GT GreenbergTraurig

Memorandum

TO:	Dutch Ministry of Justice and Security
FROM:	Greenberg Traurig LLP | Gretchen Ramos and Herald Jongen
DATE:	February 21, 2022
RE:	Schrems II – U.S. Legislation

You have requested us to advise on step 3 of the "Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data", adopted by the EDPB on 18 June 2021. You have asked the following 10 questions regarding the US.

1. Please briefly list the US legislation and regulations (defined in its broadest sense) that were mentioned by the ECJ in Schrems II.
2. Please indicate in that list which legislation and regulations were held by the ECJ not to comply with the rule of law standard of Article 45(2)(a) GDPR.
3. Please confirm if any of this legislation/regulations has recently been changed to such extent that it arguably now meets the rule of law standard.
4. Please briefly list all other US legislation/regulations (i.e. not addressed in Schrems II) that is relevant.
5. Please indicate in that list whether this legislation/regulation arguably meets the Schrems II rule of Law test.
6. Please advise if there are any proposals pending or other developments in the US addressed at remedying the rule of law test.
7. Please indicate if there is any legislation or regulation that formally meets EU standards but that is manifestly not applied/complied with in practice.
8. Please indicate if there are any practices incompatible with the commitments of the SCC where relevant legislation/regulation in the United States is lacking.
9. if applicable, please provide evidence that there is no reason to believe that relevant and problematic legislation/regulation will be applied in practice.
10. Does a commitment of a processor to continue to comply with the requirements of the invalidated Privacy Shield affect the rule of law assessment? If so, how?

We will answer these questions below.

Conclusion

Our conclusion is that the rule of law standard is not always met. This means that step 4 and 5 of the EDPB Recommendations shall be addressed.

Question 1: Please briefly list the US legislation and regulations (defined in its broadest sense) that were mentioned by the ECJ in Schrems II.

Question 2: Please indicate in that list which legislation and regulations were held by the ECJ not to comply with the rule of law standard of Article 45(2)(a) GDPR.

Response: The following U.S. legislation and regulations were mentioned by the ECJ in the Schrems II:

(1) Foreign Intelligence Surveillance Act, Section 702 ("FISA 702")

a. The ECJ concluded that surveillance under FISA 702 does not comply with the rule of law standard of Article 45(2)(a) GDPR.

(2) Executive Order 12333 ("E.O. 12333")

a. The ECJ concluded that monitoring programs based on E.O. 12333 do not comply with the rule of law standard of Article 45(2)(a) GDPR.

(3) Presidential Policy Directive 28 ("PPD-28")

a. The ECJ concluded that PPD-28 permits the monitoring programs in the U.S. based on E.O. 12333, and surveillance programs based on FISA 702 to undertake the bulk collection of a 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', which results in access to data in transit to the United States without that access being subject to any judicial review. As such, the ECJ concluded that PPD-28 does not comply with the rule of law standard of Article 45(2)(a) GDPR.

(4) the Fourth Amendment of the United States Constitution

a. The ECJ notes that the Fourth Amended does not apply to EU citizens.

Question 3: Please confirm if any of this legislation/regulations has recently been changed to such extent that it arguably now meets the rule of law standard.

Response: While there have been many changes to FISA 702 over the years, since the right to redress issue raised in Schrems II has not been addressed it seems unlikely these changes are sufficient to satisfy the rule of law standard.

(1) FISA 702. As described below, FISA 702 has been amended several times to minimize the data processed and to provide further oversight and checks on FISA 702 activities, and three provisions of FISA recently lapsed. As described in more detail below, while the amendments now require more targeted investigations to prevent against mass surveillance; the lack of redress for non-U.S. citizens has not been addressed through the FISA amendments.

The FISA statute permits a person who has been subject to FISA surveillance and whose communications are used or disclosed unlawfully to seek compensatory damages, punitive damages, and attorney's fees against the individual who committed the violation.[1] The Electronic Communications Privacy Act provides a separate cause of action for compensatory damages and attorney's fees against the government for willful violations of various FISA provisions.[2] In addition, individuals may also challenge unlawful government access to personal data, including under FISA, through civil actions under the Administrative Procedure Act ("APA"), which allows persons "suffering legal wrong because of" certain government conduct to seek a court order enjoining that conduct.[3] However, absent such communications being used, there is generally no opportunity for targets of surveillance to know whether their

[1] 50 U.S.C. § 1810.

[2] 18 U.S.C. § 2712.

[3] 5 U.S.C. § 702.

personal data have been acquired by U.S. government officials under Section 702 and such individuals are without standing to seek redress in such circumstances.

Nevertheless, two important points should be noted in relation to FISA. First, absent another extension, FISA will sunset at the end of 2023. Second, pursuant to FISA, certain governmental agencies may seek orders for national security related purposes that require "electronic communication service providers" to disclose communication-related information of specific data subjects.

The term "electronic communications service providers" is defined to include "any service which provides to users thereof the ability to send or receive wire or electronic communications,"[4] U.S. courts have consistently interpreted the definition of "electronic communication service" in 18 U.S.C. § 2510(15) broadly to include even companies that provide employees with email service.[5]

Despite the potentially expansive reach of FISA Section 702, it seems likely—based on the limited public sources available—that the primary targets of NSA collection are major technology firms. For example, the National Security Agency ("NSA")'s summary of its mission suggests that section 702 applies to U.S. telecommunication providers,[6] Also, a 2014 report from the Privacy and Civil Liberties Oversight Board (PCLOB) implied that internet service providers were the key targets of much of the NSA's data collection.[7] The Edward Snowden leaks revealed that Microsoft, Google, Yahoo, AOL and Apple have provided the vast majority

---

[4] 50 U.S.C. § 1881(b)(4) (incorporating definition found in 18 U.S.C. § 2510). The term "electronic communication service provider" includes:

(A) a telecommunications carrier, as that term is defined in section 153 of title 47;

(B) a provider of electronic communication service ("ECS"), as that term is defined in section 2510 of title 18;

(C) a provider of a remote computing service ("RCS"), as that term is defined in section 2711 of title 18;

(D) any other communication service provider who has access to wire or electronic communications either as such communications are transmitted or as such communications are stored; or

(E) an officer, employee, or agent of an entity described in subparagraph (A), (B), (C), or (D).

