Schrems II Transfer Risk Assessment for CBRE U.S.

A. Executive Summary

In light of the decision by the European Court of Justice ("**ECJ**") of 16 July 2020 (C-311/18; "**Schrems II**"), as set out in more detail below, CBRE, Inc. and its EU/EEA affiliates (collectively "**CBRE**") have reached the conclusion, with the assistance of CBRE's outside counsel and by consulting various sources in the U.S. with relevant expertise and experience under U.S. national security law, that:

1. **EEA Personal Data is protected from disclosure to U.S. intelligence authorities as CBRE US is not an "electronic communication service provider":**
   Transfers of the personal data of European Economic Area ("**EEA**") persons under the protection of the GDPR ("**EEA Personal Data**") to CBRE, Inc. and its U.S.-based affiliates ("**CBRE US**") are protected from disclosure to U.S. intelligence authorities because CBRE US is not an "electronic communication service provider" within the meaning and context of the Foreign Intelligence Surveillance Act (50 U.S.C. § 1810 *et al*) ("**FISA**") Section 702 (50 U.S.C. §1881a), and therefore U.S. intelligence authorities cannot lawfully impose a data disclosure demand under FISA Section 702 upon CBRE US.

2. **EEA Personal Data transferred to CBRE US is protected from disclosure to U.S. intelligence authorities as it is considered "communication data of U.S. persons":**
   Transfers of EEA Personal Data to CBRE US are additionally protected from disclosure because U.S. intelligence authorities cannot target the "communication data of U.S. persons" and personal data CBRE US receives (directly or indirectly as an intermediary for hosting / processing purposes) qualifies as such protected U.S. person communication data within the meaning and context of FISA Section 702 and Executive Order 12333 ("**EO 12333**"). Moreover, all data encrypted during transmission serves as an additional layer of protection from disclosure to U.S. intelligence authorities.

3. **EEA Personal Data hosted on CBRE US's behalf by U.S. cloud service providers is protected from disclosure to U.S. intelligence authorities because it remains the "communication data of U.S. persons" and may not be targeted under FISA Section 702 and EO 12333:**
   EEA Personal Data transferred to CBRE US and hosted by CBRE US's commercial cloud service providers headquartered in the U.S. ("**U.S. Hosting Providers**") is also protected from disclosure to U.S. intelligence authorities as such hosted data remains "communication data of U.S. persons" and may not be targeted under FISA Section 702 and EO 12333. The U.S. Hosting Providers therefore have no legal obligation to comply with a data disclosure demand under FISA Section 702 for purposes of targeting any communications of U.S. persons (whether individuals or corporate entities); and CBRE US relies on U.S. Hosting Providers who have committed to challenging any such unlawful data disclosure demand in order to prevent the disclosure of EEA Personal Data.

4. **EEA Personal Data is protected as the U.S. legal system provides essentially equivalent safeguards and remedies not considered by the ECJ:**
   The current legal system of the U.S. provides for certain additional safeguards and remedies for non-U.S. persons which have not been considered by the ECJ in Schrems II but which provide essentially equivalent protection for the rights and liberties of EEA persons when their personal data under the protection of the GDPR (i.e., their EEA Personal Data) is transferred from the EEA to CBRE US. These additional safeguards and remedies include but are not limited to: strict

oversight of the data collection process by all three branches of the U.S. government, including by the FISA Court, independent federal courts, Congress, the U.S. Attorney General, the independent Privacy and Civil Liberties Oversight Board, and Inspector General, as well as statutory remedies for aggrieved individuals (including non-U.S. persons) in the form of private rights of civil action, damages and compensation of attorneys' fees to individuals of any nationality (including EEA citizens) for purposes of seeking redress in U.S. courts for violations of FISA Section 702.

5. **CBRE US has not been subject to FISA Section 702 demands:**
As of this writing, CBRE US has not received any National Security Letters or FISA court orders from U.S. intelligence authorities. In its final recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data[1] ("**Recommendation on Supplementary Measures**") the European Data Protection Board ("**EDPB**") confirms that transfers of EEA Personal Data may proceed without implementing supplementary measures if there is no reason to believe that relevant and problematic legislation in the third country will be applied in practice to such transferred data.

