy interests of individuals in the EU.[47] The resulting agreement was titled the Safe Harbor Principles, and the European Commission issued a decision on July 26, 2000, that the framework satisfied the adequacy requirements of the Directive.[48]

The Safe Harbor Principles included a specific provision related to access to the data by law enforcement: "Adherence to these Principles may be limited: (a) to the extent necessary to meet national security, public interest, or law enforcement requirements."[49]

The Frequently Asked Questions ("FAQ") that were incorporated into the Safe Harbor Principles by the decision also identify that the likelihood of interfering with national security or defense is an exception to providing access to information:

> 5. A: Such circumstances are limited, and any reasons for denying access must be specific. An organization can refuse to provide access to information to the extent that disclosure is likely to interfere with the safeguarding of important countervailing public interests, such as national security; defense; or public security. In addition, where personal information is processed solely for research or statistical purposes, access may be denied. Other reasons for denying or limiting access are:
>
> a. interference with execution or enforcement of the law, including the prevention, investigation or detection of offenses or the right to a fair trial.[50]

Regulation the most comprehensive way to legally authorize transfers of personal data from the European Union to other countries.

[46] O.J. (L 215) Article 4(1).

[47] MARTIN A. WEISS & KRISTIN ARCHICK, CONG. RSCH. SERV., R44257, U.S.-EU DATA PRIVACY: FROM SAFE HARBOR TO PRIVACY SHIELD 5 (2020).

[48] O.J. (L 215), *supra* note 46 at Article 1(1).

[49] *Id.* at Annex I.

[50] *Id.* at Annex I, FAQ 8 - Access, 5-5(a).

As a result of these provisions, most companies included a statement in their privacy policies notifying individuals that the company may provide access to information when required by law.[51] It was this ability for law enforcement to access personal data under the Safe Harbor Principles that formed the basis for the European Court of Justice's decision in what is now commonly referred to as the *Schrems I* case.[52] In that decision, the Court invalidated the European Commission's adequacy decision for the Safe Harbor Principles on the basis of concerns about a lack of controls for U.S. government access to the data held by Facebook.[53]

In the *Schrems I* opinion, the Court provided the first interpretation of the obligation of "adequacy" to be defined as "essential equivalence" to the provisions of the Directive, **"**read in light of the Charter":

> The word 'adequate' in Article 25(6) of Directive 95/46 admittedly signifies that a third country cannot be required to ensure a level of protection identical to that guaranteed in the EU legal order. However, as the Advocate General has observed in point 141 of his Opinion, the term 'adequate level of protection' must be understood as requiring the third country in fact to ensure, by reason of its domestic law or its international commitments, a level of protection of fundamental rights and freedoms that is essentially equivalent to that guaranteed within the European Union by virtue of Directive 95/46 read in the light of the Charter. If there were no such requirement, the objective referred to in the previous paragraph of the present judgment would be disregarded. Furthermore, the high level of protection guaranteed by Directive 95/46 read in the light of the Charter could easily be circumvented by transfers of personal data from the European Union to third countries for the purpose of being processed in those countries.[54]

This reference to the Charter of the Fundamental Rights of the European Union ("the Charter") broadens the analysis of adequacy

---

[51] For many companies, these insertions were already included in their privacy policies as it had been a long- accepted practice to provide notice to individuals that information may be provided to law enforcement and other government agencies when required by law. *Privacy Policy*, AICPA (June 4, 2019), https://www.aicpa.org/privacyandterms/privacy.html [https://perma.cc/84S8-XZ55] (provising as example of industry best practice recommendations).

[52] Schrems v. Data Prot. Comm'r [2015], ECLI:EU:C:2015:650, ¶¶ 1-2 (H.Ct.) (Ir.).

[53] *Id.* at ¶ 106.

[54] *Id.* at ¶ 73.

beyond just the provisions of the Directive, which specifically exempts uses of personal data for law enforcement and national security.[55] Articles 7 and 8 of the Charter dictate the privacy and data protection rights of individuals in the EU.[56] Article 7 states that "[e]veryone has the right to respect for his or her private and family life, home and communications."[57] Article 8 provides in part "[e]veryone has the right to the protection of personal data concerning him or her" and further that the "data must be processed fairly" and "[e]veryone has the right of access . . . and the right to have it rectified."[58]

The Court then determined that the United States did not have appropriate legislative protections governing the collection of personal data for national security purposes.

> Moreover, the foregoing analysis of Decision 2000/520 is borne out by the Commission's own assessment of the situation resulting from the implementation of that decision . . . the Commission found that the United States authorities were able to access the personal data transferred from the Member States to the United States and process it in a way incompatible, in particular, with the purposes for which it was transferred, beyond what was strictly necessary and proportionate to the protection of national security. Also, the Commission noted that the data subjects had no administrative or judicial means of redress enabling, in particular, the data relating to them to be accessed and, as the case may be, rectified or erased.[59]

Other sections of the opinion further provided that permitting authorities to have access to personal data on a "generalised basis," or in situations where the individual does not have an adequate ability to pursue legal remedies, can cause a framework to fail the test of essential equivalence.[60] The Court specifically called out the PRISM program, which it described as a "large-scale intelligence [program,]" finding that it was "beyond what is strictly necessary and proportionate to the protection of national security."[61] The

---

[55] 2012 O.J. (C 326) 395.
[56] *Id.* at 397.
[57] *Id.*
[58] *Id.*
[59] Schrems v. Data Prot. Comm'r [2015], ECLI:EU:C:2015:650, ¶ 90 (H.Ct.) (Ir.).
[60] *Id.* at ¶¶ 94–95.
[61] *Id.* at ¶ 22.

opinion also states "there are no opportunities for either EU or US data subjects to obtain access, rectification or erasure of data, or administrative or judicial redress with regard to collection and further processing of their personal data taking place under the US surveillance programmes."[62]

The *Schrems I* opinion's specific mention of PRISM and the risks from large-scale access highlight concerns about how the U.S. intelligence agencies will use the personal data of individuals in the EU. The Court notably did not include any discussion of the controls that U.S. law applies to the use of that data by the relevant intelligence agencies, including the detail provided in Director of National Intelligence Clapper's letter.[63] The United States has arguably the most comprehensive and complicated oversight structure of its foreign surveillance activities, including Inspectors General, Congressional committees, a specially created federal court of life-tenured judges, and significant data minimization and reporting requirements.[64] The *Schrems I* case's lack of discussion of these controls called into question the Court's overall analysis of whether the collection and processing of data under Section 702 was sufficiently proportionate.

The *Schrems I* decision sent shockwaves throughout the privacy legal community and the U.S. government, due to the potential to disrupt transatlantic commerce.[65] Since the Snowden disclosures, there had been considerable calls for reform of U.S. surveillance legal authorities, including Section 702.[66] U.S. companies quickly pivoted to the use of other European Commission-approved

---

[62] *Id.* at ¶ 23.

[63] *See* OFF. OF THE DIR. OF NAT'L INTEL., *supra* note 37.

[64] *Director's Report on Foreign Intelligence Surveillance Courts' Activities*, ADMIN. OFF. OF THE U.S. CTS. 1, 2 (Apr. 27, 2020), https://www.uscourts.gov/statistics-reports/analysis-reports/directors-report-foreign-intelligence-surveillance-courts [https://perma.cc/9J26-ZYLU].

[65] *See, e.g., Max Schrems v. Data Protection Commissioner (CJEU - "Safe Harbor")*, EPIC, https://epic.org/privacy/intl/schrems/ [https://perma.cc/Y772-TGRT] (last visited Apr. 9, 2021).

[66] Spencer Ackerman, *Snowden Disclosures Helped Reduce use of Patriot Act Provision to Acquire Email Records*, GUARDIAN (Sept. 29, 2016, 3:34 PM), https://www.theguardian.com/us-news/2016/sep/29/edward-snowden-disclosures-patriot-act-fisa-court [https://perma.cc/HY99-YMRG].

mechanisms for transfer of data, such as Binding Corporate Rules and Standard Contractual Clauses.[67] The U.S. government and the European Commission entered into negotiations for a new agreement in an attempt to cure the Safe Harbor Principles deficiencies called out by the *Schrems I* decision.[68] On February 29, 2016, the two parties entered into a new agreement called the Privacy Shield, which was formally adopted on July 12, 2016.[69]

The Privacy Shield strengthened many aspects of privacy protection over transferred data, such as increased oversight and enforcement by the European Commission and the FTC, new complaint processes (including an Ombudsperson position reporting to the State Department to shepherd requests for information),[70] and the creation of an annual review process to create transparency on implementation of the agreement.[71] The documents adopted by the European Commission included several letters from U.S. government officials describing in detail the privacy protections available under U.S. law.[72] Two of these letters were from Robert Litt, the then-General Counsel of the Office of the Director of National Intelligence.[73] The letters provide a thorough description of U.S. national security intelligence collection authorities, including overviews of FISA Section 702, Presidential Policy Directive 28 ("PPD-28"), the function of the Privacy and Civil Liberties Oversight Board, the role of Inspectors General, and the USA

---

[67] SCHREMS ECJ / SAFE HARBOR RULING – FAQS, ALSTON & BIRD 5, https://www.alston.com/files/docs/Safe-Harbor-FAQs.PDF [https://perma.cc/386T-EUSH] (last visited Mar. 21, 2021).

