Opinion Regarding Enhanced Security Measures After the *Schrems II* Decision

Summary:

Data transfers to the United States do not require enhanced security measures because:

- FISA 702 has been amended to let any person subject to a FISA warrant sue the United States government,
- the Foreign Intelligence Surveillance Court shrank the scope of FISA searches, and
- judicial review of intelligence surveillance in the United States is equivalent to similar surveillance programs in the European Union.

Those changes negate the need for enhanced security measures when sending information to the United States.

This document serves as Ivanti's analysis about U.S. law and its ability to uphold privacy obligations from the European Union. It addresses concerns from the *Schrems II* court and the European Data Protection Board's Final Recommendations on measures that supplement transfer tools.

Ivanti will not answer questionnaires evaluating data transfers to the United States.

Analysis:

Upon reviewing recent changes to U.S. law, Ivanti does not believe transfers to the United States require additional security measures to address the ECJ's concerns about FISA 702. FISA does not apply to U.S. citizens and corporations generally. The U.S. government must have a warrant for such data under the 4th amendment to the U.S. Constitution. It may apply to entities out of the United States if those entities are engaged in terrorist activity, but Ivanti is not engaged in that type of activity. Ivanti is not aware of any situation where Ivanti has received a FISA warrant.

Furthermore, under GDPR Art. 6 (1)(d) and (e) and Art. 49 processing of Personal Data is lawful if it is done to "protect the vital interest of the data subject" or "necessary for the performance of a task carried out in the public interest . . . ." FISA 702 surveillance programs process Personal Data that is ultimately turned over to European authorities to prevent terrorism. Preventing terrorism protects the vital interests of data subjects in the European Union and is a task performed in the public interest.[1]

Focusing on specific concerns from the ECJ in *Schrems II*, that court was concerned about three things: redressability, privacy safeguards, and equivalence between U.S. and EU law.

Redressability

One of the ECJ's critical concerns related to an individual's ability to redress U.S. courts for alleged violations of the FISA 702 program. In 2018, Congress gave any "aggrieved person . . . who has been subjected to an electronic surveillance or about whom information obtained by electronic surveillance of

[1] *See* ODNI, "Guide to Section 702 Value Examples" at p. 4-5 explaining that the use of FISA 702 surveillance with the Turkish government helped capture a terrorist who bombed a nightclub and killed 39 people and injured 70 others. Guide-to-Section-702-Value-Examples.pdf (dni.gov)

such person has been disclosed or used in violation [of this statute] shall have a cause of action against any person who committed such violation." 50 U.S.C. 1810. https://www.law.cornell.edu/uscode/text/50/1810. There were concerns that EU citizens could not seek relief in U.S. courts, but this statute addressed those concerns.

The Electronic Communications Privacy Act provides an additional layer of redressability by letting "any person who is aggrieved by any willful violation of . . . the Foreign Intelligence Surveillance Act of 1978 may commence an action in United States District Court against the United States to recover money damages." 18 U.S.C. 2712. https://www.law.cornell.edu/uscode/text/18/2712

These recent changes to the U.S. law were not considered in the *Schrems II* decision but demonstrate an increased level of redressability for individuals outside of the United States who are subjects of electronic surveillance.

Privacy Safeguards

The *Schrems II* court did not evaluate FISA with relevant rulings and executive orders since decision 2016/1250. Since that decision, the U.S. government has expanded privacy protections under FISA 702.

In 2017, the Foreign Intelligence Surveillance Court ("FISC") issued an order terminating the legal authority to conduct "about" searches. Accordingly, FISA searches under 702 cannot gather information that may be about a targeted individual, but the communication must be "to" or "from" that targeted individual.

In 2018, the U.S. amended FISA to bolster privacy protections including the following:

1. The government must submit and the FISC must approve querying procedures, targeting procedures, and data minimization procedures before conducting a search of an individual;
2. Congress must be notified before the government before resuming "about" searches of foreign individuals;
3. Expanding the advisory and oversight functions of the Privacy and Civil Liberties Oversight Board over FISA 702 searches;
4. Requiring the FBI and the NSA to maintain Privacy and Civil Liberties Officers;
5. Extending whistleblower protections to contract employees (like Edward Snowden) so they can report privacy concerns without the fear of retaliation; and
6. Expanded disclosure requirements to the federal government.

Equivalence between U.S. and EU Law

Finally, the ECJ was concerned about whether privacy protections in FISA 702 meet the EU legal standards such that there is essential equivalence between the two regions. As a general matter the European Union does not have general authority over foreign intelligence. Such programs are left up to member states. Where there is a specific court (the FISC) that reviews all FISA 702 activity in the US, a little more than half of member states in the EU require judicial review of intelligence collection of foreign data. *See Surveillance by Intelligence Services – Volume I: Member States' Legal Frameworks*, European Union Agency for Fundamental Rights, p. 51-52 (noting "just over half [of member states] charge the judiciary (judges or prosecutors) with the approval process . . . .").

Furthermore, while the U.S. ended bulk data collection by terminating "about" searches, several member states allow bulk data collection for domestic intelligence collection programs. Of those member states,

in 2015 three of them allowed untargeted surveillance domestically while others did not regulate domestic surveillance of communications at all. *See Report on Surveillance by Intelligence Services, Volume II: field perspectives and legal update*, European union Agency for Fundamental Rights, p. 42-43.

Given the above, Ivanti does not need additional security measures in its SCCs or DPAs to address FISA 702.

--

Given the analysis above, enhanced security measures are not required when transferring information to the United States. Moreover, Ivanti believes the completion of an Art. 28 Data Processing Agreement and Standard Contractual Clauses satisfy concerns about equivalent security between the United States and the European Union.