Conclusion:

Consequently, any supplementary measures for the transfer of EEA Personal Data to CBRE US (such as contractual, organizational and technical measures) as required by the ECJ in Schrems II and the EDPB pursuant to Art. 46 (1) and 45 GDPR are unwarranted. In any case, to provide additional comfort on the level of protection afforded to any EEA Personal Data that is transferred from the EEA to CBRE US, CBRE may implement any or all of the supplementary measures described in Section III below.

B. Analysis

In light of Schrems II, CBRE US has assessed, with the assistance of outside counsel and by consulting various resources in the U.S. with relevant expertise and experience, (i) the current legal system of the U.S., in particular the additional safeguards and remedies that are available under the U.S. legal system to data subjects whose personal data is transferred to the U.S., (ii) whether and to what extent CBRE US is subject to FISA Section 702 and may thereby lawfully receive any data disclosure demands by U.S. intelligence authorities under FISA Section 702, and (iii) whether and to what extent the EEA Personal Data that is transmitted to CBRE US can be subject to surveillance measures based on EO 12333. We note that, as of this writing, CBRE Inc. has not received any National Security Letters or FISA court orders from U.S. intelligence authorities.[2]

I. Current Legal System of the U.S., in particular Additional Safeguards and Remedies for Non-U.S. Persons

1. Scope of U.S. Intelligence Gathering Program

1.1 FISA Section 702

[1] https://edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-012020-measures-supplement-transfer_en.

[2] In on the Recommendation on Supplementary Measures published on June 18, 2021, the EDPB noted that, while the absence of prior data demand requests alone should not be viewed as dispositive for purposes of assessing risk post-Schrems II, organizations may take into account their practical experience with data demands from law enforcement authorities to inform their overall level of risk. *See* https://edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-012020-measures-supplement-transfer_en.

FISA outlines in considerable detail the scope for U.S. intelligence gathering activities. Under FISA Section 702, among other things, data collection must be targeted (i.e., not bulk) and limited to non-U.S. person targets located outside the U.S. who are expected to possess, receive, and/or are likely to communicate foreign intelligence information that is specified in one of the certifications approved by the Foreign Intelligence Surveillance Court ("**FISC**"). While CBRE accepts the ECJ's decision as binding, it is worth noting that the independent Privacy and Civil Liberties Oversight Board[3] described the FISA Section 702 intelligence-gathering program as follows:

> "Although the program is large in scope and involves collecting a great number of communications, it consists entirely of targeting individual persons and acquiring communications associated with those persons, from whom the government has reason to expect it will obtain certain types of foreign intelligence. The program does not operate by collecting communications in bulk…. [T]he Section 702 program is not based on the indiscriminate collection of information in bulk. Instead, the program consists entirely of targeting specific persons about whom an individualized determination has been made. …. [T]he Board does not regard Section 702 as a 'bulk' collection program, because it is based entirely on targeting the communications identifiers of specific people…."[4].

1.2 EO 12333

EO 12333 is reflective of a policy regime governing intelligence gathering activities. Comprised of three parts, EO 12333:

(i) establishes the goals of U.S. intelligence and assign roles and responsibilities to the entities that comprise the U.S. intelligence community ("**IC**");

(ii) explains the need for foreign intelligence information and establishes principles that balance that need with the protection of the rights of U.S. persons. It specifically requires IC elements to adopt certain procedures for the collection, retention, and dissemination of information concerning U.S. persons and the use of specific collection techniques; and

(iii) addresses oversight, instructs intelligence agencies on how to implement the EO 12333, and defines certain terms.

As with other elements of U.S. law, EO 12333 does not operate in a vacuum. Other executive orders, policy directives, statutes, or the like may impose requirements above and beyond those

[3] The Privacy and Civil Liberties Oversight Board is an independent agency within the executive branch of the United States government, established by Congress in 2004 to advise the President and other senior executive branch officials to ensure that concerns with respect to privacy and civil liberties in the United States are appropriately considered in the development and implementation of all laws, regulations, and executive branch policies related to terrorism.

[4] Report on the FISA Section 702 Surveillance Program, Privacy and Civil Liberties Oversight Board (2014).

contained in EO 12333, including activities subject to FISA requirements.