[68] John Sander, *U.S. and EU Negotiationg New Data Transfer Agreement to Replace Invalid Safe Harbor*, SHRM (Jan. 14, 2016), https://www.shrm.org/resourcesandtools/hr-topics/global-hr/pages/u.s.-and-eu-negotiating-new-data-transfer-agreement-.aspx [https://perma.cc/H6WV-MCZE].

[69] European Commission Press Release IP/16/433, Restoring Trust in Transatlantic Data Flows Through Strong Safeguards: European Commission Presents EU-U.S. Privacy Shield (Feb. 29, 2016); Commission Implementing Decision (EU) 2016/1250, 2016 O.J. (L 207) 3.

[70] Commission Implementing Decision (EU) 2016/1250, *supra* note 69, at annex A, 72.

[71] *Id.* at annexes IV, V, VI, 78–108.

[72] *See id.* at annex VI, 91–108.

[73] *Id.*

Freedom Act.[74] In the conclusion of the first letter, Litt provides the following defense of the level of privacy protections for individuals outside the United States:

> The United States recognizes that our signals intelligence and other intelligence activities must take into account that all persons should be treated with dignity and respect, regardless of their nationality or place of residence, and that all persons have legitimate privacy interests in the handling of their personal information. The United States only uses signals intelligence to advance its national security and foreign policy interests and to protect its citizens and the citizens of its allies and partners from harm. In short, the IC does not engage in indiscriminate surveillance of anyone, including ordinary European citizens. Signals intelligence collection only takes place when duly authorized and in a manner that strictly complies with these limitations; only after consideration of the availability of alternative sources, including from diplomatic and public sources; and in a manner that prioritizes appropriate and feasible alternatives. And wherever practicable, signals intelligence only takes place through collection focused on specific foreign intelligence targets or topics through the use of discriminants.
>
> U.S. policy in this regard was affirmed in PPD-28. Within this framework, U.S. intelligence agencies do not have the legal authority, the resources, the technical capability or the desire to intercept all of the world's communications. Those agencies are not reading the emails of everyone in the United States, or of everyone in the world. Consistent with PPD-28, the United States provides robust protections to the personal information of non-U.S. persons that is collected through signals intelligence activities. To the maximum extent feasible consistent with the national security, this includes policies and procedures to minimize the retention and dissemination of personal information concerning non-U.S. persons comparable to the protections enjoyed by U.S. persons. Moreover, as discussed above, the comprehensive oversight regime of the targeted Section 702 FISA authority is unparalleled. Finally, the significant amendments to U.S. intelligence law set forth in the USA FREEDOM Act and the ODNI-led initiatives to promote transparency within the Intelligence Community greatly enhance the privacy and civil liberties of all individuals, regardless of their nationality.[75]

However, even before the Privacy Shield was formally adopted by the European Commission, experts were already predicting that

---

[74] *Id.*

[75] *Id.* at annex VI, 103–04.

the U.S. government surveillance reforms may not be enough to satisfy the European Court of Justice ("CJEU").[76] These concerns proved prescient as Schrems quickly amended his existing complaint to challenge Facebook's transfers of data to the United States, based on the company's assertion that the bulk of those transfers were done using European Commission-approved Standard Contractual Clauses ("SCC"), and those protections were insufficient to provide essentially equivalent privacy protection.[77]

In an opinion now known as *Schrems II*, the CJEU generally upheld the use of the SCC but significantly found that the Privacy Shield did not meet the standard of essential equivalence to justify an adequacy determination under European law.[78] Moreover, the CJEU noted that the use of the SCC would depend on the facts and circumstances of each transfer, including the likelihood that those transfers may be accessed by a non-EU government agency.[79]

In the *Schrems II* decision, the Court specifically rejected three arguments made in Litt's letter, by concluding: (1) the collection was not targeted; (2) there is not an independent tribunal; and (3) the Ombudsperson does not have the necessary independence and is not

---

[76] Jens-Henrik Jeppesen, *EU-US Privacy Shield Offers Partial Response to a Wider Issue*, CTR. FOR DEMOCRACY & TECH. (Mar. 10, 2016), https://cdt.org/insights/eu-us-privacy-shield-offers-partial-response-to-a-wider-issue/ [https://perma.cc/TS2R-C84Z].

[77] Davina Garrod, et al., *The Case of Schrems 2.0 – the Challenge to Standard Contractual Clauses Allowing Personal Data Transfer Outside the European Union*, AKIN GUMP: AG DATA DIVE (July 10, 2019), https://www.akingump.com/en/experience/practices/cybersecurity-privacy-and-data-protection/ag-data-dive/the-case-of-schrems-2-0-the-challenge-to-standard-contractual.html [https://perma.cc/DG7D-4HSW].

[78] Case C-311/18, Data Prot. Comm'r, v. Facebook Ireland Ltd (*Schrems II*), ECLI:EU:C: 2020:559, ¶ 181 (July 16, 2020).

[79] *Id.* at ¶¶ 132–33. The European Data Protection Board has subsequently published a paper to describe what supplementary protections may need to be put in place to justify a transfer. *See* EUROPEAN DATA PROT. BD., RECOMMENDATIONS 01/2020 ON MEASURES THAT SUPPLEMENT TRANSFER TOOLS TO ENSURE COMPLIANCE WITH THE EU LEVEL OF PROTECTION OF PERSONAL DATA (Nov. 10, 2020), https://edpb.europa.eu/sites/edpb/files/consultation/edpb_recommendations_202001_supplementarymeasurestransfertools_en.pdf [https://perma.cc/G23D-GC5J].

sufficiently empowered to enforce decisions.[80] First, the Court explicitly disagreed that intelligence collection under Section 702 was targeted, and therefore failed the principle of proportionality:[81]

> In that regard, as regards the surveillance programmes based on Section 702 of the FISA, the Commission found, in recital 109 of The Privacy Shield Decision, that, according to that article, "the [Foreign Intelligence Surveillance Court ("FISC")] does not authorise individual surveillance measures; rather, it authorises surveillance programs (like PRISM, UPSTREAM) on the basis of annual certifications prepared by the Attorney General and the Director of National Intelligence (DNI)". As is clear from that recital, the supervisory role of the FISC is thus designed to verify whether those surveillance programmes relate to the objective of acquiring foreign intelligence information, but it does not cover the issue of whether "individuals are properly targeted to acquire foreign intelligence information".
>
> It is thus apparent that Section 702 of the FISA does not indicate any limitations on the power it confers to implement surveillance programmes for the purposes of foreign intelligence or the existence of guarantees for non-US persons potentially targeted by those programmes. In those circumstances and as the Advocate General stated, in essence, in points 291, 292 and 297 of his Opinion, that article cannot ensure a level of protection essentially equivalent to that guaranteed by the Charter, as interpreted by the case-law set out in paragraphs 175 and 176 above, according to which a legal basis which permits interference with fundamental rights must, in order to satisfy the requirements of the principle of proportionality, itself define the scope of the limitation on the exercise of the right concerned and lay down clear and precise rules governing the scope and application of the measure in question and imposing minimum safeguards.[82]

The Court went even further, stating that the collection done under Executive Order 12333 ("E.O. 12333")[83] also failed that same proportionality test:

---

[80] Case C-311/18, Data Prot. Comm'r, v. Facebook Ireland Ltd (*Schrems II*), ECLI:EU:C: 2020:559, *passim* (July 16, 2020).

[81] *Id.* at ¶¶ 179–80.

[82] *Id.*

[83] *See* Exec. Order No. 12333, 46 Fed. Reg. 59941 (Dec. 8, 1981). Executive Order 12333, signed by President Ronald Reagan on December 4, 1981, describes the roles of the various U.S. intelligence agencies and makes clear that those agencies have broad authority to collect data that is stored outside the U.S. and does not relate to a U.S. person. *Id.*

> It should be added that PPD-28, with which the application of the programmes referred to in the previous two paragraphs must comply, allows for '"bulk" collection . . . of a relatively large volume of signals intelligence information or data under circumstances where the Intelligence Community cannot use an identifier associated with a specific target . . . to focus the collection', as stated in a letter from the Office of the Director of National Intelligence to the United States Department of Commerce and to the International Trade Administration from 21 June 2016, set out in Annex VI to the Privacy Shield Decision. That possibility, which allows, in the context of the surveillance programmes based on E.O. 12333, access to data in transit to the United States without that access being subject to any judicial review, does not, in any event, delimit in a sufficiently clear and precise manner the scope of such bulk collection of personal data.
>
> It follows therefore that neither Section 702 of the FISA, nor E.O. 12333, read in conjunction with PPD-28, correlates to the minimum safeguards resulting, under EU law, from the principle of proportionality, with the consequence that the surveillance
>
> programmes based on those provisions cannot be regarded as limited to what is strictly necessary.[84]

The Court's discussion of E.O. 12333 is particularly remarkable, as it covered collection by U.S. surveillance authorities of data stored or transited outside of the U.S. geographic borders in a case that specifically focused on the protection of data that Facebook transfered to the United States. The Court appeared to rely upon the theory that some of the collections under E.O. 12333 are in the process of transiting to the United States, but it is unclear what basis the CJEU had to reach that conclusion.[85] The result of this broadened scope of analysis is to judge all U.S. surveillance activity that could potentially collect personal data of individuals in the EU, instead of just whether the specific transfers by Facebook in Schrems' case had "essentially equivalent" protection as what would have been granted under European law.[86]

The second topic the Court disagreed with in Litt's letter was whether Europeans had sufficient access to an independent tribunal

---

[84] Case C-311/18, Data Prot. Comm'r, v. Facebook Ireland Ltd (*Schrems II*), ECLI:EU:C: 2020:559, ¶¶ 183–84 (July 16, 2020).