[5] *See Fraser v. Nationwide Mut. Ins. Co.,* 352 F.3d 107, 114–15 (3d Cir. 2003) (finding defendant provided an electronic communication service because it provided its employees with email services); *Bohach v. City of Reno*, 932 F. Supp. 1232 (D. Nev. 1996) (holding the the city fell within the provisions of the ECPA because it provided pager service to its police officers);*see also Shefts v. Petrakis*, No. 10-cv-1104, 2011 WL 5930469, at *6 (C.D. Ill. Nov. 29, 2011) ("Authorization to access a 'facility' can be given by the entity providing the electronic communications service, which includes a private employer that provides email service to its employees."); *United States v. Mullins*, 992 F.2d 1472, 1478 (9th Cir. 1993) (finding a travel agency that provides its agents with computer terminals running an electronic reservation system was also held to be an electronic communication service).

[6] "The principal application of this authority is in the collection of communications by foreign persons that utilize U.S. communications service providers. The United States is a principal hub in the world's telecommunications system and FISA is designed to allow the U.S. Government to acquire foreign intelligence while protecting the civilliberties and privacy of Americans." The National Security Agency: Missions, Authorities, Oversight andPartnerships, NSA Release No: PA-026-18 (Aug. 9, 2013), available at https://www.nsa.gov/news-features/pressroom/Article/1618729/the-national-security-agency-missions-authorities-oversight-and-partnerships/; see also 2 Judicial Oversight of Section 702 of the Foreign Intelligence Surveillance Act, National Security Agency (2017),available at https://www.nsa.gov/news-features/speeches-testimonies/Article/1619167/judicial-oversight-of-section702-of-the-foreign-intelligence-surveillance-act/.

[7] PRIVACY AND CIVIL LIBERTIES OVERSIGHT BD., EXEC. OFFICE OF THE PRESIDENT, REPORT ON THE SURVEILLANCE PROGRAM OPERATED PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT [PCLOB 702 REPORT] 33-34 (2014), https://documents.pclob.gov/prod/Documents/OversightReport/823399ae-92ea-447a-ab60-0da28b555437/702-Report-2.pdf; *see also* Sneha Indrajuit et al., FISA's Section 702 & the Privacy Conundrum: Surveillance in the U.S and Globally, HENRY M. JACKSON SCH. OF INT'L STUD. (Oct. 25, 2017), https://jsis.washington.edu/news/controversy-comparisons-data-collection-fisas-section-702/.

of the data that the NSA collected via its 'downstream' collections.[8] And the NSA supplements data collection from these entities with 'upstream' collections from 'communications as they cross the backbone of the internet'.[9] Thus, while firms operating their own email servers could become targets of Section 702 'downstream' data collection under the statute's expansive definitions, such targeting appears infrequent, at least based on currently available information.

In 2008, Title VII was added to FISA. Section 702 of FISA with a 5-year sunset, which has been extended twice, and is now scheduled to sunset at the end of 2023. FISA 702 establishes procedures to collect foreign intelligence when communications travel through the United States' communications infrastructure. Under Section 702, the government may compel electronic communications service providers for a period of up to one year to assist in targeting non-U.S. persons reasonably believed to be located outside the United States.

On April 26, 2017 the Foreign Intelligence Surveillance Court ("FISC")[10] issued an order terminating the legal authority to conduct acquisition of so-called "about" collection under FISA 702, which was a form of FISA 702 collection that acquired communications which contained the selector in the text of the communication.[11] The government's termination of "about" collection was accompanied by new NSA targeting procedures implementing the change, stating that "[a]cquisition conducted under these procedures will be limited to communications to or from persons targeted in accordance with these procedures."[12] The elimination of "about" collection reduces the potential for collection of personal data of EU (and other non-U.S.) citizens because their communications now may no longer be acquired under FISA 702 solely because a communication contains a reference to a lawfully tasked selector. The April 2017 Order specifically provides:

> The NSA Targeting Procedures are amended to state that "[a]cquisitions conducted under these procedures will be limited to communications ***to or from*** persons targeted in accordance with these procedures," NSA Targeting Procedures § I, at 2 (emphasis added), and NSA's Minimization Procedures now state that Internet transactions acquired after March 17, 2017, "that are not to or from a person targeted in accordance with NSA's section 702 targeting procedures are unauthorized acquisitions and therefore will be destroyed upon recognition." NSA Minimization Procedures §3(b)(4)b28 Because they are regarded as unauthorized, the government will report any acquisition of such communications to the Court as an incident of non-compliance.[13]

The targeting procedures detail the requirements that the government must take before tasking a selector, as well as verification steps after tasking, to ensure that the user of the tasked selector is being targeted appropriately under Section 702 – specifically, that the user is, and remains, a non-U.S. person, located outside the United States, whose selector is being tasked

---

[8] *See* Steven Levy, How the NSA Almost Killed the Internet, WIRED (Jan. 7, 2014), https://www.wired.com/2014/01/how-the-us-almost-killed-the-internet/; Julian Sanchez, All About 'About' Collection, JUST SECURITY (Aug. 28, 2017), https://www.justsecurity.org/40384/ado-about/.

[9] OFFICE OF DIRECTOR OF NAT'L INTELLIGENCE, SECTION 702 OVERVIEW (Accessed Feb. 6. 2022), https://www.dni.gov/files/icotr/Section702-Basics-Infographic.pdf.

[10] The Foreign Intelligence Surveillance Court was established by Congress in 1978. The Court entertains applications made by the United States Government for approval of electronic surveillance, physical search, and certain other forms of investigative actions for foreign intelligence purposes.

[11] 7 FISC Memorandum Opinion and Order at 25 (26 Apr. 2017), available at https://www.intelligence.gov/assets/documents/702%20Documents/declassified/2016_Cert_FISC_Memo_Opin_Order_Apr_2017.pdf .