Under EO 12333, U.S. intelligence authorities are permitted to engage in data gathering activities outside the U.S. through a variety of clandestine techniques and are subject to the constraints of FISA Section 702, which limits targeting a non-U.S. person located outside the U.S. to whom the U.S. Constitution and laws do not apply. Because EO 12333 is subject to the constraints of FISA Section 702, U.S. intelligence authorities are expressly prohibited from targeting "communication data of U.S. persons" ("**U.S. person data**") under EO 12333. There are a limited number of exceptions addressing incidental collection of U.S. person data, none of which are likely to implicate data transmitted to CBRE US.[5]

Such U.S. intelligence gathering activities do not require any involvement by U.S. companies and therefore do not require a warrant or demand for data disclosure as the U.S. intelligence authority would gather the data directly during the transmission by clandestine means such as tapping under-water cables outside of the U.S.

2. Court Oversight for FISA surveillance activities

The FISC conducts significant oversight and exercises supervisory authority over decision making around targeting individuals to acquire foreign intelligence information under FISA Section 702.

The U.S. Director of National Intelligence and Attorney General (either separately or jointly) are required to submit to the FISC for approval a certification describing the proposed surveillance. The certification must include a number of elements, including assurances that: (i) only non-U.S. persons located outside the U.S. are being targeted, (ii) a significant purpose of the acquisition is to obtain foreign intelligence information, and (iii) the information will be obtained from or with the assistance of an "electronic communication service provider" ("**ECSP**") according to FISA Section 702 in connection with FISA Section 1881(b)(4). Following approval of the certification, U.S. intelligence authorities can issue a directive for immediate compliance to any ECSP. An ECSP may file a petition with the FISC to set aside or modify a directive and the FISC may grant the petition if the directive does not meet the requirements of FISA Section 702 or is otherwise unlawful.

The FISC also maintains an active role in supervising and enforcing compliance relative to targeting procedures in the following respects: (i) requiring National Security Agency ("**NSA**") analysts, and other intelligence analysts to create a record of their targeting assessments and targeting rationale[6];

---

[5] EO 12333 requires that U.S. person data may be collected, retained, and disseminated "only in accordance with procedures approved by the Attorney General," in consultation with the Director of National Intelligence. U.S. person data can only be collected if it is permitted under Attorney General guidelines and if the information fits within one of the categories enumerated under EO 12333, to wit: (i) information collected during the course of a lawful foreign intelligence, counterintelligence, international counternarcotics, or international counterterrorism investigation; (ii) information necessary to preserve the safety of persons or organizations; (iii) information necessary to protect intelligence sources and methods; and (iv) information incidentally collected that indicates involvement in activities that violate federal law. See Attorney General's Approved U.S. Persons Procedures (March 2021) (https://www.intel.gov/assets/documents/guide/Chart_of_EO_12333_AG_approved_Guidelines_March_2021.pdf). In practice, however, it is unlikely that EEA Personal Data transmitted to CBRE US would fall into one of these exceptions.

[6] One example of the oversight conducted by the FISC is found in a recently declassified FISC opinion, where the Court directly addressed the NSA's legal obligation to provide justification and support for its assessment that the target is a non-U.S. person located outside the U.S. To that end, NSA analysts are subject to specialized, annual training and testing on the legal and policy guidelines that govern the handling and use of the data and additional training is required for access to FISA Section 702 data. *See* Mem. Op. and Order, FISC, at 9 (Dec. 6, 2019; released Sept. 4,

(ii) requiring U.S. Department of Justice ("**DOJ**") intelligence oversight attorneys to conduct review of targeting assessments as well as the "selectors" used in a given directive and report to FISC any noncompliance; (iii) imposing remedial action including modification of programs and termination of the government's authority to engage in data collection; and (iv) receiving semi-annual joint DOJ-ODNI[7] assessments of whether individuals, including foreign nationals, are properly targeted.

In addition, the FISC has an active role in overseeing compliance with scope requirements of active data collections under its purview, including imposing modifications to programs and termination of the U.S. intelligence authority to engage in data collection.