[85] *See id.*

[86] *Id.* at ¶ 185.

for them to demand access to the personal data collected by the U.S. government, as well as the ability for Europeans to request the deletion or correction of that data.[87] The Court noted that while the requirements of PPD-28 applied, those requirements did "not grant data subjects actionable rights before the courts against the U.S. authorities. Therefore, the Privacy Shield Decision cannot ensure a level of protection essentially equivalent to that arising from the Charter."[88] The Court went on to state that for surveillance done under E.O. 12333, "it is clear from the file before the Court that that order does not confer rights which are enforceable against the U.S. authorities in the courts either."[89] The Court then noted the requirement of enforceable redress for individuals by quoting Recital 104 of the General Data Protection Regulation ("GDPR"), which states that, "the data subjects should be provided with effective and enforceable rights and effective administrative and judicial redress."[90]

Going one step further, the Court then focused on the need for redress in the context of international data transfers:

> The existence of such effective redress in the third country concerned is of particular importance in the context of the transfer of personal data to that third country, since, as is apparent from recital 116 of the GDPR, data subjects may find that the administrative and judicial authorities of the Member States have insufficient powers and means to take effective action in relation to data subjects' complaints based on allegedly unlawful processing, in that third country, of their data thus transferred, which is capable of compelling them to resort to the national authorities and courts of that third country.[91]

Finally, the Court concluded that the surveillance authorities at issue did not provide effective redress mechanisms:

> Furthermore, as regards both the surveillance programmes based on Section 702 of the FISA and those based on E.O. 12333, it has been noted in paragraphs 181 and 182 above that neither PPD-28 nor E.O. 12333 grants data subjects rights actionable in the courts against the US

---

[87] *Id.* at ¶ 181.
[88] *Id.*
[89] *Id.* at ¶ 182.
[90] *Id.* at ¶ 188 (quoting Regulation (EU) 2016/679 of the Parliament and of the Council, 2016 O.J. (L 119/1) 104).
[91] *Id.* at ¶ 189.

> authorities, from which it follows that data subjects have no right to an effective remedy.[92]

The Court explicitly rejected the U.S. government's assertion that the creation of the Ombudsperson in the State Department would satisfy the level of essential equivalence to meet the standard of an effective redress mechanism, as it found that the Ombudsperson was not sufficiently independent.[93] Unfortunately, the CJEU did not provide much detail on what mechanisms could be put in place to make the Ombudsperson sufficiently independent to satisfy the requirement.[94] The relevant text of the opinion focuses on the fact that the Secretary of State has the ability to dismiss or revoke the appointment of the Ombudsperson.[95] Notably, the United States does have its own forms of independent regulatory agencies, such as the FTC. However, it is unclear whether the FTC would have sufficient independence to pass the Court's standard as a home for the Ombudsperson. It is also unclear how much weight the Court would give to other potential safeguards that could be put in place to restrict the ability of a U.S. executive agency to dismiss the Ombudsperson.[96]

The Court continued, stating that the Ombudsperson is not only insufficiently independent, but the Ombudsperson also does not have enough authority to provide effective redress for individuals in the EU:

> Similarly, as the Advocate General stated, in point 338 of his Opinion, although recital 120 of the Privacy Shield Decision refers to a commitment from the US Government that the relevant component of the intelligence services is required to correct any violation of the applicable rules detected by the Privacy Shield Ombudsperson, there is nothing in that decision to indicate that that ombudsperson has the power to adopt decisions that are binding on those intelligence services and does not mention any legal safeguards that would accompany that political commitment on which data subjects could rely.[97]

---

[92] *Id.* at ¶ 192.
[93] *Id.* at ¶ 194–95.
[94] *See id.*
[95] *Id.* at ¶ 195.
[96] *See id.*
[97] *Id.* at ¶ 196.

> Therefore, the ombudsperson mechanism to which the Privacy Shield Decision refers does not provide any cause of action before a body which offers the persons whose data is transferred to the United States guarantees essentially equivalent to those required by Article 47 of the Charter.[98]

The Court's language on these three issues—(1) bulk versus targeted collection; (2) access to a judicial tribunal; and (3) the independence and authority of the redress mechanism—provides a roadmap to analyze what could be deemed sufficient protections in situations where national security agencies access personal data collected by private sector companies and transfer that data to another country.

Reactions to the *Schrems II* decision came quickly. U.S. Secretary of Commerce, Wilbur Ross, noted his desire to continue conversations with the EU to allow for continued data transfers:

> While the Department of Commerce is deeply disappointed that the court appears to have invalidated the European Commission's adequacy decision underlying the EU-U.S. Privacy Shield, we are still studying the decision to fully understand its practical impacts," said Secretary Wilbur Ross. "We have been and will remain in close contact with the European Commission and European Data Protection Board on this matter and hope to be able to limit the negative consequences to the $7.1 trillion transatlantic economic relationship that is so vital to our respective citizens, companies, and governments. Data flows are essential not just to tech companies—but to businesses of all sizes in every sector. As our economies continue their post-COVID-19 recovery, it is critical that companies—including the 5,300+ current Privacy Shield participants—be able to transfer data without interruption, consistent with the strong protections offered by Privacy Shield.[99]

U.S. Secretary of State, Mike Pompeo, also conveyed a desire to work with the EU to find an acceptable mechanism to allow the continued transatlantic flow of data that enables economic development for both the United States and EU member states:

> The United States and the EU have a shared interest in protecting individual privacy and ensuring the continuity of commercial data

---

[98] *Id.* at ¶ 197.

[99] Press Release, Wilbur Ross, U.S. Sec'y of Com., U.S. Secretary of Commerce Wilbur Ross Statement on Schrems II Ruling and the Importance of EU-U.S. Data Flows (July 16, 2020), https://2017-2021.commerce.gov/index.php/news/press-releases/2020/07/us-secretary-commerce-wilbur-ross-statement-schrems-ii-ruling-and.html [https://perma.cc/9LM9-E3ZW].

> transfers. Uninterrupted data flows are essential to economic growth and innovation, for companies of all sizes and in every sector, which is particularly crucial now as both our economies recover from the effects of the COVID-19 pandemic. This decision directly impacts both European companies doing business in the United States as well as American companies, of which over 70 percent are small and medium enterprises. The United States will continue to work closely with the EU to find a mechanism to enable the essential unimpeded commercial transfer of data from the EU to the United States.[100]

In a similar fashion, EU officials have made public statements of working collaboratively with the U.S. government to find a solution. European Commission Vice-President Věra Jourová commented, "we will be working closely with our American counterparts, based on today's ruling. Both Didier and I have been in contact with U.S. Commerce Secretary Wilbur Ross in the past days."[101]

Vice President Jourova then continued her statement to include the principles for further cooperation when she added:

> [O]ur priorities are very clear: One: Guaranteeing the protection of personal data transferred across the Atlantic; Two: Working constructively with our American counterparts with an aim of ensuring safe transatlantic data flows. [and] Three: Working with the European Data Protection Board and national data protection authorities to ensure our international data transfer toolbox is fit for purpose."[102]

EU Commissioner of Justice Didier Reynders struck the same tone when he noted that the United States and the EU should work together "constructively," while "(i)n the meantime, transatlantic data flows between companies can continue using other mechanisms for international transfers . . . ."[103]

---

[100] Michael R. Pompeo, Sec'y of State, European Court of Justice Invalidates EU-U.S. Privacy Shield (July 17, 2020), https://2017-2021.state.gov/european-court-of-justice-invalidates-eu-u-s-privacy-shield/index.html [https://perma.cc/6UND-YVQB].

[101] European Commission Press Release STATEMENT/20/1366, Opening Remarks by Vice-President Jourová and Commissioner Reynders at the Press Point Following the Judgment in Case C-311/18 Facebook Ireland and Schrems (July 16, 2020), https://ec.europa.eu/commission/presscorner/detail/en/statement_20_1366 [https://perma.cc/6KHD-P2BF].

[102] *Id.*

[103] *Id.*

The U.S. government and some experts have reacted to the *Schrems II* ruling with recommendations for specific paths forward.[104] In September of 2020, the U.S. Department of Commerce issued a detailed white paper analyzing the judgment and offering several opportunities to support a new analysis.[105] The white paper makes the following three key points:

(1) 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 ECJ in Schrems II.

(2) The U.S. government frequently shares intelligence information with EU Member States, including data disclosed by companies in response to FISA 702 orders, to counter threats such as terrorism, weapons proliferation, and hostile foreign cyber activity. Sharing of FISA 702 information undoubtedly serves important EU public interests by protecting the governments and people of the Member States.

