US-EU Data Transfer Framework Signals Strengthened Collaboration

By **Alan Raul and Lauren Kitces** (October 14, 2022)

Alan Raul

Lauren Kitces

A series of coordinated announcements on Oct. 7 lifted the veil on a new trans-Atlantic data transfer mechanism.

This announcement has been hotly anticipated since a joint declaration from the U.S. and European Union governments on March 25, that there was an agreement in principle for a new EU-U.S. Data Privacy Framework.

The key document in the framework process is Executive Order No. 14086 on enhancing safeguards for U.S. signals intelligence activities,[1] accompanied by a detailed fact sheet on the executive order.[2]

The executive order rescinds the bulk of and moves far beyond former President Barack Obama's 2014 Presidential Policy Directive-28, or PPD-28.[3] Indeed, it provides a powerful and comprehensive new governance framework for electronic surveillance conducted in the name of U.S. national security.

PPD-28 had previously directed U.S. intelligence agencies to respect the privacy rights of all persons regardless of nationality, not just U.S. persons, and to establish detailed minimization procedures to achieve that end.

However, the Court of Justice of the European Union dismissed Obama's directive as a mere executive order, and not a law, and the CJEU did not so much as consider the intricate minimization procedures promulgated under PPD-28 with the intent to protect the privacy interests of non-U.S. persons.

The new executive order, however, provides significantly more independent review and remediation authority with respect to the conduct of signals intelligence by the U.S. intelligence community. This is genuinely a game-changer.

In the interest of putting the EU Commission in a good position to satisfy the CJEU this time, the new executive order establishes vastly more detailed substantive conditions and prescriptive procedural requirements than PPD-28.

EU persons who file qualifying complaints under the executive order will be entitled to a full investigation and an option to appeal to an independent body, the Data Protection Review Court. The determination of whether a complaint "qualifies" under the executive order will be made on the EU side, essentially taking the U.S. out of the "standing" equation.

The executive order also empowers the civil liberties protection officer at the Office of the Director of National Intelligence to conduct independent and unfettered investigations, and to provide assessments to the president that may differ from those of the director of national intelligence.

Most significantly, the interests of the complainant will be independently represented before the Data Protection Review Court by a special advocate.

And conformance with all of the executive order's standards and obligations will be reviewed by the independent Privacy and Civil Liberties Oversight Board, which will issue an annual public certification as to whether the redress mechanism protecting foreign persons is operating consistent with the executive order's specifications.

The collective weight of the executive order's stipulated limitations, and compliance and oversight protocols, is powerful, but Austrian privacy activist Max Schrems has already stated that the process is defective.[4] He believes the executive order continues to allow disproportionate bulk data collection — as he characterizes it — under Section 702 of the Foreign Intelligence Surveillance Act.

Below, we examine how the executive order should stack up against the CJEU's expectations.

At the outset, it should be noted that an executive order is legally binding on all of the agencies of the intelligence community. The president has authority over matters of national security and executive orders have the full force of law to govern the executive branch — consistent with applicable statutory law and the U.S. Constitution.

The executive order creates a web of requirements and protections that apply in addition to applicable laws and executive orders.

The executive order covers signals intelligence activities, and thus directly targets the CJEU's concerns about Section 702 of the Foreign Intelligence Surveillance Act — which relates to direct collection of data from electronic communications providers pursuant to compulsory legal process — and Executive Order No. 12333, which relates to indirect collection of communications through covert means.

In a fundamental departure from the general thrust of U.S. legal precedent, and building beyond PPD-28, the executive order extends legal protection to persons without distinction to country of origin, though the redress mechanism applies only to persons from qualifying states as will be discussed below.

It recognizes that U.S. persons — as defined in Executive Order No. 12333 — are protected by rights under the Constitution and specific laws, but the executive order requires that foreign personal information be protected in a manner that is substantially comparable to protections afforded to U.S. persons.

The transparency and independent oversight protocols mandated by the executive order are almost certainly among the most comprehensive and powerful controls on the intelligence activity of any country in the world.

Recognizing that foreign intelligence services collect information about U.S. persons, the executive order requires that qualifying states — whose persons are entitled to invoke the executive order's redress mechanism — must accord appropriate safeguards to protect the personal information collected through their own surveillance.