[12] NSA Section 702 Targeting Procedures pt. I (29 Mar. 2017), available at https://www.dni.gov/files/documents/icotr/51117/2016_NSA_702_Targeting_Procedures_Mar_30_17.pdf.

[13] 7 FISC Memorandum Opinion and Order at 25 (26 Apr. 2017) at 17-18.

to acquire foreign intelligence information. An individual determination must be made that each tasked selector meets the requirements of the targeting procedures.[14]

In early 2018, Congress passed the FISA Amendments Reauthorization Act of 2017, extending FISA 702 for six years, and amending the law to include new privacy protections and safeguards. These amendments included:

- requiring that with each annual FISA 702 certification, the government must submit and FISC must approve querying procedures, in addition to targeting procedures and minimization procedures;
- requiring additional steps including notification to Congress before the government may resume acquisition of "about" collection under FISA 702;[15]
- amending the enabling statute for the Privacy and Civil Liberties Oversight Board to allow it to better exercise its advisory and oversight functions; [16]
- adding the Federal Bureau of Investigation and NSA to the list of agencies required to maintain their own Privacy and Civil Liberties Officers, instead of being subject only to their parent department-level officers, to advise their agencies on privacy issues and ensure there are adequate procedures to receive, investigate, and redress complaints from individuals who allege that the agency violated their privacy or civil liberties;[17]
- extending whistleblower protections to contract employees at intelligence agencies;[18] and
- imposing several additional disclosure and reporting requirements on the government, including to provide annual good faith estimates of the number of FISA 702 targets.[19]

---

[14] NSA Section 702 Targeting Procedures pt. I (29 Mar. 2017), available at https://www.dni.gov/files/documents/icotr/51117/2016_NSA_702_Targeting_Procedures_Mar_30_17.pdf, and FBI Section 702 Targeting Procedures (16 Sept. 2019), available at https://www.intelligence.gov/assets/documents/702%20Documents/declassified/2019_702_Cert_FBI_Targeting_17Sep19_OCR.pdf.

[15] *See* FISA Amendments Reauthorization Act of 2017, 50 U.S.C. 1801, Section 103, available at https://www.govinfo.gov/content/pkg/PLAW-115publ118/html/PLAW-115publ118.html. Pursuant to Section 103, should the attorney general and Director of National Intelligence decide to recommence "intentional acquisition of abouts communications," they must inform Congress by written notice thirty days prior to restarting the program. The written notice must include a FISC decision, order, or opinion approving the program and "a summary of the protections in place to detect any material breach." During the thirty-day period of congressional review, the NSA may not perform "about" collection unless the attorney general and DNI determine "that exigent circumstances exist" such that, in the absence of "about" collection, "intelligence important to the national security of the United States may be lost or not timely acquired." The intelligence community must report material breaches—defined as "significant noncompliance with applicable law or an order of the [FISC] concerning any acquisition of abouts communications"—to Congress. Finally, Section 103 provides that the FISC's first review of a Section 702 certification authorizing "about" collection will presumptively present "a novel or significant interpretation of the law," and therefore trigger the appointment of amici curiae under FISA Section 103(i)(2)(A).

[16] *Id*. Section 108 allows the Privacy and Civil Liberties Oversight Board (PCLOB) to exercise the authority of the chairman by unanimous vote when the position of chairman is vacant,

[17] *Id*. Section 109 explicitly adds the NSA and the FBI to the list of agencies required to appoint privacy and civil liberties officers under the Intelligence Reform and Terrorism Prevention Act of 2004 (Title I of Public Law 108-458; 118 Stat. 3688).

[18] *Id*. Section 110 extends whistleblower protections to contractor employees in the intelligence community and of the FBI. It prohibits contractors from taking or failing to take personnel actions "as a reprisal for a lawful disclosure of information" that the disclosing party reasonably believes is evidence of a violation of federal law or other misbehavior.

[19] FISA Amendments Reauthorization Act of 2017, Pub. L. No. 115-118, 132 Stat. 3 (19 Jan. 2018).

In January 2021, the NSA released a document on the guidelines that govern signals intelligence, the so-called SIGINT Annex,[20] which offered further protections for non-U.S. persons abroad, with the main restriction being that data collection should be restricted to foreign intelligence requirements, support to military operations or to protect the safety of a U.S. person held captive and also contained further requirements to filter non-pertinent information.

While the three provisions of FISA described below recently lapsed and are no longer in effect, these changes do not alter FISA such that it now meets the rule of law standard of Article 45(2)(a) GDPR.

- Section 206 of the Patriot Act, amended FISA to permit "roving wiretaps." Specifically, if the surveillance target is taking actions that "may have the effect of thwarting" surveillance (such as using disposable cell phone numbers or email addresses), the government could use a single FISA order to conduct surveillance on new phone numbers or email addresses used by the target without needing to apply to the FISC for a new order.
- Section 215 of the Patriot Act enlarged the scope of business records that the government could request to include "any tangible thing." Section 215 also eased the standard that an applicant must meet to obtain a FISA order compelling the production of "tangible thing[s]." As a result, an applicant for a FISA order needed only to provide "a statement of facts showing that there are reasonable grounds to believe that the tangible things sought are relevant to" a foreign intelligence, international terrorism, or espionage investigation.
- The final expired provision, Section 6001(a) of the Intelligence Reform and Terrorism Prevention Act (IRTPA), also known as the "lone wolf" provision, permitted surveillance of non-U.S. persons who are shown to be engaged in international terrorism, but without requiring evidence linking those persons to an identifiable foreign power or terrorist organization.

(2) E.O. 12333. No**.** Executive Order 12333 was originally signed in 1981, and establishes the Executive Branch framework for the United States national intelligence efforts, and for protecting privacy and civil liberties in the conduct of intelligence activities. It is a general directive organizing U.S. intelligence activities, but does not include any authorization to compel private companies to disclose data

(3) PD-228. No. Presidential Policy Directive 28: Signals Intelligence Activities is an executive branch policy document issued in January 2015, that lays out safeguards aimed at protecting the privacy interests of foreign nationals whose communications are incidentally collected by American intelligence agencies in their surveillance of other foreign nationals who may pose a security threat. Presidential Directives are a specific form of Executive Order that state the Executive Branch's national security policy, and carry the force and effect of law, stating requirements for the Executive Branch. Unlike Executive Orders, which are unclassified and also carry the force of law, Presidential Directives are typically classified and the public is usually not aware of their content.