3. Additional Remedies in U.S. law not considered by the ECJ

FISA, the Electronic Communication Privacy Act (18 U.S.C. § 2712), and the Administrative Procedure Act (5 U.S.C. § 702) ("**APA**") provide statutory remedies to individuals, including non-U.S. persons. Each of these laws provide for private rights of civil action, damages and compensation of attorneys' fees to individuals of any nationality (including EU/EEA citizens) for purposes of seeking redress in U.S. courts for violations of FISA Section 702 and EO 12333. Additionally, the U.S. Judicial Redress Act of 2015 (5 U.S.C. § 552a) was enacted to extend to non-U.S. citizens certain rights of redress established for U.S. citizens. Furthermore, U.S. intelligence authorities are required to provide notice to any aggrieved individual, whether a target or other individual whose communications were improperly intercepted (U.S. and non-U.S. person) who may have been subject to any surveillance measures that have been taken if the data gathered by the U.S. intelligence authorities will be used against this individual in U.S. criminal proceedings and any other proceeding, including before any "department, officer, agency, regulatory body, or other authority of the United States". This notice enables the individual to challenge not only the use of the data as evidence but also the lawfulness of the initial collection through surveillance measures under FISA Section 702 and/or EO 12333.

Additional privacy protection results from the independent Privacy and Civil Liberties Oversight Board ("**PCLOB**") and Presidential Policy Directive 28 ("**PPD-28**") applicable to U.S. "signals intelligence activities", which covers FISA Section 702 and EO 12333. PPD-28 expressly protects privacy and civil liberties rights of U.S. and non-U.S. citizens. Even though PPD-28 is a presidential directive, it is legally binding on the Executive Branch, in particular the U.S. intelligence authorities, and remains in full force and effect. In extending the protections for U.S. persons to non-U.S. persons, PPD-28 has established a new international norm. A declassified report issued by the PCLOB describing the protection granted by PPD-28 is referenced below.[8]

Amendments to FISA in 2018 added querying procedures (in addition to targeting and minimization procedures), provisions improving oversight by the PCLOB, privacy and civil liberties officer requirements to additional relevant intelligence authorities, expanded whistle-blower protections to contractors, and transparency requirements including provisions for disclosing the number of FISA Section 702 targets.

II. Application of FISA and EO 12333 to CBRE US

1. Application of FISA and EO 12333 only to communication of U.S. persons

---

2020) (addressing Section 702 2019 certification) (https://www.intelligence.gov/assets/documents/702%20Documents/declassified/2019_702_Cert_FISC_Opinion_06Dec19_OCR.pdf).

[7] Office of the Director of National Intelligence ("**ODNI**").

[8] *See* https://fas.org/irp/offdocs/pclob-ppd28.pdf.

U.S. intelligence authorities may not, under FISA Section 702 or EO 12333, target communication data of U.S. persons (including U.S. companies) or non-U.S. persons believed to be in the U.S. Therefore, EEA Personal Data that is transferred to a U.S. company qualifies as "communication data of U.S. persons" and, thus, falls outside the scope of FISA Section 702 and EO 12333. This includes not only EEA Personal Data contained in email or other form of messages, but also EEA Personal Data that is transferred for processing and storage in IT systems / databases to a U.S. company.

"Communication data of U.S. persons" excluded from the scope of FISA Section 702 and EO 12333 includes not only data directly transmitted to CBRE US as recipient, but also data relating to communication between non-US persons / companies where such data is transmitted through CBRE US as an intermediary for hosting / processing purposes. In particular, this encompasses email communication between CBRE entities located in the EEA and CBRE US using the email communication facilities made available to such CBRE EEA entities by CBRE US.

There is considerable support for this position arising from a number of sources.

1.1. The text of FISA Section 702 provides that the U.S. government (1) may not intentionally target any person (regardless of nationality) known at the time of acquisition to be located in the U.S.; (2) may not intentionally target a person reasonably believed to be located outside the U.S. if the purpose of such acquisition is to target a particular, known person reasonably believed to be in the U.S.; and (3) may not intentionally target a U.S. person reasonably believed to be located outside the U.S.

Where EEA Personal Data subject to the GDPR is transferred to CBRE US (both in the case of direct communication and through company-internal IT systems or IT databases), such data represents communication data of a U.S. person, *i.e.*, communication of CBRE US. Both the NSA and FBI are legally obligated to assess and evaluate whether a target is a non-U.S. person located outside the U.S. and review decisions impacting U.S. persons involved in the targeting of facilities where the U.S. intelligence authorities knew or should have known that at least one user of the facility was a U.S. person.[9] If such review and assessment determines that at least one user of the communication facility is a U.S. person, the U.S. intelligence authorities are prohibited from carrying out the surveillance measures under FISA Section 702.

