Morgan Lewis

EU-US DATA PRIVACY FRAMEWORK

RA Dr. Axel Spies, November 2, 2022

Morgan Lewis

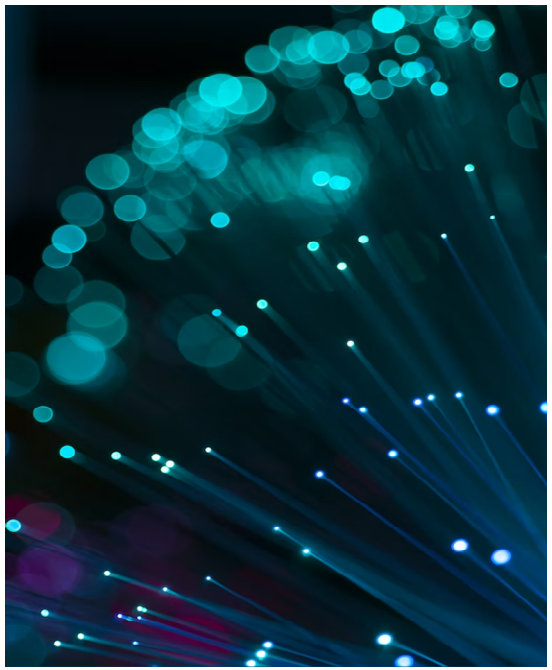
OVERVIEW

- How did we get here?
- Executive Order – what's in it?
- Arguments – pros and cons.
- Looking ahead.

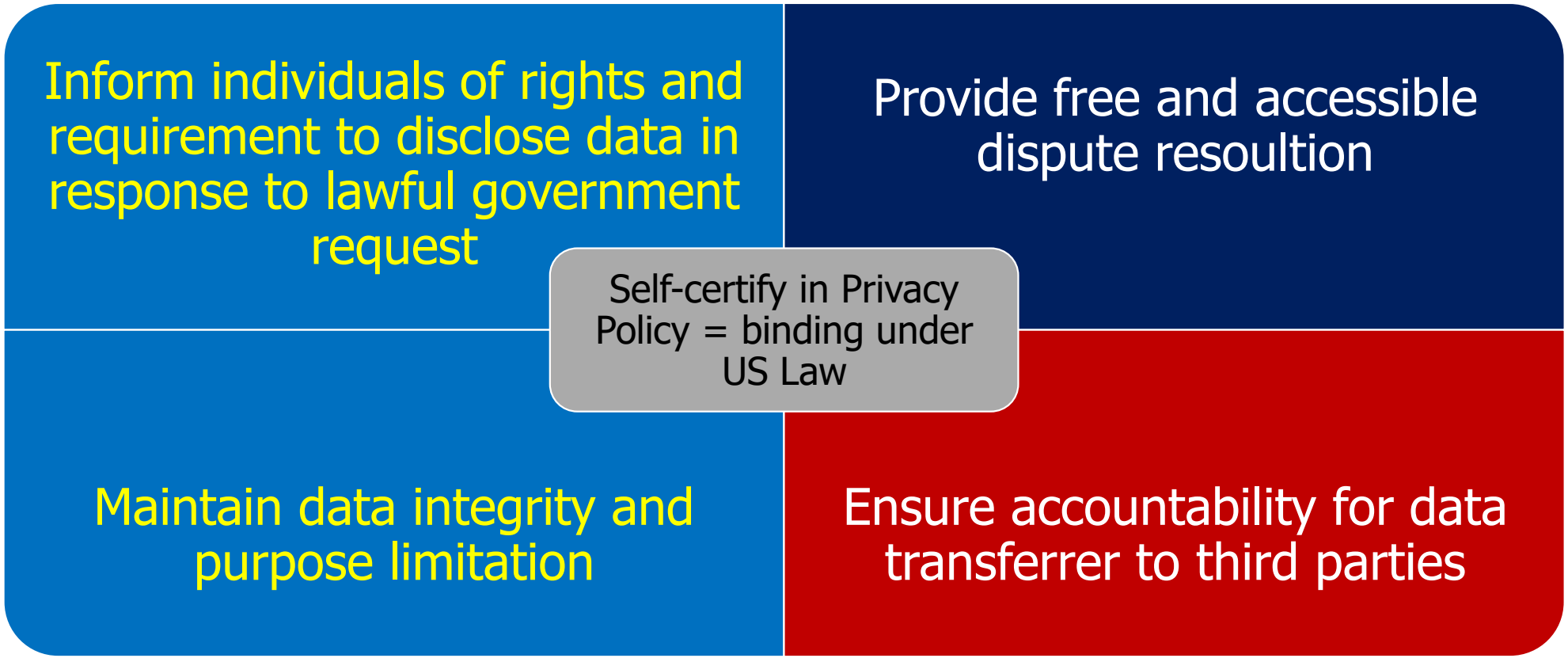
PART 1: How did this EO come about?