Question 4: Please briefly list all other U.S. legislation/regulations (i.e. not addressed in Schrems II) that are relevant.

Question 5: Please indicate in that list whether this legislation/regulation arguably meets the Schrems II rule of law test.

Response: Listed below are other U.S. laws, not addressed in Schrems II that require organizations to disclose personal data to public authorities.

[20] Procedures governing the conduct of Department of Defense intelligence activities: Annex governing signals intelligence information and data collected pursuant to section 1.7(c) of E.O. 12333, available at https://assets.documentcloud.org/documents/20454757/redacted-annex-dodm-524001-a.pdf.

1. ECPA. Pursuant to the Electronic Communications Privacy Act of 1986 (ECPA),[21] U.S. law enforcement may access domestic and foreign subscriber data, including the content of the communications, of "wire or electronic communication service providers."[22] The term "electronic communications service providers" is defined to include "any service which provides to users thereof the ability to send or receive wire or electronic communications."[23] The ECPA contains three parts: Title I, known as the Wiretap Act, Title II, the Stored Communications Act (SCA), and Title III, Pen Register/Trap and Trace Devices section.

The Wiretap Act provides an exception for the government to intercept communications or conduct electronic surveillance where it can show probable cause that intercepting communications will reveal evidence of a certain type of crime. If the government can establish such probable cause, the court can issue a warrant authorizing the government to intercept communications for up to 30 days. However, information collected through this process remains subject to limits on its use and disclosure.

The SCA governs the disclosure of user data, content, and non-content to law enforcement.[24] Section 2703 outlines the requirements for disclosure of user information using search warrants, subpoenas, or court orders. While the SCA initially allowed law enforcement to obtain user content via a subpoena if the data had been stored for over 180 days, typically law enforcement is required to obtain a warrant to compel user content. While the SCA requires that notice of the law enforcement request be provided to the user at some point, it allows courts to issue an order barring service providers from notifying the user of the law enforcement request.[25]

The ECPA also expands law enforcement's use of National Security Letters (NSLs), which allow the FBI to compel records from third-party service providers. NSLs are accompanied by an indefinite gag order and prohibit the receiving party from disclosing the existence of the NSL unless certain requirements are met.[26] The Judicial Redress Act of 2015 (JRA) expanded the Privacy Act to apply to foreign citizens such that they can assert a claim and challenge the validity of U.S. federal agency's data collection.[27] However, under the current U.S. case law it is often difficult for a foreign plaintiff to establish standing to bring such a claim.[28] In fact, a party solely alleging the violation of a statutory right without a showing of tangible, actual, and imminent harm is generally precluded from seeking redress in U.S. courts.

Nevertheless, for violations of these rules the ECPA allows for the data subject may bring a civil suit against the agency and/or the individual.[29] But in order to prevail, data subjects do not need to establish proof of harm but must demonstrate that the individual or federal agency's violation of ECPA was "willful."[30] If the

---

[21] 18 U.S.C. § 2709, et seq. https://www.govregs.com/uscode/expand/title18_partI_chapter121_section2703#uscode_8.

[22] 18 U.S.C. § 2709(a).

[23] 50 U.S.C. § 2711(1) (incorporating definition found in 18 U.S.C. § 2510); 18 U.S.C. § 2510).

[24] Stored Communications Act, Pub. L. No. 99-508, 100 Stat. 1848 (1986). Content is generally considered to include information, such as e-mail messages, while non-content information includes transactional or subscriber information. RICHARD M. THOMPSON II & JARED P. COLE, CONG. RESEARCH SERV., R44036, STORED COMMUNICATIONS ACT: REFORM OF THE ELECTRONIC COMMUNICATIONS PRIVACY ACT (ECPA) 5 (2015), https://fas.org/sgp/crs/misc/R44036.pdf.

[25]. A 2703(d) order is a combination of a warrant and a subpoena that allows law enforcement to obtain transactional information, such as user sign-in logs, but not email content.

[26] 18 U.S.C. § 2709(c).

[27] Judicial Redress Act of 2015, Pub. L. 114-126, 130 Stat. 282 (to be codified at 5 U.S.C. § 552a note). Outside of the JRA, foreign nationals may seek redress under the Administrative Procedure Act (APA).

[28] U.S. case law has interpreted standing to require that plaintiffs show (1) an injury-in-fact that is concrete and particularized, and actual or imminent; (2) that there is a causal connection between the injury and the alleged conduct; and (3) that the injury will be redressed by the court's decision. *See Lujan v. Defenders of Wildlife*, 504 U.S. 555, 560–61 (1992); *Spokeo v. Robins*, 136 S. Ct. 1540 (2016).

[29] 18 U.S.C. § 2520, https://uscode.house.gov/view.xhtml?path=/prelim@title18/part1/chapter119&edition=prelim.

[30] 18 U.S.C. § 2520. The civil provision requiring "willful" violation has exceptions for good faith reliance on court orders, grand jury subpoenas, legislative authorizations, statutory authorizations, or a valid request from an investigative or law enforcement officer. 18 U.S.C. § 2520(d). Similarly, there is no "willful" violation where the individual or agency being sued made a good faith determination that the alleged action was valid under ECPA. *Id*.

data subject prevails with a suit against an individual officer, the data subject may receive money damages of at least $1,000 USD, equitable or declaratory relief, reasonable attorney's fees, reimbursement of legal fees, and/or punitive damages.[31] Suits against a US agency may result in actual damages or $10,000 USD, whichever is greater, plus litigation costs.