(3) There is a wealth of public information about privacy protections in U.S. law concerning government access to data for national security purposes, including information not recorded in Decision 2016/1250, new developments that have occurred since 2016, and information the ECJ neither considered nor addressed. Companies may wish to take this information into account in any assessment of U.S. law post-Schrems II.[106]

The white paper's second point above may be a consideration outside the *Schrems* Court's reach, but it is worthy of consideration as the United States and the EU develop a path forward, and it could be important in the analysis of whether the surveillance programs' data collection are proportionate to the purpose of enhancing

---

[104] 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 [https://perma.cc/CFH4-GB5R]. S*ee* 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 (2020), https://www.commerce.gov/sites/default/files/2020-09/SCCs WhitePaperFORMATTEDFINAL508COMPLIANT.PDF [https://perma.cc/UMA9-FG86].

[105] 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 1 (2020).

[106] *Id.* at 1–2.

national security and thereby protecting civil liberties from incursion by malicious actors. Experts have previously pointed out that national security surveillance and intelligence analysis provides protections for individuals that help protect the fundamental human rights in the Charter.[107] The processing of personal data is often necessary to protect privacy, as scanning internet network traffic can identify and prevent malicious cybersecurity attacks that would otherwise result in the stealing of sensitive personal data.[108]

The white paper's third key point suggests that a more detailed review of U.S. surveillance laws, policies, and practices is necessary to properly determine whether the U.S. system is "essentially equivalent" with that of the EU.[109] With specific focus on Section 702, the white paper argues that the *Schrems II* decision was incorrect in determining that surveillance under the section is not targeted.[110] In support of the U.S. model, the paper notes that the Foreign Intelligence Surveillance Court ("FISC"), a body composed of "life-tenured federal judges," must approve and enforce Section 702 targeting procedures.[111] The paper then offers points in opposition to the *Schrems II* ruling that the United States does not provide adequate access for individuals in the EU to seek redress for violations of Section 702, offering the following three specific statutes that provide such access:

1. Section 1810 of the Foreign Intelligence Surveillance Act, 50 U.S.C. § 1810 (2018).
2. Section 2712 of the Electronic Communications Privacy Act, 18 U.S.C. § 2712 (2018).

---

[107] Glenn S. Gerstell, *Public Surveillance to Keep Us Healthy and Protect Our Privacy*, CTR. FOR STRATEGIC & INT'L STUD. (Apr. 16, 2020), https://www.csis.org/analysis/public-surveillance-keep-us-healthy-and-protect-our-privacy [https://perma.cc/8VF2-FR95].

[108] David A. Hoffman & Patricia A. Rimo, *It Takes Data to Protect Data*, *in* THE CAMBRIDGE HANDBOOK OF CONSUMER PRIVACY 546 (Evan Selinger, et al. eds., 2018).

[109] DEP'T. OF COM., *supra* note 105, at 2.

[110] DEP'T. OF COM., *supra* note 105, at 11.

[111] *Id.* at 6–7.

3. Section 702 of the Administrative Procedure Act, 5 U.S.C. § 702 (2018).[112]

After the discussion of redress, the paper describes changes made under U.S. law to enhance the privacy protections in, and oversight of, surveillance conducted under Section 702.[113] Finally, the paper points out the peculiarity of the Court's analysis of E.O. 12333 since that is an authority for overseas collection and, "[u]nlike FISA 702 . . . E.O. 12333 does not authorize the U.S. government to *require* any company or person to disclose data."[114] The additional information provided on redress, the clarification on E.O. 12333, and the new protections could justify a different decision on "essential equivalence" and support discussions between the EU and United States on a replacement data transfer mechanism for the Privacy Shield.

Privacy experts have also offered opinions on the *Schrems II* ruling and options for future modifications that could cure the deficiencies noted by the *Schrems II* Court.[115] Stewart Baker, former Assistant Secretary for Policy at the U.S. Department of Homeland Security, has referred to the Court's ruling as "gobsmacking in its mix of judicial imperialism and Eurocentric hypocrisy." Among other proposals, he believes the United States should use trade sanctions to force the EU to amend its operating treaty and law to better accommodate the international transfer of data.[116] Baker has been outspoken in his belief that EU member state surveillance

---

[112] *Id.* at 12–13.

[113] *Id.* at 14–15.

[114] *Id.* at 16 n.57.

[115] Christopher Kuner, *The Schrems II Judgment of the Court of Justice and the Future of Data Transfer Regulation*, EUR. L. BLOG (July 27, 2020), https://europeanlawblog.eu/2020/07/17/the-schrems-ii-judgment-of-the-court-of-justice-and-the-future-of-data-transfer-regulation/ [https://perma.cc/KQX9-YTYP]; Kenneth Propp & Peter Swire, *After Schrems II: A Proposal to Meet the Individual Redress Challenge*, LAWFARE (Aug. 13, 2020 7:28 PM), https://www.lawfareblog.com/after-schrems-ii-proposal-meet-individual-redress-challenge [https://perma.cc/3NPP-J4QR].

[116] Stewart Baker, *How Can the U.S. Respond to Schrems II?*, LAWFARE (July 21, 2020, 8:11 AM), https://www.lawfareblog.com/how-can-us-respond-schrems-ii [https://perma.cc/YY63-6H36].

practices cannot satisfy the same standards that have been applied in the *Schrems II* opinion.[117]

It is unfortunate that the *Schrems II* opinion does not provide an overview of existing European Court of Human Rights ("ECHR") case law that has examined the proportionality of surveillance practices in light of the European Convention on Human Rights ("Convention"), specifically, Article 8 of that treaty.[118] This lack of analysis is all the more surprising, as Article 52, Section 3 of the Charter explicitly states the rights and the "meaning and scope" of the rights should be the same as those in the Convention.[119] Commentators have observed a recent pattern of the CJEU increasingly failing to look to the separate ECHR case law to help interpret the Charter.[120]

The Convention is an instrument of the Council of Europe, which is not an EU institution, although all of the EU member states have adopted the Convention.[121] Unlike the Charter, the Convention does explicitly apply to national security surveillance, and there is a growing body of case law to determine when surveillance programs violate the Convention's right to respect for privacy.[122] Section 2 of Article 8 specifically states:

---

[117] *See* Tech Pol'y Podcast, *#19: Europocrisy: EU Privacy Hypocrisy with Stewart Baker,* TECHFREEDOM, at 20:55 (Feb. 9, 2016), https://techfreedom.org/19-europocrisy-eu-privacy-hypocrisy-with-stewart-baker/ [https://perma.cc/AQ33-JN6J].

[118] 2012 O.J. (C 326) 397.

[119] *Id.* at 406 ("In so far as this Charter contains rights which correspond to rights guaranteed by the Convention for the Protection of Human Rights and Fundamental Freedoms, the meaning and scope of those rights shall be the same as those laid down by the said Convention. This provision shall not prevent Union law providing more extensive protection.").

[120] Martin Kuijer, *The Challenging Relationship Between the European Convention on Human Rights and the EU Legal Order: Consequences of a Delayed Accession*, 24 INT'L J. HUM. RTS. 998, 1001–02 (2020).

[121] *What is the European Convention on Human Rights?*, EQUAL. & HUM. RTS. COMM'N, https://www.equalityhumanrights.com/en/what-european-convention-human-rights [https://perma.cc/5E6Q-F443] (last updated Apr. 17, 2017).

[122] *See* EUR. CT. OF HUM. RTS., PRESS UNIT, MASS SURVEILLANCE 1 (2020), https://www.echr.coe.int/documents/fs_mass_surveillance_eng.pdf [https://perma.cc/HZ7F-GXLE].

> 1. Everyone has the right to respect for his private and family life, his home and his correspondence.
> 2. There shall be no interference by a public authority with the exercise of this right except such as in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.[123]

It is the inclusion of the phrase "necessary in a democratic society" that provides the ECHR the need to assess the proportionality of surveillance's impact on privacy. The CJEU could also look to EU member state court examinations of whether surveillance programs have been proportionate in light of member state constitutions and laws, such as in the recent German Bundesnachrichtendienst Act case.[124] In that case, the court found substantial, but not unlimited, latitude was necessary to safeguard national security interests.[125]

Also, the EU institutions are increasingly narrowing the scope of national security within which they will defer to member states.[126] In two cases decided subsequent to *Schrems II*, the CJEU determined that "indiscriminate data retention" requirements by nation states can be justified by national security concerns, but the decisions must be reviewed by a court or independent tribunal.[127] The developments in the CJEU, the ECHR and member state courts, and the arguments that the *Schrems II* opinion did not include a full

---

[123] Convention for the Protection of Human Rights and Fundamental Freedoms art. 8, *opened for signature* Apr. 11, 1950, E.T.S. No. 005.

[124] BVERFG, HEADNOTES TO THE JUDGEMENT OF THE FIRST SENATE OF 19 MAY 2020 - 1 BVR 2835/17 (2020) https://www.bundesverfassungsgericht.de/SharedDocs/Downloads/EN/2020/05/rs20200519_1bvr283517en.pdf;jsessionid=23960014948D3CA040679C991345EF38.1_cid386?__blob=publicationFile&v=4 [https://perma.cc/T8BL-AHN8].