Presumably, EU member states believe they already accord such appropriate safeguards to personal information of U.S. persons, but we are not aware of any processes or reports more transparent and detailed than those stipulated by Biden's executive order.

Overcoming Past CJEU Decisions

Structurally, the executive order is divided into two main concepts:

- Protection-creating principles for all signals intelligence activities; and
- A redress mechanism for foreign individuals who allege their personal information was transferred to the U.S. and that U.S. signals intelligence activities "adversely affect[ed] the complainant's individual privacy and civil liberties interests" in violation of the executive order, the U.S. Constitution, the Foreign Intelligence Surveillance Act or Executive Order No. 12333.

Following Schrems II — the CJEU's 2020 ruling in Data Protection Commissioner v. Facebook Ireland and Maximillian Schrems — the European Data Protection Board set out four prongs of essential equivalency for transfers to third countries.[5] The executive order is clearly intended to fulfill these prongs.

In addition to other aspects of U.S. law that meet the conditions of essential equivalency, the language of the European Data Protection Board is deployed throughout the executive order. In other words, the executive order manifestly strives to directly address each of these board requirements.

Seeking to meet the requirement of proportionality,[6] a purported failing of the EU-U.S. Privacy Shield, the executive order presents a robust series of safeguard principles with a delineated process for the initial approval of collection activities. These work together to create a narrow scope of permissible use for signals intelligence activities.[7]

The likelihood that an argument of proportionality could prevail is further increased by additional requirements for signals intelligence activities, including data minimization; controls and limitations on the retention, sharing — i.e., dissemination within the government — and disclosure of personal information; and requirements for data security controls.[8]

Unsurprisingly, the continued permissibility of "bulk" collection of signals intelligence in the U.S. — even though such collection is also permitted in EU member states — has already drawn criticism, including from Schrems. But the fact is that bulk collection is significantly constrained under the executive order,[9] and targeted collection must be used where possible.[10]

If and when the executive order is subject to scrutiny by the CJEU, the court will need to address whether U.S. bulk collection under the executive order's limits and safeguards is essentially equivalent to bulk collection carried out by EU member states under current EU legal standards and CJEU jurisprudence.

Continuing to focus on transparency that will allow for a greater knowledge of whether the signals intelligence activities truly are necessary and in turn meeting the notion of proportionality, the Privacy and Civil Liberties Oversight Board is encouraged to provide oversight to the updated policies and procedures brought about by the executive order, and the head of each element of the intelligence community is required to implement the board's recommendations.

The Privacy and Civil Liberties Oversight Board is independent of the White House, so the president only encouraged this oversight given that it arguably extends somewhat beyond

the agency's specific statutory remit.

The board released an announcement Oct. 7 that it accepts this and other requests from the president to undertake an advice and oversight role in relation to the executive order.[11]

Following the policies and procedures regarding signals intelligence activities, a significant portion of the executive order is dedicated to the second concept: the creation of a specific two-step redress mechanism.

The redress mechanism responds to the CJEU's finding that the ombudsperson established for the Privacy Shield was not sufficiently independent, and the executive order prescribes an entirely different adjudication system to provide EU persons a means of effective redress.

The first layer in the redress process provides a mechanism by which foreign persons can file a complaint with the civil liberties protection officer[12] in the Office of the Director of National Intelligence.

The officer is charged with impartially investigating complaints to determine whether the executive order's safeguards or other relevant U.S. laws were violated, and it must do so in a matter that protects classified or otherwise privileged or protected information.

If the officer determines that there were violations of law or the requirements of the executive order, he or she will also identify and order the implementation of appropriate remediation.

The second level of the redress mechanism is the creation of an independent court created by the attorney general in the U.S. Department of Justice called the Data Protection Review Court.

The role of the court is to review appeals of civil liberties protection officer determinations upon request of an individual complainant or an element of the intelligence community that disagrees with the civil liberties protection officer's findings or remediation.

The court will be comprised of individuals who are not currently part of the U.S. government, and who have experience in data privacy and national security. If an appeal is pursued, a special advocate will be selected by the Data Protection Review Court to advocate on behalf of the complainant's interest in the matter.