1.2 EO 12333 similarly reserves the highest level of protection for U.S. persons, and is the foundational authority by which NSA collects, retains, analyzes, and disseminates foreign signals intelligence information. The principal application of this authority is the collection of communications by foreign persons that occur wholly outside the U.S. Intelligence activities conducted under this authority are governed by minimization procedures established by the Secretary of Defense and approved by the Attorney General. Thus, if a U.S. intelligence authority is gathering data under EO 12333 qualified by the U.S. intelligence authority as U.S. person data, the U.S. intelligence authority is required under EO 12333 to segregate and purge such data and prohibited from further reviewing and analyzing such U.S. person data.

[9] *See* SEMIANNUAL ASSESSMENT OF COMPLIANCE WITH PROCEDURES AND GUIDELINES ISSUED PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT, SUBMITTED BY THE ATTORNEY GENERAL AND THE DIRECTOR OF NATIONAL INTELLIGENCE, Office of the Director of National Intelligence (Dec. 2019) at 44.

2. Application of FISA only to electronic communication service providers

Having consulted various sources and legal experts, CBRE is of the view that CBRE US is not subject to data disclosure demands made under FISA Section 702 because CBRE US does not qualify as an "electronic communication service provider" under FISA Section 702.

2.1 According to FISA Section 702, the U.S. intelligence authorities can issue a data disclosure demand only to ECSPs, as defined in FISA Section 1881(b)(4). According to FISA Section 1881(b)(4) (B) and (C), the term ECSP means a "provider of electronic communication service", as that term is defined in the Electronic Communications Privacy Act of 1986 (18 U.S.C. § 2510 *et al*) ("**ECPA**") Section 2510 (18 U.S.C. § 2510), and a "provider of a remote computing service," as that term is defined in ECPA (18 U.S.C. § 2711).

2.1.1 ECPA Section 2510 defines "provider of electronic communication services" as a provider of any services which provides to users thereof the ability to send or receive wire or electronic communications, and further defines an "electronic communication" as "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photo-electronic or photo-optical system that affects interstate or foreign commerce."

2.1.2 ECPA Section 2711 defines "provider of a remote computing service" as a public provider of computer storage or processing services by means of an electronic communications system.[10]

2.2 The weight of authority among U.S. federal courts holds that companies that provide traditional products and services over the Internet are not "electronic communication service" providers within the meaning of the ECPA. *See In Re Jet Blue Airways Privacy Lit.* 379 F.Supp. 2d 299 (2d Cir. 2005); *Crowley v. Cybersource Corp.*, 166 F.Supp. 2d 1263 (N.D. Cal. 2001) (online merchant Amazon.com was not an ECSP despite the fact that it maintains a website and receives electronic communications containing personal information from its customers in connection with the purchase of goods); *Andersen Consulting LLP v. UOP*, 991 F.Supp. 1041, 1043 (N.D. Ill. 1998) (court finding distinction between companies that purchase Internet services and those that furnish such services as a business offering); *Sega Enterprises Ltd. v. MAPHIA,* 948 F. Supp. 923, 930-31 (N.D. Cal. 1996) (video game manufacturer that accessed private email of users of another company's bulletin board service was not a provider of electronic communication service); The prevailing weight of federal court opinions is consistent with the DOJ guidance for obtaining electronic evidence DOJ states that, while any company that provides others with the means to communicate electronically, regardless of their primary business or function, could conceivably be a provider of electronic communication service under the ECPA, "a mere user of [electronic communication services] provided by another is not a provider of ECS."[11] CBRE US is not a

[10] This definition would pertain to companies that offer computer storage to the general public for a fee and those companies that provide computer storage often for free. The statute's legislative history explains that such services exist to provide sophisticated and convenient data processing services to subscribers and customers from remote facilities. *See* S.Rep. No. 99-541 (1986), reprinted in 1986 U.S.C.C.A.N. 3555, 3564. As CBRE's service lines do not fall within this definition, it does not have any application to this analysis.

[11] *See* Office of Legal Educ., U.S. Dep't of Justice, Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations 117 (2009) available at https://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/01/14/ssmanual2009.pdf ("DOJ Manual"), at p. 117.

provider of electronic communication services within the meaning of FISA Section 702 and ECPA Section 2510 because (i) it is a "mere user" of electronic communication services (e.g., email system, instant messaging system, internal internet access) provided by a third party commercial communication / internet access provider, and (ii) it does not offer to the public user-to-user communications via electronic communication services, such as apps or website services.