[125] *Id.*at 49–50.

[126] *See* Monika Zalnieriute, *The Future of Data Retention Regimes and National Security in the EU After the Quadrature Du Net and Privacy International Judgments*, 24 AM. SOC'Y OF INT'L L. INSIGHTS, Nov. 5, 2020, at 4, https://www.asil.org/sites/default/files/ASIL_Insights_2020_V24_I28.pdf [https://perma.cc/4HVL-4GJB].

[127] *Id.* at 1, 3.

analysis of the privacy protections in the U.S. system all support that there may be an opportunity for a new agreement between the United States and the European Commission to satisfy the CJEU's implementation of the essential equivalence standard. That opportunity may be enhanced by additional changes the United States can make without increasing national security risks.

Professors Peter Swire and Kenneth Propp authored a particularly interesting proposal to address "two dimensions: a credible fact-finding inquiry into classified surveillance activities in order to ensure protection of the individual's rights, and the possibility of appeal to an independent judicial body that can remedy any violation of rights should it occur."[128] Their recommendation would utilize the fact-finding ability of U.S. government agency privacy and civil liberties officers while allowing for judicial appeals to the FISC.[129]

The messages of cooperation from U.S. and EU officials noted above signal a desire for conversations about what legal framework is necessary to allow global companies to be able to transfer data while government agencies pursue their needs to access that information for legitimate national security and law enforcement purposes. Any resulting framework, however, will be more useful if it applies to more than just access by U.S. government agencies to information held in the United States by domestic companies. Companies from other countries also have a need for international data flows, and those countries will have to demonstrate that their privacy protections provide the requisite level of protection to individuals.[130]

Given the international reach and rapid growth of Chinese technology companies and services such as Huawei, Alibaba, Baidu, Tencent, ZTE, and TikTok,[131] public policy stakeholders are turning their attention to the degree to which those companies transfer data

---

[128] Propp & Swire, *supra* note 104.

[129] *Id.*

[130] *Id.*

[131] Jaime Henriquez, *The Big Seven: China's Up-and-Coming Technology Companies*, TECHREPUBLIC, https://www.techrepublic.com/article/the-big-seven-chinas-up-and-coming-technology-companies/ [https://perma.cc/6DK2-TXKZ] (last visited Apr. 5, 2021).

back to China, and how readily the Chinese government can access that data once it is there.[132] The current dispute between the U.S. government and TikTok's parent company, Bytedance, is an instructive example of how discussions similar to those in the *Schrems* cases are playing out in the U.S.-China relationship.

III. TIKTOK AND THE TRUMP ADMINISTRATION

On January 5, 2021, President Trump issued an executive order ("EO") prohibiting transactions with eight Chinese technology applications, including "Alipay, CamScanner, QQ Wallet, SHAREit, Tencent QQ, VMate, WeChat Pay, and WPS Office."[133] That EO included an explanation of the specific threat to national security that it intended to address:

> By accessing personal electronic devices such as smartphones, tablets, and computers, Chinese connected software applications can access and capture vast swaths of information from users, including sensitive personally identifiable information and private information. This data collection threatens to provide the Government of the People's Republic of China (PRC) and the Chinese Communist Party (CCP) with access to Americans' personal and proprietary information — which would permit China to track the locations of Federal employees and contractors, and build dossiers of personal information.[134]

The January 5, 2021 EO was substantially similar to two Trump Administration actions that received much more press attention: the August 6, 2020 EO ("IEEPA Order")[135] and the August 14, 2020 EO

---

[132] Robert D. Williams, *Beyond Huawei and TikTok: Untangling US Concerns Over Chinese Tech Companies and Digital Security* 30–31(unpublished working paper), https://www.brookings.edu/wp-content/uploads/2020/10/FP_20201030_huawei_tiktok_williams.pdf [https://perma.cc/5QXK-QXTR].

[133] Exec. Order No. 13,971, 86 Fed. Reg. 1,249, 1,250 (Jan. 8, 2021).

[134] *Id.* at 1,249.

[135] Exec. Order No. 13,942, 85 Fed. Reg. 48,637 (Aug. 11, 2020); Sam Byford, *Trump's WeChat Ban Could Touch Everything From Spotify to League of Legends*, VERGE (Aug. 7, 2020, 10:13 AM), https://www.theverge.com/2020/8/7/21358252/tencent-wechat-ban-trump-executive-order-consequences [https://perma.cc/PYC5-TD2C] (explaining the IEEPA order also accompanied a similar Executive Order banning transactions with the application WeChat and its parent company Tencent, which could have even greater significance due to Tencent's diverse business holdings including investments in Spotify, Riot Games, Epic Games, and Supercell).

("CFIUS Order").[136] The International Emergency Economic Powers Act ("IEEPA") is the authority that President Trump used for the IEEPA Order.[137] IEEPA authorizes the President of the United States to impose sanctions on any foreign entity during a declared "national emergency."[138] The IEEPA Order relied upon a prior May 15, 2019 EO that had declared a national emergency due to cybersecurity hacking from "foreign adversaries."[139]

The IEEPA Order included similar language to the January 5th Order describing the risks of Chinese government access to the personal data of U.S. citizens:

> TikTok automatically captures vast swaths of information from its users, including Internet and other network activity information such as location data and browsing and search histories. This data collection threatens to allow the Chinese Communist Party access to Americans' personal and proprietary information — potentially allowing China to track the locations of Federal employees and contractors, build dossiers of personal information for blackmail, and conduct corporate espionage.[140]

The IEEPA Order bans any company within the jurisdiction of the United States from entering into transactions with TikTok or its parent company ByteDance Ltd., and requires the Commerce Department to identify any prohibited transactions.[141]

The CFIUS Order relied on a different Presidential authority. The Committee on Foreign Investment in the United States ("CFIUS") was established under Section 721 of the Defense Production Act of 1950 and then strengthened by regulations to implement the Foreign Investment Risk Review Modernization Act of 2018.[142] CFIUS creates an interagency committee to review

---

[136] Order Regarding the Acquisition of Musical.ly by ByteDance Ltd., 85 Fed. Reg. 51,297 (Aug. 14, 2020).

[137] International Emergency Economic Powers Act, 50 U.S.C §§ 1701–1706.

[138] *Id.* at § 1702.

[139] Exec. Order No. 13,873, 84 Fed. Reg. 22,689, 22,689 (May 17, 2019).

[140] Exec. Order No. 13,942, 85 Fed. Reg. 48,637, 48,637 (Aug. 11, 2020).

[141] *Id.* at 48637–38.

[142] 31 C.F.R. § 800 (2020); *The Committee on Foreign Investment in the United States (CFIUS),* DEP'T OF TREASURY, https://home.treasury.gov/policy-issues/international/the-committee-on-foreign-investment-in-the-united-states-cfius [https://perma.cc/YR8L-8JDB] (last visited Apr. 5, 2021).

transactions involving foreign investment in the United States.[143] A U.S. company does not need to be involved in the transaction, as long as one of the parties is involved in interstate commerce in the United States that threatens to impair national security.[144] If a company does not get prior approval from CFIUS for a transaction, the law allows the committee to impose sanctions, including requiring unwinding the transaction after the fact.[145]

The CFIUS Order calls out that ByteDance Ltd. (a Cayman Islands corporation) purchased Musical.ly (another Cayman Islands corporation) and then merged ByteDance's TikTok operations into Musical.ly.[146] The sanctions in the CFIUS Order require ByteDance to divest itself of the operation of TikTok in the United States and any data provided by TikTok or Musical.ly U.S. users.[147] ByteDance was given ninety days, with a possible extension of another thirty days, to divest both the business and the data.[148]

On September 18, 2020, the Commerce Department issued a statement describing the TikTok transactions that would be prohibited under the IEEPA Order.[149] That statement prohibited online application stores from allowing users to download the TikTok application or software updates to previously downloaded versions of the application.[150] In addition, the Commerce Department disallowed several other types of companies from playing a role in assisting TikTok, including internet hosting

---

[143] *CFIUS Overview,* DEP'T OF TREASURY, https://home.treasury.gov/policy-issues/international/the-committee-on-foreign-investment-in-the-united-states-cfius/cfius-overview [https://perma.cc/2FM9-28MQ] (last visited Apr. 5, 2021).

[144] 31 CFR § 800.101 (2020).

[145] *Id*.

[146] Order Regarding the Acquisition of Musical.ly by ByteDance Ltd, 85 Fed. Reg. 51,297 (Aug. 19, 2020).

[147] *Id*.

[148] *Id*.

[149] Peter Jeydel, et. al., *US Commerce Department Identifies Prohibited Transactions Involving WeChat and TikTok*, STEPTOE (Sept. 20, 2020), https://www.steptoeinternationalcomplianceblog.com/2020/09/us-commerce-department-identifies-prohibited-transactions-involving-wechat-and-tiktok/ [https://perma.cc/DF22-ZSVU].