Thus, the ECPA arguably meets the Schrems II rule of law test as it requires judicial authorization and customer notice of such requests (to the extent such customer notification actually occurs). Furthermore, U.S. law allows individuals whose data have been accessed in violation of ECPA to recover damages directly from responsible federal officials in their personal capacity, municipal governments, and state or local officials. However, in those cases where the customer is never notified, the ECPA likely does not satisfy the Schrems II rule of law test.

2. RFPA. Pursuant to the Right to Financial Privacy Act (RFPA),[32] certain U.S. law enforcement agencies may seek records from financial institutions. If the data importer is not a financial institution,[33] the law enforcement agencies cannot submit a request pursuant to the RFPA.

The RFPA arguably meets the Schrems II rule of law test since to obtain access to copies of, or information contained in a customer's financial records, a government authority, generally, must first obtain one of the following:

- an authorization, signed and dated by the customer, that identifies the records, the reasons the records are being requested, and the customer's rights under the act
- an administrative subpoena or summons
- a search warrant
- a judicial subpoena
- a formal written request by a government agency

Additionally, the RFPA also imposes duties and limitations on financial institutions prior to the release of information sought by government agencies. In addition, the act generally requires that customers receive:

- a written notice of the federal authority's intent to obtain financial records;
- an explanation of the purpose for which the records are sought; and
- a statement describing procedures to follow if the customer does not wish such records or information to be made available.[34]

---

[31] 18 U.S.C. § 2707(c).

[32] 12 U.S.C. § 3414.

[33] See 12 U.S.C. § 3401 which contains the following definition of "financial institution":

> "except as provided in section 3414 of this title, means any office of a bank, savings bank, card issuer as defined in section 1602(n) [1] of title 15 [which defines a "card issuer" as "any person who issues a credit card, or the agent of such person with respect to such card"], industrial loan company, trust company, savings association, building and loan, or homestead association (including cooperative banks), credit union, or consumer finance institution, located in any State or territory of the United States, the District of Columbia, Puerto Rico, Guam, American Samoa, or the Virgin Islands;

[34] Per 12 U.S.C. § 3401, the U.S. government authority must serve the subpoena or summons on the customer and provide the following notice:

> Records or information concerning your transactions held by the financial institution named in the attached subpoena or summons are being sought by this (agency or department) in accordance with the Right to Financial Privacy Act of 1978 for the following purpose: If you desire that such records or information not be made available, you must:
>
> 1. Fill out the accompanying motion paper and sworn statement or write one of your own, stating that you are the customer whose records are being requested by the Government and either giving the reasons you believe that the records are not relevant to the legitimate law enforcement inquiry stated in this notice or any other legal basis for objecting to the release of the records.
>
> 2. File the motion and statement by mailing or delivering them to the clerk of any one of the following United States district courts:
>
> 3. Serve the Government authority requesting the records by mailing or delivering a copy of your motion and statement to
>
> 4. Be prepared to come to court and present your position in further detail.

3. CLOUD Act. Pursuant to the Clarifying Lawful Overseas Use of Data Act ("CLOUD Act"), U.S. government agencies may seek any information from a communications service provider ("CSP")[35] who is subject to U.S. law, regardless of where the information is stored or located. The CLOUD Act defines CSPs to include "remote computing services" (the provision to the public of computer storage or processing services by means of an electronic communications system) as well as "electronic communication services" (any service which provides users the ability to send or receive wire or electronic communications).

The Cloud Act arguably does not meet the Schrems II rule of law test to the extent the request made under the CLOUD Act is made through the courts. Nevertheless, it is important to note that the presence of the CLOUD Act does not increase the risk that the U.S. government will access data transmitted to the United States because the CLOUD Act focuses on access to data held overseas. This means that the CLOUD Act would permit access to data stored abroad but have no effect on data stored in the United States, and thus, the CLOUD Act does not provide a rationale for limiting transfers of personal data to the United States.

Where instead the parties rely on bi-lateral agreements with foreign countries negotiated by the Executive branch, the process arguably does meet the Schrems II rule of law test.[36] This is because, these agreements eliminate conflicts of law issues, allowing CSPs to disclose electronic data directly to foreign authorities pursuant to covered orders without the use of a mutual legal assistance treaty. The CLOUD Act requires that all agreements with foreign territories include numerous provisions protecting privacy and civil liberties, and may only allow orders to be used to obtain information relating to the prevention, detection, investigation, or prosecution of serious crime, including terrorism. Among other things, all covered orders must be subject to review or oversight by an independent authority, such as a judge or magistrate.

4. Administratively Issued Subpoena or Demand. Approximately 335 U.S. federal agencies have the ability to issue administrative subpoenas or civil investigatory demands compelling the production of documents or information from U.S. organizations. This includes, for example, the Securities Exchange Commission (SEC) and the Federal Trade Commission (FTC). Agencies in each of the fifty U.S. states have similar investigatory powers.

Since administrative agencies are established by statute, a statute must authorize their issuance of administrative subpoenas. Administrative subpoena authorities permit executive branch agencies to issue a compulsory request for documents or testimony without prior approval from a grand jury, court, or other judicial entity. If a federal governmental agency did not have sufficient investigatory powers, including some authority to issue administrative subpoena requests, it would be unable to fulfill its statutorily imposed responsibility to implement regulatory or fiscal policies. Thus, Congress has granted some form of administrative subpoena authority to most federal agencies. In some instances, the decision to issue a subpoena is made unilaterally by an agency official; in other instances, the issuance of a subpoena requires the vote, approval, or resolution of multiple individuals. [37]

---

5. You do not need to have a lawyer, although you may wish to employ one to represent you and protect your rights.

If you do not follow the above procedures, upon the expiration of ten days from the date of service or fourteen days from the date of mailing of this notice, the records or information requested therein will be made available. These records may be transferred to other Government authorities for legitimate law enforcement inquiries, in which event you will be notified after the transfer."

[35] 18 U.S.C. 2523 (2021) (incorporating definition found in 18 U.S.C. § 2510 and 18 U.S.C. §2711(2)).