2.2.1 Furthermore, the DOJ has acknowledged that, from a practical perspective, regardless of whether they are ECSPs, "[m]ost companies doing business in the EU do not, and have no grounds to believe they do, deal in any data that is of any interest to U.S. intelligence agencies" under FISA Section 702.[12]

2.2.2 The scope of ECS "provider" under FISA Section 702 is widely understood to apply to companies that are in the business of providing communication services to others, rather than merely for their own corporate use. FISA Section 702 authorizes data collection from communication services that are "provid[ed] to the target of the acquisition"[13] - in other words, communications services provided by a company in the business of providing communication services, as noted in the PCLOB's Section 702 Report ("FISA defines electronic communication service providers to include a variety of telephone, Internet service, and other communications providers.").

The NSA has publicly stated that: "[t]he 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 civil liberties and privacy of Americans."[14]

2.2.3 In its opinion approving the U.S. Government's 2019 certification to use FISA Section 702, the FISC noted that the U.S. Government is authorized to acquire information from "Internet backbone carrier[s]," "from systems operated by providers of services," and "[t]raditional telephone communications." Nowhere in

---

[12] The DOJ (along with the Director of National Intelligence and U.S. Commerce Department) observed the following in their written response to Schrems II in September 2020, at p.2: "As a practical matter, for many companies, the issues of national security data access that appear to have concerned the ECJ in Schrems II are unlikely to arise because the data they handle is of no interest to the U.S. intelligence community… [FISA] Section 702 [is] a statute establishing a judicial process authorizing a specific type of data acquisition. Most companies doing business in the EU do not, and have no grounds to believe they do, deal in any data that is of any interest to U.S. intelligence agencies. U.S. government commitments and public policies restrict intelligence collection to what is required for foreign intelligence purposes and expressly prohibit the collection of information for the purpose of obtaining a commercial advantage. Companies whose EU operations involve ordinary commercial products or services, and whose EU-U.S. transfers of personal data involve ordinary commercial information like employee, customer, or sales records, would have no basis to believe U.S. intelligence agencies would seek to collect that data. Indeed, the overwhelming majority of companies have never received orders to disclose data under FISA 702 and have never otherwise provided personal data to U.S. intelligence agencies."

[13] 50 U.S.C. Section 1881a(i)(A).

[14] *See* The National Security Agency: Missions, Authorities, Oversight and Partnerships, NSA Release No: PA-026-18 (Aug. 9, 2013), available at https://www.nsa.gov/Press-Room/Press-Releases-Statements/Press-Release-View/Article/1618729/the-national-security-agency-missions-authorities-oversight-and-partnerships/.

the opinion does the FISC reflect any support for U.S. intelligence authorities attempting to target corporate email accounts.[15]

3. Practical Application of FISA Section 702 to CBRE

In the U.S. Government's recent submission to the European Commission in response to the proposed amended EU Standard Contractual Clauses - SCCs (dated December 10, 2020), the following confirms that, even if an ECSP, there is a low likelihood that CBRE US will receive a data disclosure demand under FISA Section 702:

> *"[T]he vast majority of U.S. companies doing business in the EU do not, and have no grounds to believe, that they deal in any data that is of any interest to U.S. intelligence agencies. Given U.S. policy not to gather intelligence for purposes of assisting U.S. companies commercially, companies trading in ordinary products or services, and whose EU-U.S. transfers of personal data involve ordinary commercial information like employee, customer, or sales records, would have no basis to believe U.S. intelligence agencies would seek to collect that data. In particular, only a very small number of U.S. companies have ever received orders to disclose data under Section 702 of the Foreign Intelligence Surveillance Act, the form of compulsory process of concern to the Court of Justice in Schrems II. The Commission's direction that data exporters should take into account the specific circumstances of each data transfer shows an awareness and sensitivity to these kinds of facts. Highlighting this implication would alleviate unfounded anxiety in the business communities—both in the United States and in the European Union—over the impact of the Schrems II decision on their enterprises."*[16]

4. Hosting of EEA Personal Data by commercial cloud service providers in the U.S. (Onward Transfers)

CBRE US utilises to some extent commercial cloud service providers headquartered in the U.S. to host EEA Personal Data that has been transferred under the GDPR from EEA companies to CBRE US.