[150] *Id*.

companies, content delivery services, and transit and peering capability.[151]

However, the IEEPA Order started several lawsuits, including multiple requests for preliminary injunctions.[152] At the same time, TikTok issued a statement describing the considerable efforts they had taken to address the issues raised by the U.S. government and to demonstrate that they should be trusted to operate in the United States.[153] Concurrently, TikTok pursued relationships with U.S. companies to resolve the issues, including a potential arrangement with Oracle and Walmart.[154] Secretary of Commerce Wilbur Ross issued a statement on September 19, 2020, reacting positively to the proposed solution with Oracle and Walmart and delaying implementation of the sanctions until September 27, 2020.[155]

Judge Carl J. Nichols granted TikTok a request for the injunction on September 27, 2020.[156] Judge Nichols' opinion provides more insight into the reasoning of the Department of Commerce when it quotes an internal Commerce Department memo saying:

> Before issuing those prohibited transactions, the Secretary reviewed and relied on a decision memorandum that assessed the threats posed by ByteDance and TikTok . . . In particular, the Secretary of Commerce, found that the PRC is "building massive databases of Americans' personal information" to help the "Chinese government to further its intelligence-gathering and to understand more about who to target for espionage, whether electronically or via human recruitment."[157]

---

[151] *Id*.

[152] Katy Stech Ferek & Georgia Wells, *TikTok Files Another Lawsuit to Block Ban on App*, WALL ST. J. (Sept. 19, 2020), https://www.wsj.com/articles/tiktok-files-another-lawsuit-to-block-ban-on-app-11600541730 [https://perma.cc/7WBB-ZZ5J].

[153] *Why We are Suing the Administration*, TIKTOK, *supra* note 1.

[154] Vanessa Pappas, *An Update for our TikTok Family*, TIKTOK (Sept. 19, 2020), https://newsroom.tiktok.com/en-us/an-update-for-our-tiktok-family [https://perma.cc/4Z4G-P9QS].

[155] Makena Kelly & Kim Lyons, *Preisdent Trump Says He Approves of Oracle's Bid for TikTok 'in Concept'*, THE VERGE (Sept. 19, 2020, 5:55 PM), https://www.theverge.com/2020/9/19/21437850/president-trump-approves-oracle-tiktok-partnership-bytedance-china-ban [https://perma.cc/SL2F-D5CX].

[156] TikTok v. Trump, No. 1:20-CV-02658, 2020 WL 5763634, at *1 (D.D.C. Sept. 27, 2020).

[157] *Id*. at *3.

The opinion further describes the Administration's position for why these risks apply to TikTok:

> The Secretary also found that the CCP will exploit "close ties" with ByteDance to further its foreign policy agenda . . . ByteDance is headquartered in Beijing and remains subject to the PRC's National Intelligence Law, which "permits Chinese intelligence institutions" to "take control of" any China-based firm's "facilities" and "communications equipment." . . . ByteDance has signed a cooperation agreement with a PRC security agency, closed one of its media platforms in response to CCP demands, and (as of August 2020) placed over 130 CCP committee members in management positions throughout the company . . . And because "ByteDance is subject to PRC jurisdiction, [and] PRC laws can compel cooperation from ByteDance, regardless of whether ByteDance's subsidiaries are located outside the territory of the PRC," the data held by ByteDance's subsidiary companies may also be extracted by the PRC.[158]

On October 30, 2020, the United States District Court for the Eastern District of Pennsylvania also issued an injunction against imposition of the IEEPA Order sanctions.[159] Both issued injunctions include language calling into question whether the U.S. government will be successful using IEEPA against TikTok.[160] At the time this Article was written, it is still unclear whether the Biden Administration will continue with the litigation to pursue action against TikTok, will enforce the CFIUS Order, or whether they will revoke the EOs. However, even if the orders are revoked, the underlying risks remain.

Concerns about the national security implications of the Chinese government's access to large amounts of personal information of Americans is not a new issue. Experts have expressed concerns going back at least to the 2017 hack of Equifax[161] and the 2015 theft

---

[158] *Id*.

[159] Maryland v. Trump, No. 20-4597, 2020 WL 6381397 (E.D. Pa. Oct. 30, 2020).

[160] *Id*. at *8–9; *TikTok*, 2020 WL5763634 at *3.

[161] Brian Barrett, *How 4 Chinese Hackers Allegedly Took Down Equifax*, WIRED (Feb. 10, 2020, 12:52 PM), https://www.wired.com/story/equifax-hack-china/ [https://perma.cc/TZ2S-KVMB].

of data from the Office of Personnel Management.[162] What made the concerns about TikTok different was the idea that the Chinese government would not have to illegally obtain the data, but could just demand the information from TikTok under Chinese law.[163]

There are three specific Chinese laws that point to risk that the Chinese government could demand access to information of individuals from the United States that is stored in China, or require TikTok to make changes in its software to transfer such data from the United States back to China (and then to the Chinese government). These three laws are the Cybersecurity Law of 2017 ("Cybersecurity Law"),[164] the Counterrorism Law of 2015 ("Counterrorism Law"),[165] and the National Security Law of 2015 ("National Security Law").[166] Article 28 of the Cybersecurity Law provides:

> Network operators shall provide technical support and assistance to public security organs and national security organs that are safeguarding national security and investigating criminal activities in accordance with the law.[167]

Similar language requiring cooperation by private companies is included in Articles 9 and 84 of the Counterrorism Law:

> All units and individuals have the obligation to assist and cooperate with relevant government authorities in carrying out counter-terrorism efforts, and where discovering suspected terrorist activities or suspected terrorist individuals, shall promptly report to the public security organs or relevant departments.[168]

---

[162] Brendan I. Koerner, *Inside the Cyberattack That Shocked the US Government*, WIRED (Oct. 23, 2016, 5:00 PM), https://www.wired.com/2016/10/inside-cyberattack-shocked-us-government/ [https://perma.cc/DUS2-X2FG].

[163] Richie Koch, *TikTok and the Privacy Perils of China's First International Social Media Platform*, PROTON MAIL (July 23, 2020), https://protonmail.com/blog/tiktok-privacy/ [https://perma.cc/D8J2-X72S].

[164] Cybersecurity Law of the People's Republic of China (Standing Comm. Nat'l People's Cong., Nov. 6, 2016, effective June 1, 2017) (China).

[165] Counter-Terrorism Law of the People's Republic of China (promulgated by the Standing Comm. Nat'l People's Cong., Dec. 27, 2015, effective Jan. 1, 2016) (China).

[166] National Security Law of the People's Republic of China (Standing Comm. Nat'l People's Cong., July 1, 2015) (China).

[167] Cybersecurity Law of the People's Republic of China, art. 28 (China).

[168] Counter-Terrorism Law of the People's Republic of China, at art. 9.

> In any of the following circumstances, the competent departments shall fine telecommunications operators or internet service providers between 200,000 and 500,000 yuan, and fine directly responsible managers and other directly responsible personnel up to 100,000 yuan; where circumstances are serious, the fine is 500,000 or more, and directly responsible managers and other directly responsible personnel are fined between 100,000 and 500,000 yuan, and the public security organs may detain directly responsible managers and other directly responsible personnel for between five and fifteen days:
>
> (1) Not providing technical interfaces, decryption and other technical support assistance to public security organs and state security organs conducting prevention and investigation of terrorist activities in accordance with law.
>
> (2) Not following a competent department's request to stop transmission, delete information that has terrorist or extremist content, store relevant records, or to close down relevant websites, or shut down related services;
>
> (3) Not putting into place systems for network security and supervision of information content, technological security precautionary measures, causing the transmission of information with terrorist or extremist content; where the circumstances are serious.[169]

The National Security law also includes sweeping language requiring assistance from Chinese companies, including in the collection of intelligence:

> Article 53: The carrying out of intelligence information efforts shall fully utilize contemporary scientific and technical techniques, strengthening the distinction, screening, synthesis and analytic assessment of intelligence information.[170]
>
> Article 77: Citizens and organizations shall perform the following obligations to preserve national security.
>
> (1) Obeying the relevant provisions of the Constitution, laws, and regulations regarding national security;
>
> (2) Promptly reporting leads on activities endangering national security;
>
> (3) Truthfully providing evidence they become aware of related to activities endangering national security;
>
> (4) Providing conditions to facilitate national security efforts and other assistance;
>
> (5) Providing public security organs, state security organs or relevant military organs with necessary support and assistance;

---

[169] *Id*. at art. 84.

[170] National Security Law of the People's Republic of China, at art. 53.

(6) Keeping state secrets they learn of confidential [sic];

(7) Other duties provided by law or administrative regulations.

Individuals and organizations must not act to endanger national security and must not provide any kind of support or assistance to individuals or organizations endangering national security.[171]

These vague legal requirements are difficult to interpret. Are Chinese authorities regularly requiring technology companies to provide intelligence assistance, including the inclusion of backdoors, the provision of personal data, the moderation of content on platforms to influence behavior of users, or the use of advanced analytics to analyze information and to supplement information obtained through direct government offensive cybersecurity attacks and other methods like purchasing information from data brokers? Some commentators, such as leading cybersecurity policy expert Samm Sacks, point to the fact that there is little evidence of the Chinese government demanding such assistance from companies.[172] Sacks points to examples of Chinese companies resisting requests from the Chinese government and notes the important interests these companies and the Chinese government have in governments and users around the world trusting Chinese technology products and services.[173]

On July 9, 2020, TikTok published a transparency report that explicitly stated that they had not received any requests for information from the Chinese government.[174] However, Sacks noted that the vagueness of these Chinese legal requirements and the lack of legal structures would not provide trust and confidence: "In China there is no guarantee that the government cannot access data because China's system lacks clarity of law, oversight mechanisms and clear pathways for contestation."[175]

---

[171] *Id*. at art. 77.

