

VMware Statement Regarding Application of FISA Section 702 and Executive Order 12333 in View of Schrems II

Following the decision of the European Union Court of Justice (ECJ) in Data Protection Commissioner v. Facebook Ireland and Maximilian Schrems, Case C-311/18 (Schrems II), VMware has prepared the following information regarding the likely application of certain U.S. authorities to VMware Service offerings.¹

U.S. Authorities

The ECJ expressed concerns about U.S. intelligence agencies having access to data transiting from the EU to the U.S. under two authorities: Executive Order (EO) 12333 and the Foreign Intelligence Surveillance Act (FISA) Section 702.

- EO 12333 establishes a general framework for conducting U.S. intelligence activities. It does not include any mechanism to compel private companies to disclose data or any legal means to require U.S. companies to disclose data transferred under SCCs “in bulk.”
- FISA Section 702 is a statutory framework that establishes a judicial process for the authorization of a specific type of data acquisition.
 - The program 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, such as international terrorism or international proliferation of weapons of mass destruction.²
 - The program consists entirely of targeting specific persons about whom an individualized determination has been made and thus Section 702 is not considered a ‘bulk’ collection program because it is based entirely on targeting the communications identifiers of specific people.³

¹ This document is intended to address U.S. authorities and excludes civil and criminal government investigations

² Report by the independent Privacy and Civil Liberties Oversight Board (PCLOB) on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act (2014) at 103,111, 113, available at: <https://documents.pcllob.gov/prod/Documents/OversightReport/823399ae-92ea-447a-ab60-0da28b555437/702-Report-2.pdf>

³ Report by the independent Privacy and Civil Liberties Oversight Board (PCLOB) on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act (2014) at 103,111, 113, available at: <https://documents.pcllob.gov/prod/Documents/OversightReport/823399ae-92ea-447a-ab60-0da28b555437/702-Report-2.pdf>

- The data to be acquired must conform with court-approved targeting procedures⁴ and the data requests would be for specific “selectors” (such as an email address or a telephone number of an individual). As part of this decision, the court must also determine whether the targeting procedures, along with the querying and minimization procedures, are consistent with the requirements of the Fourth Amendment of the U.S. Constitution.⁵
- Bulk data collection and collection of information for the purpose of obtaining a commercial advantage are expressly prohibited.

Section 702 is based on very broad definitions of “electronic communication service provider” and “remote computing services” which would include VMware and similarly operating U.S. companies.

VMware’s Position

VMware strongly believes there is a low likelihood that it would be subject to Section 702 or EO 12333 in relation to its provision of the Service offerings and processing of customer content for the following reasons:

1. VMware provides enterprise solutions that allow customers to build, manage, secure, and run applications across multiple systems and environments. Thus, to the extent any of our customers use the VMware services to transmit data that would be subject to Section 702, those customers would likely receive those orders directly.
2. VMware does not have access to the type of customer data that would be of any interest to U.S. intelligence agencies. As stated by the U.S. government in a September 2020 white paper, “[c]ompanies 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.”
3. EO 12333 contains no authority to compel private companies to disclose data and VMware will not provide any voluntary assistance to U.S. intelligence agencies to conduct EO 12333 activities.

For information regarding how VMware handles government access requests, see the [VMware Trust Center FAQs](#).

Last Revised: May 2021

⁴ See e.g., Memorandum Opinion and Order, Foreign Intelligence Surveillance Court, at 9 (Dec. 6, 2019; released Sept. 4, 2020) (granting approval of the certification and related procedures under Section 702), available at https://www.intelligence.gov/assets/documents/702%20Documents/declassified/2019_702_Cert_FISC_Opinion_06Dec19_OCR.pdf.

⁵ See § 702(j)(3)(A)-(B).