[36] *See* Marcin Rojscscak "CLOUD act agreements from an EU perspective," Computer Law & Security Review, Volume 38, September 2020, https://www.sciencedirect.com/science/article/pii/S0267364920300479, accessed February 6, 2022 (noting that "The assumption is that these will be bilateral agreements (the so-called congressional-executive agreement), under which each of the parties may address orders regarding the handover of electronic evidence directly to CSPs [cloud service providers] that operate under the law of the other party.")

[37] For more information regarding administrative subpoena authorities see U.S. Department of Justice Office of Legal Policy, Report to Congress on the Use of Administrative Subpoena

Authorities by Executive Branch Agencies and Entities, Pursuant to P.L. 106-544, Section 7 (2001), https://www.justice.gov/archive/olp/rpt_to_congress.htm#f89.

The Supreme Court has construed administrative subpoena authorities broadly and has consistently permitted the expansion of the scope of administrative investigative authorities, including subpoena authorities, in recognition of the principle that overbearing limitation of these authorities would leave administrative entities unable to execute their respective statutory responsibilities. [38] While an agency's exercise of administrative subpoena authority is not subject to prior judicial approval, a subpoena issuance is subject to judicial review upon a recipient's motion to modify or quash the subpoena or upon an agency's initiation of a judicial enforcement action.

Unlike grand jury subpoenas, there is no general expectation of secrecy for administrative subpoenas, and it is unclear whether a third-party recipient is forbidden from disclosing the existence and content of a subpoena to the target of an investigation. For example, one statute, which authorizes administrative subpoenas in several federal crimes, including health care offenses, child exploitation, and threats to Secret Service protectees, permits the government to seek *ex parte* gag orders under specified circumstances such as when notice risks "endangerment to the life or physical safety of any person," "flight to avoid prosecution," "destruction of or tampering with evidence," or the "intimidation of potential witnesses."[39]

To determine whether a specific administrative subpoena meets the Schrems II rule of law test would require a detailed analysis of each statute authorizing each federal agency with such subpoena power. Although companies receiving subpoenas can file objections and challenge them before a court, courts are often deferential to the agency requesting the subpoena. Furthermore, depending on the statute providing the subpoena authority and the specific circumstances, the party receiving the administrative subpoena or civil investigatory demand may be precluded from disclosing that fact to a third party. This is especially true in those instances where the U.S. federal agency asserts "state secrets privilege" which allows the U.S. government to block the disclosure of particular information in a lawsuit where the disclosure of that information would cause harm to national security.[40] And recently the government has successfully used the state secrets privilege to keep entire cases out of court based on their subject matter.[41]

Even if an EU data subject is notified of such processing by a federal agency, as previously noted, although foreign nationals can assert a claim pursuant to the Judicial Redress Act, under U.S. case law it could be difficult for a foreign citizens to establish standing to bring such a claim without a showing of tangible, actual, and imminent harm.[42] This holds true for administratively issued subpoenas, as well as in relation to search warrants, judicially issues subpoenas, and grand jury subpoenas (addressed below).

Therefore, for the reasons described above, it appears likely that at least some of the federal agencies' administratively issues subpoenas would not satisfy the Schrems II rule of law test.

5. Search Warrant. A search warrant is a court order that a judge issues to authorize a law enforcement officer to conduct a search of a person, office, or other location to identify, and confiscate, evidence of a crime. As noted above, there is always the possibility that a federal agency making such request successfully asserts a privilege barring the company that receives a search warrant from disclosing that fact to a third party. Consequently, to the extent the company receiving the search warrant is precluded from informing the third party whose information is at issue of the search warrant, such search warrants arguably would not meet the Schrems II rule of law test.

---

[38] See *Endicott Johnson Corp. v. Perkins*, 317 U.S. 501 (1943); *Oklahoma Press Publishing Co. v. Walling*, 327 U.S. 186 (1946); *United States v. Morton Salt Co*., 338 U.S. 632 (1950).

[39] 18 U.S.C. § 3486(a)(6)(B); id. § 3486(a)(6)(A) ("A United States district court for the district in which the summons is or will be served, upon application of the United States, may issue an ex parte order that no person or entity disclose to any other person or entity . . . the existence of such summons for a period of up to 90 days."); id. § 3486(a)(6)(C) ("An order under this paragraph may be renewed for additional periods of up to 90 days upon a showing that the circumstances described in subparagraph (b) continues to exist.").

[40] *See United States v. Reynolds*, 345 U.S. 1 (1953).

[41] *See Mohamed v. Jeppesen Dataplan, Inc*., 614 F.3d 1070, 1093 (9th Cir. 2010) (dismissing challenge to U.S. government's extraordinary rendition and torture program on state secrets grounds).

[42] U.S. case law has interpreted standing to require that plaintiffs show (1) an injury-in-fact that is concrete and particularized, and actual or imminent; (2) that there is a causal connection between the injury and the alleged conduct; and (3) that the injury will be redressed by the court's decision. *See Lujan v. Defenders of Wildlife*, 504 U.S. 555, 560–61 (1992); *Spokeo v. Robins*, 136 S. Ct. 1540 (2016).

6. Judicially Issued Subpoena. A judicially issued subpoena is a formal written order issued by a judge that commands a person, or a company, to appear before a court, or to provide information to an officer of a court under penalty for failure to comply. Unless a party to the litigation successfully asserts a privilege, such as the "state secrets privilege" noted above, courts cannot prohibit a company that receives a judicial subpoena from disclosing that fact to a third party. To the extent a third party's personal data is at issue, and the third party is informed of the subpoena, the third party then will have the chance to object to the subpoena, and file a request for an order to quash the subpoena or seek a protective order[43] Thus, barring an privilege assertion which prevents the party receiving the subpoena of notifying the impacted third party of the subpoena, a judicially issued subpoena would arguably be compliant with the Schrems II rule of law test.