4.1 Such U.S. Hosting Providers typically qualify as a provider of a remote computing service, as defined in ECPA Section 2711 (18 U.S.C. § 2711), and thereby as an ECSP according to FISA Section 702 (50 U.S.C. § 1881(b)(4)(C)).

4.2 However, as elaborated above, the EEA Personal Data protected under the GDPR that is transferred to CBRE US either directly or indirectly (i.e., where CBRE US is an intermediary for IT hosting and support services) qualifies as "communication data of U.S. persons" and such "communication data of U.S. persons" falls outside the scope of FISA Section 702 and EO 12333.

---

[15] *See* Mem. Op. and Order, FISC, at 9 (Dec. 6, 2019; released Sept. 4, 2020) (addressing section 702 2019 certification). Notably, the plaintiff in *Schrems II* (Maximillian Schrems, Austrian data privacy advocate) appears to implicitly corroborate this interpretation of Section 702 by citing on his website the narrow set of communication service providers subject to Section 702: https://noyb.eu/en/next-steps-eu-companies-faqs (citing as examples AT&T, Amazon, Apple, Cloudflare, Dropbox, Facebook, Google, Microsoft, Verizon Media (former Oath & Yahoo), Verizon.

[16] *See* "Comments on Proposed SCC Decisions" at p. 9 (December 10, 2020). The Comments also note the following: "If a data importer has never received a data disclosure request from a government, recital 20 [in EU Proposed SCCs] indicates it should be able to rely on that fact to conclude that any actual risk of such access to the personal data it handles is negligible. This enables the data importer to focus pragmatically on the concrete impacts a transfer of personal data will have on individual privacy, as opposed to engaging in a speculative exercise about theoretical possibilities."

4.2.1 Hence, any data disclosure demand issued upon the U.S. Hosting Provider by U.S. intelligence authorities under FISA Section 702 would arguably be unlawful.

4.2.2 Consequently, the U.S. Hosting Provider has no legal obligation to comply with a data disclosure demand by a U.S. intelligence authority under FISA Section 702 and is contractually required or must have made legally consequential representations to object to or not comply with any such data disclosure demand in order to prevent the disclosure of EEA Personal Data.

III. Conclusion

CBRE has reached the conclusion, together with its external legal counsel and available sources with relevant expertise and experience under U.S. national security law, that U.S. intelligence authorities cannot lawfully target EEA Personal Data transferred to CBRE US under FISA Section 702 or EO 12333 because:

1. Transfers of EEA Personal Data to CBRE US are subject to additional safeguards and remedies for non-U.S. persons under the current U.S. legal system which were not considered by the ECJ in Schrems II but which provide protection for the rights and liberties of EEA persons when their EEA Personal Data is transferred from the EEA to CBRE US. As outlined above, the additional safeguards include multiple levels of oversight for FISA Section 702 data disclosure demands within the Executive, Judicial, and Legislative branches of the U.S. government, as well as multiple statutory remedies for aggrieved parties.

2. As of this writing, CBRE US has not received any National Security Letters or FISA court orders from U.S. intelligence authorities.

3. CBRE US is not an "electronic communication service provider" within the meaning and context of FISA Section 702, and therefore U.S. intelligence authorities cannot lawfully impose a data disclosure demand under FISA upon CBRE US.

4. EEA Personal Data transmitted to CBRE US may not be targeted pursuant to FISA Section 702 and EO 12333 by U.S. intelligence authorities as such data qualifies as "communication data of U.S. person".

5. CBRE US has engaged U.S. Hosting Providers who have committed to objecting to any data disclosure demands under FISA Section 702 as EEA Personal Data hosted by the U.S. Hosting Provider do not fall within the scope of FISA Section 702 and any such data disclosure demand is unlawful.[17]

Consequently, any supplementary measures for the transfer of EEA Personal Data to CBRE US (such as contractual, organizational and technical measures) as required by the ECJ in Schrems II and the EDPB pursuant to Art. 46 (1) and 45 GDPR are unwarranted. In any case, to provide additional comfort on the level of protection afforded to any EEA Personal Data that is transferred from the EEA to CBRE US, CBRE may implement any or all of the supplementary measures described below

[17] CBRE's assessment is buttressed by published opinions of other U.S. security law experts reaching the same conclusions.