[172] Samm Sacks, *Data Security and U.S.-China Tech Entanglement*, LAWFARE (Apr. 2, 2020, 8:00 AM), https://www.lawfareblog.com/data-security-and-us-china-tech-entanglement [https://perma.cc/5DBN-T53X].

[173] *Id*.

[174] *TikTok Transparency Report 2019 H2*, TIKTOK (July 9, 2020), https://www.tiktok.com/safety/resources/transparency-report?lang=en&appLaunch= [https://perma.cc/A49E-WQRQ].

[175] Sacks, *supra* note 172.

Both the U.S. and Chinese governments have the legal ability to require companies to provide them with personal data of citizens of other countries. While that ability is also likely true for many countries, the success and global reach of U.S. and Chinese technology companies makes the issue more prominent with respect to companies like Facebook and TikTok. The data collected by Facebook and TikTok has the potential to create both privacy concerns for individuals and national security risks. The United States and the EU are not the only countries addressing these issues. Recently, India decided to ban the use of many Chinese phone applications over similar concerns.[176] As in the *Schrems* cases, the EU has attempted to address these concerns about U.S. access to data transferred to other countries with enforcement of the requirements of the Directive and GDPR. The United States has attempted to address similar issues with EOs, CFIUS and IEEPA. However, the legal environments in the United States and China are not equivalent.

The United States has a highly detailed set of legal protections for privacy and an independent federal judiciary, while China is still developing many of its similar institutions.[177] The question remains of how governments should evaluate whether those systems (or others) are robust enough to trust technology that could transfer data. If not, then, what criteria should be used? The World Justice Project Rule of Law Index ranks the United States as twenty-first in the world and China eighty-eighth for adherence to the rule of law.[178] That index evaluates the following seven factors: (1) constraints on government powers; (2) absence of corruption; (3) open government; (4) fundamental rights; (5) order and security; (6) regulatory enforcement; and (7) civil justice.[179] Is it possible to

---

[176] Saheli Roy Choudhury, *China is an Opportunity for India — Not a Threat, Beijing Says as More Apps are Banned*, CNBC (Nov. 26, 2020, 11:57 PM), https://www.cnbc.com/2020/11/26/china-responds-to-india-banning-43-additional-chinese-apps.html [https://perma.cc/6HVN-DFLY].

[177] Overcoming Embeddedness: How China's Judicial Accountability Reforms Make its Judges More Autonmous, 43 FORDHAM INT'L L. J. 737, 763–65 (2020).

[178] *WJP Rule of Law Index*, WORLD JUST. PROJECT (2020), https://worldjusticeproject.org/rule-of-law-index/factors/2020 [https://perma.cc/FHV3-BJKV].

[179] *Id.*

develop similar solutions and criteria for the oversight of government engagement with technology companies to properly evaluate what technologies should be allowed market access?

IV. A POTENTIAL SOLUTION

Many U.S. surveillance law and policy experts have expressed doubts about the *Schrems I* and *II* decisions.[180] One of the concerns they note is that if the robust U.S. system of intelligence community oversight and commitment to privacy protections are insufficient, then is it unlikely that any other country will be able to meet the court's standard of "essential equivalence."[181] While the *Schrems II* decision states that Standard Contractual Clauses may still be used to transfer data in some situations, the court's reasoning calls into question whether that will be true for any significant technology service that allows for large quantities of personal data to be accessed and analyzed by government agencies. It is quite possible that Binding Corporate Rules[182] may also fail such a test, since there is nothing inherent in those provisions that can limit the access to data by government agencies.

Therefore, the Court's *Schrems* decisions should not just call into question transfers of personal data from the EU to the United States, but also transfers to countries that have robust surveillance practices, but even less transparency, access to tribunals, or legally enforceable privacy protections. This list of countries should include Russia, India, Israel, Brazil, Turkey, Singapore, Vietnam, and

---

[180] As an example, see Joshua P. Meltzer, *Why Schrems II Requires US-EU Agreement on Surveillance and Privacy*, BROOKINGS (Dec. 8, 2020) https://www.brookings.edu/techstream/why-schrems-ii-requires-us-eu-agreement-on-surveillance-and-privacy/ [https://perma.cc/4JMK-U5E7].

[181] Propp & Swire, *supra* note 104.

[182] Another mechanism for transfer under the Directive and the General Data Protection Regulation that allows corporate entities to bind themselves to sets of rules for data processing and then have those rules approved by the European privacy regulators. *See* 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. 108, 2016 J.O. (L 119) 1, 9.

China.[183] If the three issues noted in the *Schrems II* decision, including (1) bulk versus targeted collection; (2) access to a judicial tribunal; and (3) the independence and authority of the redress mechanism, are applied to the transfer of data from the EU to these other countries, then the EU may become a digital island. However, the impact would be well beyond just digital services, as most companies rely upon the transfer of personal data to provide goods and other non-digital services. It is quite conceivable that the natural extension of the *Schrems II* decision would be to substantially limit European access to essential items, such as oil and natural gas, as it would be extremely difficult to transact business without some exchange of personal data between the business participants.[184]

Likewise, the U.S. approach to TikTok focuses on the possibility of the corporate parent using the software update functionality to begin to export personal data back to China.[185] Similar to the recent SolarWinds cybersecurity attack, automated software updates can be used by nation states to introduce code that can do a variety of things, including exfiltrating data.[186] However, the timely installation of software updates is also critical to patch known cybersecurity vulnerabilities.[187] In theory, the rapid implementation

---

[183] *See* 2017 SURVEILLANCE LAW COMPARISON LAW GUIDE, BAKER MCKENZIE (2017), https://tmt.bakermckenzie.com/-/media/minisites/tmt/files/2017_surveillance_law.pdf?la=en [https://perma.cc/M475-BA4F].

[184] *See From Where do We Import Energy and How Dependent are We?,* EUROSTAT, https://ec.europa.eu/eurostat/cache/infographs/energy/bloc-2c.html [https://perma.cc/QC74-JRNB] (last visited Apr. 9, 2021).

[185] Justin Sherman, *Unpacking TikTok, Mobil Apps and National Security* Risks, LAWFARE (Apr. 2, 2020, 10:06 AM) https://www.lawfareblog.com/unpacking-tiktok-mobile-apps-and-national-security-risks [https://perma.cc/D7YV-5B88].

[186] The updated code can be used to collect information from the service and send it to another location, such as government servers within China. Laura Hautala, *SolarWinds Not the Only Company Used to Hack Targets, Tech Execs Say at Hearing,* CNET (Feb. 24, 2021, 2:56 PM), https://www.cnet.com/news/solarwinds-hack-officially-blamed-on-russia-what-you-need-to-know/ [https://perma.cc/7WD7-KMGH].

[187] *How Malicious Software Updates Endanger Everyone*, ACLU, https://www.aclu.org/issues/privacy-technology/consumer-privacy/how-malicious-software-updates-endanger-everyone [https://perma.cc/Y38A-F2WX] (last visited Apr. 16, 2021).

of software updates makes the entire digital infrastructure more secure.[188] Invalidating the ability for software updates to come from other countries to the United States could have the end result of making the United States less secure.[189]

Both the *Schrems* cases and the TikTok issues boil down to a question of whether the technology can be trusted not to provide information to government agencies in a way that will cause harm to individuals and/or society. Evaluating the security of a given technology requires establishing criteria and standards to determine whether governments and individuals should trust the technology and the countries in which data will be stored. As noted in the prior sections of this Article, the Court in the *Schrems* cases attempts to lay out criteria for what would justify trust. While not necessary for the legal analysis in the cases, it is interesting to note that many EU countries' surveillance frameworks would likely not satisfy the criteria used by the Court.[190] The U.S. government's action against TikTok asserts that technology from China should not be trusted to process large amounts of personal data.[191] If other countries were to adopt the approach taken by the Trump administration towards TikTok, then given the decreasing global trust in the U.S. government and U.S. technology companies, there is a significant risk to market access barriers for U.S. companies.[192] The potential

---

[188] *Id.*; Graham Cluley, *Beware Malicious Software Updates for Legitimate Apps*, BITDEFENDER (June 25, 2018), https://businessinsights.bitdefender.com/malicious-software-updates-legitimate-apps [https://perma.cc/3J2T-AK2Q].

[189] *Understanding Patches and Software Updates*, DEP'T OF HOMELAND SEC. (Nov. 19, 2019), https://us-cert.cisa.gov/ncas/tips/ST04-006 [https://perma.cc/4ZDB-3A5C].

[190] *See* BAKER MCKENZIE, *supra* note 183. Many E.U. member states lack the sufficient transparency, limitations on collection, and oversight. *Id.*

[191] Bobby Allyn, *Trump Signs Executive Order That Will Effectively Ban Use of TikTok In the U.S.*, NPR (Aug. 6, 2020, 11:21 PM) https://www.npr.org/2020/08/06/900019185/trump-signs-executive-order-that-will-effectively-ban-use-of-tiktok-in-the-u-s [https://perma.cc/B79A-TC7R].