This is a highly consequential new feature of the executive order's redress process and, to our knowledge, the special advocate role may be a novel advocacy requirement in the realm of privacy protection — and certainly with respect to non-U.S. persons.

While the Data Protection Review Court is not an Article III court, the executive order undertakes significant steps to assure independence.

These include requiring the attorney general to consult the Privacy and Civil Liberties Oversight Board, among others, on appointing Data Protection Review Court judges, explicitly prohibiting the attorney general from removing judges on the court outside of several enumerated and logical circumstances — essentially when for cause — and prohibiting outside involvement in court decision making.

Even if the initial layer of the process were to be challenged, the construct of the court sits

comfortably within the recent CJEU jurisprudence that has accepted administrative tribunals playing a similar role in lieu of actual judicial courts.

Recognizing the need for further oversight, independent investigation and transparency, in addition to review intelligence community policies and procedures implementing the executive order, the oversight board is asked to:

- Conduct an annual review of the processing of qualifying complaints in the redress mechanism and to create a report of its findings;
- Publish an unclassified version of this report; and
- Publicly certify whether or not the redress mechanism is operating consistent with the executive order when processing complaints.

Specifically, the oversight board will evaluate and report on the intelligence community's implementation of the civil liberties protection officer or DPRC-ordered remediation.

These steps serve to address concerns that the signals collection activities and any purported oversight are concealed from the public and generally are not scrutinized.

An area of the redress process that may receive scrutiny is the information provided to the complainant on the outcome of its claim.

Complainants will not be informed that their personal information was part of signals intelligence activities if they pursue a claim with the civil liberties protection officer or the Data Protection Review Court through the redress mechanism.

Rather, they will be informed that "the review either did not identify any covered violations or the Civil Liberties Protection Officer of the Office of the Director of National Intelligence issued a determination requiring appropriate remediation."[13]

While this so-called Glomar response[14] might seem pointless, in reality, it is meaningful.

Through the independent investigation of and documentation prepared by the civil liberties protection officer and the Data Protection Review Court, a complainant can be assured that his or her complaint is either unfounded or has been effectively fixed, i.e., remediated.

Further, we understand that this same basic response approach is also currently used by EU intelligence agencies.

The fact that decisions of the civil liberties protection officer and the review court will be fully binding on U.S. intelligence agencies is crucial to the functionality of the redress process and the knowledge of the complainant that any statements on remediation are meaningful.

Functionally, all this should serve to overcome the issues raised by the CJEU.

Qualifying States and Reciprocity

The executive order transforms the U.S. treatment of the personal information of foreign

persons, but it also uses a short set of requirements to reshape the foreign treatment of U.S. persons. States must be designated by the attorney general as eligible for their citizens to invoke the redress mechanism.[15]

In order to receive such a designation, the other country or regional economic organization must provide

> appropriate safeguards in the conduct of signals intelligence activities for United States persons' personal information that is transferred from the United States to the territory of the country or a member country of the regional economic integration organization.[16]

This requirement, which is similar to what is included in the Judicial Redress Act,[17] turns the table on the EU and its member states to require that they have protections and redress for U.S. persons.

While it does not outright require proof of the existence of these protections, the executive order does permit the attorney general to revoke the status of qualifying states,[18] raising the question of whether it may ask for similarly public commitments.

Moreover, in order to achieve the status of a qualifying state, the country or economic organization must permit or intend to permit the transfer of personal information for commercial purposes between that jurisdiction and the U.S.[19]

These requirements show that while the U.S. is willing to adjust to EU concerns, it will expect reciprocal commitments to protect U.S. interests and the personal information of U.S. persons.

Beyond Signals Intelligence Activities

But what about commercial transfers?

Shortly after the executive order was released, the U.S. Department of Commerce — which regulates the Privacy Shield along with the U.S. Department of Transportation — announced that part of the framework will be updates to the Privacy Shield principles, thereby restoring "an accessible and affordable data transfer mechanism for participating U.S. companies."[20]

Further, the Department of Commerce committed to working with those entities that remained enrolled in the Privacy Shield — which the U.S. government has continued to treat as in force despite the EU overturning its validity for data transfer purposes in Schrems II — to "facilitate the transition to the updated privacy principles under the [framework]."