7. Grand Jury Subpoena. A grand jury is a judicially convened group of citizens that make a determination as to whether to charge an individual with a crime. A grand jury subpoena is a subpoena issued as part of a grand jury's inquiry. With respect to whether the third-party recipient of a grand jury subpoena can notify the record owner, Federal Rule of Criminal Procedure 6(e) prohibits, with limited exceptions, disclosure of matters occurring before the grand jury generally, but does not gag grand jury witnesses. Thus, a grand jury subpoena, or the letter accompanying a grand jury subpoena, may request that a company not disclose the subpoena, the investigation, or the documents or information requested, as a disclosure, if made, may impede a criminal investigation or impact national security. That said, some courts exercising their inherent authority over grand jury proceedings will issue a protective order prohibiting witness disclosures during an ongoing investigation upon a showing of "compelling necessity."[44]

Grand jury subpoenas arguably do not meet the Schrems II rule of law test since like FISA 702 requests, there is no effective means of redress by the targeted data subject unless the communication is used against them in a later proceeding.

Question 6: Please advise if there are any proposals pending or other developments in the U.S. addressed at remedying the rule of law test.

Response: In January 2021, one of the first steps the Biden administration took was to appoint Christopher Hoff as the new deputy assistant secretary for services in the Commerce Department's International Trade Administration to negotiate a new transatlantic transfer tool in light of Schrems II. Mr Hoff and European Commission Head of International Data Flows and Protection, Bruno Gencarelli, have both publicly committed to working together to find a resolution. And given the market pressures on both jurisdictions to facilitate cross-border data transfers it seems likely that some sort of agreement will be reached in 2022. However, if the new framework does not offer EU citizens adequate redress such as the ability to submit complaints to an independent judicial body if they believe U.S. national security agencies have unlawfully handled their personal information, then it will likely again be challenged in the courts.

It seems the surveillance issues present in both Safe Harbor and Privacy Shield can only be resolved with a shift in U.S. national security policies. If FISA is not extended again, it will sunset at the end of 2023, which could resolve the issue (at least as to FISA 702); however, as noted above there are other U.S. legal practices that likely do not meet the Schrems II rule of law test, so until the U.S. alters its laws it seems unlikely the issue will be resolved.

In late 2019, two promising pieces of federal privacy legislation were introduced: (1) the United Stated Data Privacy Act ("USCDPA"), and (2) the Consumer Data Privacy and Security Act ("CDPSA"). In 2021, the CDPSA was reintroduced in the Senate, and the Information Transparency & Personal Data Control Act was introduced in the House of Representatives. However, the COVID-19 pandemic and the 2020 elections diverted Congress's attention from the proposed federal privacy legislation. And while there is general agreement on several significant privacy issues, strong

[43] *See generally* Rule 45, Federal Rules of Civil Procedure.

[44] *See In re Subpoena to Testify Before Grand Jury Directed to Custodian of Records*, 864 F.2d 1559 (11th Cir. 1989); *In re Grand Jury Subpoena Duces Tecum*, 797 F.2d 676 (8th Cir. 1986); *In re Swearingen Aviation Corp*., 486 F. Supp. 9 (D. Md. 1979), *mandamus refused*, 605 F.2d 125 (4th Cir. 1979) (targets do not have standing to object to court imposed witness secrecy).

disagreement remains over whether federal privacy legislation will preempt state privacy laws and whether the federal privacy law will provide individuals with a right to bring lawsuits for privacy violations. As 2022 is another election year, it seems unlikely that federal privacy legislation will be passed in the U.S. before 2023.

Question 7: Please indicate if there is any legislation or regulation that formally meets EU standards but that is manifestly not applied/complied with in practice.*

Response: The U.S. state privacy laws that will come into effect in 2023 (the California Privacy Rights Act, the Virginia Consumer Data Protection Act, and the Colorado Privacy Act), have many requirements that align with the GDPR. However, even in these states which have adopted strong data protection laws, to the extent an organization is subject to FISA 702, these state privacy laws will not offer data subjects the judicial redress outlined in Schrems II.

Question 8: Please indicate if there are any practices incompatible with the commitments of the SCC where relevant legislation/regulation in the United States is lacking.*

Response: See discussion above in relation to response to Questions 4 and 5. While entities subject to the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), the Gramm-Leach-Bliley Act ("GLBA"), or the new data protection laws in California, Virginia and Colorado are required to adhere to practices largely compatible with the commitments contained in the SCCs, entities not subject to these laws are not required to adhere to many of the SCC commitments. For example, organizations not subject to these U.S. data protection laws would not be required: (1) to adhere to the purpose, transparency, accuracy or data minimization principles described in Clause 8 of the SCC, or (2) to have data processing contracts in place with their processors.

Question 9: If applicable, please provide evidence that there is no reason to believe that relevant and problematic legislation/regulation will be applied in practice.*

Response: In relation to FISA 702, the U.S. Department of Commerce introduced a white paper in September 2020 entitled "Information on U.S. Privacy Safeguards Relevant to SCCs and Other EU Legal Bases for EU-U.S. Data Transfers after Schrems II" ("White Paper"),[46] to assist organizations in conducting independent analyses of data transfers in light of the Schrems II decision. In the White Paper, the U.S. Department of Commerce outlines privacy safeguards relating to government access to data provided by U.S. law, and asserts that most U.S. organizations do not handle data that U.S. intelligence agencies are interested in and therefore do not engage in data transfers that present the type of privacy risks that appear to concern the ECJ.

The Annual Statistical Transparency Report for 2020, published by the Office of the Director National Intelligence supports the limited use of FISA 702. The Transparency Report identifies the following number of FISA 702 court orders: 1 in 2018, 2 in 2019 and 1 in 2020, and notes the following estimated number of targets relating to such orders as 164,770 for 2018, 204,968 for 2019 and 202,723 for 2020.[47] The report also notes the number of criminal proceedings where a government agency provided notice of their intent to enter into evidence or disclose any information obtained or derived from electronic surveillance, physical search or Section 702 acquisition was 14 cases in 2018, 7 cases in 2019 and 9 cases in 2020. The actual number of criminal cases in which the U.S. government relied on information obtained in relation to Section 702 are low in comparison to the number of targets for each of the corresponding years. While the number of targets have doubled since 2015,[48] in total the number of targets remains low, which supports the U.S. Department of Commerce's position that FISA 702 has a limited application.

* As mentioned in step 3 of the EDPB Recommendations.