[192] *See* Andrea O'Sullivan, *Would Other Countries Trust a U.S. Government-Controlled Silicon Valley?*, REASON (Aug. 18, 2020, 8:30 AM) https://reason.com/2020/08/18/would-other-countries-trust-a-u-s-government-controlled-silicon-valley/ [https://perma.cc/JDA6-JKQJ]; EDELMAN TRUST BAROMETER 2021, EDELMAN (2020), https://www.edelman.com/sites/g/files/

end result of these approaches could be that a country would only trust software developed, sold, and updated from within the borders of that country.

A different approach is needed. A new approach in regulating technology could involve an evaluation of criteria from three categories: (1) a technical analysis of the technology; (2) company commitments made public and legal mechanisms for the government to enforce those promises; and (3) a determination of whether current legal privacy protections, oversight of law enforcement, and agency surveillance activities suffice.

In the first category of technical analysis, significant academic research continues on how to measure the trustworthiness of technology and to identify cybersecurity issues.[193] Conversations around the need for testing and certification continue around the world.[194] While many companies express concern with mandatory certification regimes,[195] there is begrudging acceptance and guidance from companies on how to implement such regimes so

---

aatuss191/files/2021-01/2021-edelman-trust-barometer.pdf [https://perma.cc/B63A-5L2].

[193] Paul Rosenzweig & Claire Vishik, *Trusted Hardware and Software: An Annotated Bibliography*, LAWFARE (Oct. 1, 2020, 10:40 AM), https://www.lawfareblog.com/trusted-hardware-and-software-annotated-bibliography [https://perma.cc/YR5R-ELAV].

[194] *See* Aaron Boyd, *DOD Will Require Vendor Cybersecurity Certifications By This Time Next Year*, NEXTGOV (Sept. 6, 2019), https://www.nextgov.com/cybersecurity/2019/09/dod-will-require-vendor-cybersecurity-certifications-time-next-year/159702/ [https://perma.cc/3TCF-KY32]; *EU Cybersecurity Certification Framework,* ENISA, https://www.enisa.europa.eu/topics/standards/ [https://perma.cc/3676-ZXSK]; Jody Westby, *EU Cybersecurity Certification Schemes Will Surprise U.S. Businesses*, FORBES (Oct. 21, 2019, 10:37 AM) https://www.forbes.com/sites/jodywestby/2019/10/21/eu-cybersecurity-certification-schemes-will-surprise-us-businesses/?sh=1f14542e3802 [https://perma.cc/JT5G-RTKA].

[195] Connie Lee, *Vital Signs 2020: Small Businesses Concerned About New Cybersecurity Certification*, NAT'L DEF. (Jan. 23, 2020), https://www.nationaldefensemagazine.org/articles/2020/1/23/small-businesses-concerned-about-new-cybersecurity-certification [https://perma.cc/5Y5L-EDYX].

they maximize effectiveness.[196] In the absence of mandatory certification, the U.S. National Institute of Standards and Technology ("NIST") has led considerable work on voluntary metrics for trustworthiness of software.[197]

The company commitments included in the second category could consist of public disclosure of companies' adoptions of secure development lifecycle processes, risk management efforts, internal and external audits, specific board oversight, policies on when the company will object legally to government requests, and robust enterprise information security programs. Whether companies have implemented the NIST Cybersecurity Framework[198] and the ISO/IEC 27001 standard[199] are highly relevant factors. Also, the U.S. Department of Justice's principles to evaluate corporate compliance programs[200] and guidance documents from the Information Accountability Foundation[201] both provide useful criteria to measure responsible corporate behavior.

However, effective legal mechanisms for countries to enforce those company promises would then be needed. The United States has at least two such models with Securities and Exchange Commission ("SEC") oversight of statements of publicly traded

---

[196] *See generally* INFO. TECH. INDUS. COUNCIL, POLICY PRINCIPLES FOR CYBERSECURITY CERTIFICATION (2020) https://www.itic.org/policy/ITI_PolicyPrinciplesforCybersecurityCertification_Final.pdf [https://perma.cc/LHL6-JPAJ] (explaining that certification communicates to users of the technology the degree to which they can rely upon the robustness of the security of the particular technology).

[197] *Trustworthy Information Systems*, NIST (Mar. 23, 2018), https://www.nist.gov/itl/trustworthy-information-systems [https://perma.cc/9J7N-9WUY].

[198] *Cybersecurity Framework*, NIST, https://www.nist.gov/cyberframework [https://perma.cc/XX6S-M3UR] (last visited Mar. 23, 2021).

[199] *ISO/IEC 27001 Information Security Management*, ISO, https://www.iso.org/isoiec-27001-information-security.html [https://perma.cc/TLF3-RZM2] (last visited Mar. 23, 2021).

[200] U.S. DEP'T OF JUST., EVALUATION OF CORPORATE COMPLIANCE PROGRAMS (June 2020), https://www.justice.gov/criminal-fraud/page/file/937501/download [https://perma.cc/A4BS-L4GJ].

[201] THE INFO. ACCOUNTABILITY FOUND., https://informationaccountability.org [https://perma.cc/KC7Z-GX93] (last visited Mar. 23, 2021).

companies[202] and the FTC Act Section 5 authority for unfair and deceptive trade practices.[203] Creating an oversight mechanism to evaluate company promises, like that of the SEC or FTC, is necessary, but will be insufficient without robust, harmonized, and predictable enforcement. Such enforcement requires substantial funding, which has been noted by many experts as an issue for the FTC.[204]

The third category of criteria will require a detailed examination of the U.S. legal framework, including the Constitution, laws, regulations, and judicial system. This type of analysis is what the court in *Schrems* did but without a focus on what is a reasonable standard to which all global governments should be held. Such an effort would likely require a centralized global entity with credibility to act as convener. One possible convener could be the Organization for Economic Cooperation and Development ("OECD").[205] The OECD has tremendous credibility in the privacy area from its work on the 1980 Guidelines on the Protection of Privacy and Transborder Data Flows of Personal Data ("OECD Guidelines").[206] Noted privacy expert Paula Bruening has famously described the OECD Guidelines as the global common language of privacy.[207] The OECD has recently announced an effort to lead an

---

[202] *SEC Disclosure Laws and Regulations*, INC. (Jan. 5, 2021), https://www.inc.com/encyclopedia/sec-disclosure-laws-and-regulations.html [https://perma.cc/L55X-UXTH].

[203] *Privacy and Security Enforcement*, FTC, https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy/privacy-security-enforcement [https://perma.cc/Z42X-UP6X] (last visited Mar. 23, 2021).

[204] Chris Jay Hoofnagle et al., *The FTC Can Rise to the Privacy Challenge, but not Without Help from Congress*, BROOKINGS (Aug. 8, 2019), https://www.brookings.edu/blog/techtank/2019/08/08/the-ftc-can-rise-to-the-privacy-challenge-but-not-without-help-from-congress/ [https://perma.cc/6PSD-SLXY].

[205] ORG. FOR ECON. CO-OPERATION DEV., https://www.oecd.org [https://perma.cc/WWE9-BK4Y] (last visited Mar. 23, 2021).

[206] *See OECD Privacy Guidelines*, ORG. FOR ECON. CO-OPERATION DEV., https://www.oecd.org/sti/ieconomy/privacy-guidelines.htm [https://perma.cc/6REX-ULZZ] (last visited Mar. 23, 2021).

[207] Paula Bruening, *Fair Information Practice Principles: A Common Language for Privacy in a Diverse Data Environment*, INTEL (Jan. 28, 2016), https://blogs.intel.com/policy/2016/01/28/blah-2/ [https://perma.cc/WVT3-LPD7].

analysis to "examine the possibility of developing, as a matter of priority, high-level policy guidance for government access to personal data held by the private sector."[208] The announcement described in greater detail that the guidance may include:

> [T]he legal bases upon which governments may compel access to personal data; requirements that access meet legitimate aims and be carried out in a necessary and proportionate manner; transparency; approvals for and constraints placed on government access; limitations on handling of personal data acquired, including confidentiality, integrity and availability safeguards; independent oversight; and effective redress.[209]

V. CONCLUSION

Technology has become fundamental to how individuals live their lives. People around the globe use technology for work, leisure, healthcare, personal finance, education, and to raise families. However, the use of the technology that provides that value also ushers in risks to privacy and security. Most commercially created technology includes hardware, software, and services comprised of component portions delivered as part of a complicated global software and data supply chain. Disconnecting those supply chains and requiring vertical technology supply chain integration within each country will limit the effectiveness of the technology and the benefits to individuals and countries. The *Schrems II* ruling and the U.S. TikTok actions demonstrate the need for a global set of trustworthiness criteria, and that work should begin now.

---

[208] *Government Access to Personal Data Held by the Private Sector: Statement by the OECD Committee on Digital Economy Policy*, ORG. FOR ECON. CO-OPERATION DEV, http://www.oecd.org/digital/trusted-government-access-personal-data-private-sector.htm [https://perma.cc/KW2A-SY4L] (last visited Mar. 23, 2021).

[209] *Id.*