- ✓ Commitment that CBRE US will issue a transparency report if it ever receives a data disclosure demand under FISA Section 702.
- ✓ Implementation of CBRE Inadequate Jurisdiction Order Disclosure Standard.[18]
- ✓ Implementation of the contractually binding Law Enforcement Data Access Procedure[19] according to which CBRE US will challenge all data disclosure demands received from U.S. intelligence authorities.
- ✓ Encryption of all EEA Personal Data in transit with Transport Layer Security ("**TLS**") protocol 1.2 or higher, SSH 2 (Secure Shell), IPSec (IP Security) or S/MIME (Secure Multipurpose Internet Mail Extension) and at rest with Advanced Encryption Standard ("**AES**") or Triple Data Encryption Standard ("**3DES**").
- ✓ Assessment of further technical measures to increase the protection of EEA Personal Data s such as server locations.
- ✓ Adoption of internal policy on strict and granular data access restrictions (strict need-to-know principle), monitored with regular audits and enforced through disciplinary measures.
- ✓ Adoption of internal policy procedure for data disclosure requests including internal allocation of responsibilities, required involvement of legal, compliance and internal auditing department and approval process and recording of demands and responses.

---

[18] CBRE's Global Policy 6.22 – Data Privacy includes Section V.L. "**Disclosure Pursuant to Government Orders and Access Requests from Inadequate Jurisdictions**" which provides that:

> "This section shall be referred to as the "**Inadequate Jurisdiction Order Disclosure Standard**." [Policy 6.22 defines "**Inadequate Jurisdiction**" to mean "*a jurisdiction that does not provide an essentially equivalent level of data protection as the jurisdiction from which the Personal Data originates*."]
>
> 2. *CBRE will not disclose Personal Data in response to an order, subpoena, warrant or other request for disclosure (each, an "**Order**") issued by any court, law enforcement agency, or national security agency pursuant to the laws of an Inadequate Jurisdiction, unless legally compelled to do so.*
>
> *3. Before disclosing Personal Data pursuant to an Order issued by an Inadequate Jurisdiction, CBRE will review the legality of the Order under the laws of the Inadequate Jurisdiction and, to the extent reasonable in the given circumstances, take all reasonable legal actions and remedies available to it under applicable law to challenge the Order where reasonable grounds exist to do so, seek interim measures to suspend the effects of the Order while the challenge is pending, and if legally compelled to comply with the Order, produce only the minimum data necessary for lawful compliance.*
>
> *4. CBRE will notify Data Subjects and the data exporter before disclosing their Personal Data pursuant to an Order issued by an Inadequate Jurisdiction unless legally prohibited from doing so, in which case CBRE will take all reasonable steps available to it under applicable law to seek a waiver of the prohibition and, in any event, will notify Data Subjects and the data exporter of the Order and disclosure at the earliest time it may lawfully do so. Where CBRE is acting as data importer and notification of Data Subjects is not reasonably possible, CBRE will seek the data exporter's assistance in notifying the Data Subjects.*
>
> *5. The applicable Appointed Data Protection Officer and the Global Director and Assistant General Counsel, Data Protection & Privacy ("**Privacy Director**") must be consulted upon receipt of an Order seeking disclosure of Personal Data for the purpose of determining whether such Order is lawfully issued pursuant to the laws of an Inadequate Jurisdiction and whether reasonable grounds exist to challenge the Order under applicable law. The consulted Appointed Data Protection Officer and Privacy Director will maintain, in a confidential file, a list of Orders issued by an Inadequate Jurisdiction, the steps were taken to challenge any such Orders, any legal prohibitions preventing notification of the Data Subjects, and the categories and volume of Personal Data disclosed in response to the Order.*
>
> *6. The Appointed Data Protection Officers or the Privacy Director will publish, with the maximum detail and frequency permitted by applicable law, a transparency report on Orders from Inadequate Jurisdictions on CBRE's public website."*

[19] CBRE's Law Enforcement Data Access Procedure (which mirrors the Inadequate Jurisdiction Order Disclosure Standard in Policy 6.22 – Data Privacy) is a supplemental contractual measure to the EU SCCs that CBRE US has committed to as a data importer in the context of its Intra Group Data Transfer Agreement.

- ✓ Adoption of strict data security and data privacy policies. CBRE's Information Security Management System is ISO/IEC 27001:2013 certified in all three regions for the direct and indirect provision of IT services.
- ✓ Adoption of internal procedure to regularly review this assessment and the supplementary measures.

Date	Version
November 30, 2021	1.0