While the focal point of the executive order is signals intelligence activity, the combination of the statement on anticipated updates to the Privacy Shield, along with the requirement to allow commercial personal information transfers in order to be a qualifying state, demonstrates that commercial transfers have remained front-of-mind for the U.S. and EU.

In addition to U.S. announcements, the EU Commission — that has been working head-to-head with the U.S. on structuring and drafting the new framework — updated their Q&A post on the framework at the same time as the executive order was announced.[21]

This coordination demonstrates the European Commission's confidence that the parties have

found valid solutions for EU-U.S. data transfers.

A Lasting Solution

Will the executive order succeed in its mission?

While arguments challenging aspects of the U.S. commitments and approach to building the framework have already begun, the combination of materials and intentions presented Oct. 7 strongly advances the argument that the U.S. is able to meet the essential equivalency standards presented by the CJEU and the European Data Protection Board, and directly addresses the concerns expressed in Schrems II.

This process represents strong collaboration between the U.S. and EU, jointly driving toward a solution to sustain the over $1 trillion of trade between them.

Alan Raul is a partner and leader of the privacy and cybersecurity practice at Sidley Austin LLP.

Lauren Kitces is a senior managing associate at the firm.

[1] https://www.whitehouse.gov/briefing-room/presidential-actions/2022/10/07/executive-order-on-enhancing-safeguards-for-united-states-signals-intelligence-activities/.

[2] https://www.whitehouse.gov/briefing-room/statements-releases/2022/10/07/fact-sheet-president-biden-signs-executive-order-to-implement-the-european-union-u-s-data-privacy-framework/.

[3] https://www.whitehouse.gov/briefing-room/statements-releases/2022/10/07/national-security-memorandum-on-partial-revocation-of-presidential-policy-directive-28/.

[4] https://noyb.eu/en/new-us-executive-order-unlikely-satisfy-eu-law.

[5] EDPB Recommendations 02/2020 on the European Essential Guarantees for surveillance measures, November 10, 2020. The four prongs of essential equivalency are: (1) clear and precise rules governing the scope and application of the measure in question and the imposition of minimum safeguards; (2) demonstration that the interference with data protection rights is necessary and proportionate with respect to the legitimate objective pursued; (3) provision of an independent oversight mechanism; and (4) effective remedies for the individual.

[6] Article 5(4) of the Treaty on European Union defines the principle of proportionality to be "the content and form of Union action shall not exceed what is necessary to achieve the objectives of the Treaties.".

[7] See, e.g., EO Sec. 2(b)(i); EO Sec. 2(a)(ii)(A); EO Sec. 2(b)(iii); EO Sec. 2(b)(ii).

[8] EO Sec. 2(c)(iii).

[9] Id.

[10] EO Sec. 2(c)(ii)(A).

[11] https://documents.pclob.gov/prod/Documents/EventsAndPress/4db0a50d-cc62-4197-af2e-2687b14ed9b9/Trans-Atlantic%20Data%20Privacy%20Framework%20EO%20press%20release%20(FINAL).pdf.

[12] https://www.dni.gov/index.php/who-we-are/organizations/ic-cio/ic-cio-related-menus/ic-cio-related-links/ic-cio-contact-us?id=373#:~:text=The%20Act%20provides%20that%20the,procedures%20of%20intelligence%20agencies%3B%20overseeing.

[13] EO Sec. 3(c)(i)(E)(1) and EO Sec. 3(d)(i)(H).

[14] See, Phillippi v. CIA, 546 F.2d 1009 (D.C. Cir. 1976).

[15] EO Sec. 3(f).

[16] EO Sec. 3(f)(i)(A).

[17] See, Judicial Redress Act of 2015, 5 U.S.C. § 552a.

[18] EO Sec. 3(f)(ii).

[19] EO Sec. 3(f)(i)(B).

[20] https://www.commerce.gov/news/press-releases/2022/10/statement-us-secretary-commerce-gina-raimondo-enhancing-safeguards.

[21] https://ec.europa.eu/commission/presscorner/detail/en/qanda_22_6045.