[46] *See* https://www.commerce.gov/sites/default/files/202009/SCCsWhitePaperFORMATTEDFINAL508COMPLIANT.PDF

[47] *See* Office of Director of National Intelligence, "Annual Statistical Transparency Report Regarding the Intelligence Community's Use of National Security Surveillance Authorities (April 2021), last accessed Feb. 6, 2022, https://www.dni.gov/files/CLPT/documents/2021_ASTR_for_CY2020_FINAL.pdf.

[48] *See* Office of Director of National Intelligence, "Annual Statistical Transparency Report Regarding the Intelligence Community's Use of National Security Surveillance Authorities (April 2018), last accessed Feb. 6, 2022,

Question 10: Does a commitment of a processor to continue to comply with the requirements of the invalidated Privacy Shield affect the rule of law assessment? If so, how?

Response: Probably not. The rule of law assessment is tied to whether EEA data subjects have the right to an effective judicial review designed to ensure compliance with provisions of EU law. While the Privacy Shield Framework requires processors to certify to certain principles, the fact remains that the Ombudsperson Mechanism is not sufficient. As noted in Schrems II, this mechanism does not provide any cause of action before a body which offers the person whose data is transferred to the United States guarantees essentially equivalent to those required by Article 47 of the Charter as the Ombudsperson neither acts independently, nor does he have the power to adopt decisions that are binding on the relevant intelligence organizations.

Question 11: To what extent does the Dutch State's immunity protect data that are held by the Dutch Government and its civil servants? This question 11 may be answered after a quick scan, it does not need to be a full and final advice/opinion.

Response: From an international law perspective, there is no general treaty on sovereign immunity. The United Nations has put together a proposed Convention on Jurisdictional Immunities of States and Their Property but it has not come into effect, and the United States is not a party. [49] Thus, sovereign immunity is considered customary international law (CIL).

Some countries, such as the United States, have chosen to codify this CIL in a statute. When a codified statute is inconsistent with CIL, however, numerous U.S. courts have held the President has the "domestic legal authority" to violate CIL and that it is "subordinate in the U.S. legal system to federal legislation."[50] Thus, the Foreign Sovereign Immunities Act (FSIA), which grants foreign states immunity from suit in US courts (federal or state) unless an exception applies,[51] would prevail over inconsistent CIL, at least in the U.S. domestic legal system.

Since the enactment of the FSIA in 1976, the general exceptions to the jurisdictional immunity of a foreign state have expanded. Specifically, 28 U.S.C. 1605 now provides that a foreign state shall not be immune from the jurisdiction of courts of the United States or of the states in any case in which:

> 1605(a) (1) - explicit or implicit waiver of immunity by the foreign state;
>
> 1605(a)(2) - commercial activity carried on in the United States or an act performed in the United States in connection with a commercial activity elsewhere, or an act in connection with a commercial activity of a foreign state elsewhere that causes a direct effect in the United States;
>
> 1605(a)(3) - property taken in violation of international law is at issue;
>
> 1605(a)(4) - rights in property in the United States acquired by succession or gift or rights in immovable property situated in the United States are at issue;

---

https://www.dni.gov/files/documents/icotr/2018-ASTR----CY2017----FINAL-for-Release-5.4.18.pdf, which notes the estimated number of targets of such orders was 89,138 for 2013, 92,707 for 2014, 94,368 for 2015, 106,469 for 2016, and 129,080 for 2017.

[49] *See generally* CURTIS A. BRADLEY, INTERNATIONAL LAW IN THE U.S. LEGAL SYSTEM 233-56 (2d ed. 2015).

[50] *See United States v. Yousef*, 327 F.3d 56, 93 (2d Cir. 2003) ("[W]hile courts are bound by the law of nations which is a part of the law of the land, Congress may manifest it's will to apply a different rule by passing an act for the purpose.") (internal quotations omitted); *BarreraEchavarria v. Rison*, 44 F.3d 1441, 1450-51 (9th Cir. 1995) ("It is well-settled, however, that international law controls only 'where there is no treaty, and no controlling executive or legislative act or judicial decision.'"); *Gisbert v. U.S. Attorney General,* 988 F.2d 1437, 1447 (5th Cir.), amended, 997 F.2d 1122 (5th Cir. 1993) ("Public international law controls, however, only 'where there is no treaty and no controlling executive or legislative act or judicial decision . . . .'").

[51] 28 U.S.C. § 1602 (2012).

1605(a)(5) - money damages are sought against a foreign state for personal injury or death, or damage to or loss of property, occurring in the United States and caused by the tortious act or omission of that foreign state;

1605(a)(6) - action brought to enforce an agreement made by the foreign state with or for the benefit of a private party to submit to arbitration;

1605(A)(a)(1) - money damages are sought against a foreign state for personal injury or death that was caused by an act of torture, extrajudicial killing, aircraft sabotage, hostage taking, or the provision of material support or resources for such an act, if the foreign state is designated as a state sponsor of terrorism under section 6(j) of the Export Administration Act of 1979 (50 U.S.C. App 2405(j) or Section 620A of the Foreign Assistance Act of 1961 (22 U.S.C. 2371).

1605(b) - a suit in admiralty is brought to enforce a maritime lien against a vessel or cargo of the foreign state which maritime lien is based upon a commercial activity of the foreign state.

Thus, unless one of the exceptions above applies, the Dutch State would be immune to suit in the United States.[52] However, this immunity does not necessarily shield the Dutch State's data from foreign surveillance practices.

=0=

[52] *See generally Doe v. Federal Democratic Republic of Ethiopia*, 189 F. Supp. 3d 6 (D.D.C. 2016), *aff'd*, No. 16-7081, 2017 WL 971831 (D.C. Cir. 2017) (finding the Wiretap Act did not support liability for a country-defendant, and that the intrusion upon seclusion claim was blocked by the FSIA, and D.C. Circuit upholding decision finding that due to the "entire tort rule," the noncommercial tort exception was in applicable, and consequently the U.S. did not have jurisdiction over Ethiopian authorities under FSIA.).