Privacy Shield Framework

- Predecessor was the EU/US Safe Harbor. Adequacy decision in 2000. After a legal case between Austrian privacy campaigner Max Schrems, the Court of Justice of the EU (CJEU) decided in Oct. 2015 it was invalid, and replaced it in Feb. 2016
- Transatlantic personal data flows were then covered by the EU-US and Swiss-US Privacy Shield Frameworks
- This provided companies with a way to comply with EU/Swiss data protection rules when transferring personal data



Previous EU-US Privacy Shield Requirements



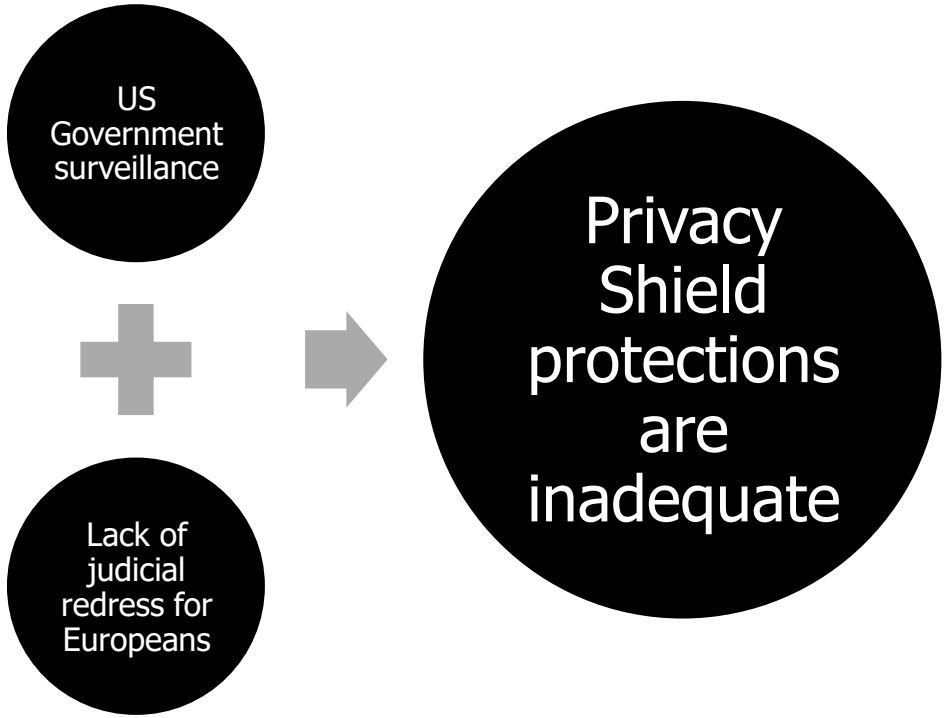
How Companies Joined the Privacy Shield

1. Confirm that the organization is an eligible US legal entity under the jurisdiction of the FTC or DoT
2. Develop a Privacy Shield-compliant privacy policy statement, reflecting notice of information handling practices compliant with the framework
3. Identify your organization's independent recourse mechanism
4. Pay the required fee to the International Centre for Dispute Resolution-American Arbitration Association for administration of a binding arbitration mechanism
5. Ensure your organization's verification mechanism is in place, using either a self-assessment or third-party assessment program
6. Designate a contact within your organization regarding Privacy Shield
7. Review the information required to self-certify and compile it for the Commerce Department
8. Submit your self-certification to the Commerce Department → **publicly accessible list**

Invalidation of the Privacy Shield

The Court of Justice of the European Union (CJEU) – decision on 07/16/2020

Data Protection Commission v. Facebook Ireland, Schrems ("Schrems II")



A Few Memorable Quotes from Schrems II

- "Article 45(2)(a) of the GDPR states that," in assessing adequacy of data protection, the Commission must particularly look for **"'effective and enforceable data subject rights' for data subjects whose personal data are transferred**."
- SIGINT activities "are not covered by requirements ensuring, subject to the principle of **proportionality**, a level of protection essentially equivalent to that guaranteed by the second sentence of Article 52(1) [requiring an independent supervisory authority]."
- FISA Section 702 **does not place limits on surveillance of non-US persons** and thus is **not proportional**, which requires "defin[ing] the scope of the limitation on the exercise of the right concerned and lay down clear and precise rules governing the scope and application of the measure in question and imposing minimum safeguards."

Post-Privacy Shield

Transatlantic personal data transfer difficulties

Lengthy Standard Contractual Clauses - 2021 version with deadline 12/27/2022

Binding Corporate Rules, adopted only by a few large corporations or "derogations"

Arduous data transfer impact assessments

PART 2: A New EU Agreement in the Making

March 2022 European Commission President von der Leyen and President Biden announce a new framework

Negotiations between the European Commission and US Government

October 2022 EO released

Executive Order (EO) on Enhancing Safeguards For Signals Intelligence Activities

- On October 7, 2022, President Biden released an EO establishing safeguards for handling personal information during signals intelligence (SIGINT) activities
- Signals intelligence is not defined in the EO, but includes intelligence collected from signals intercepted from foreign electronic information and communications systems

What is SIGINT?

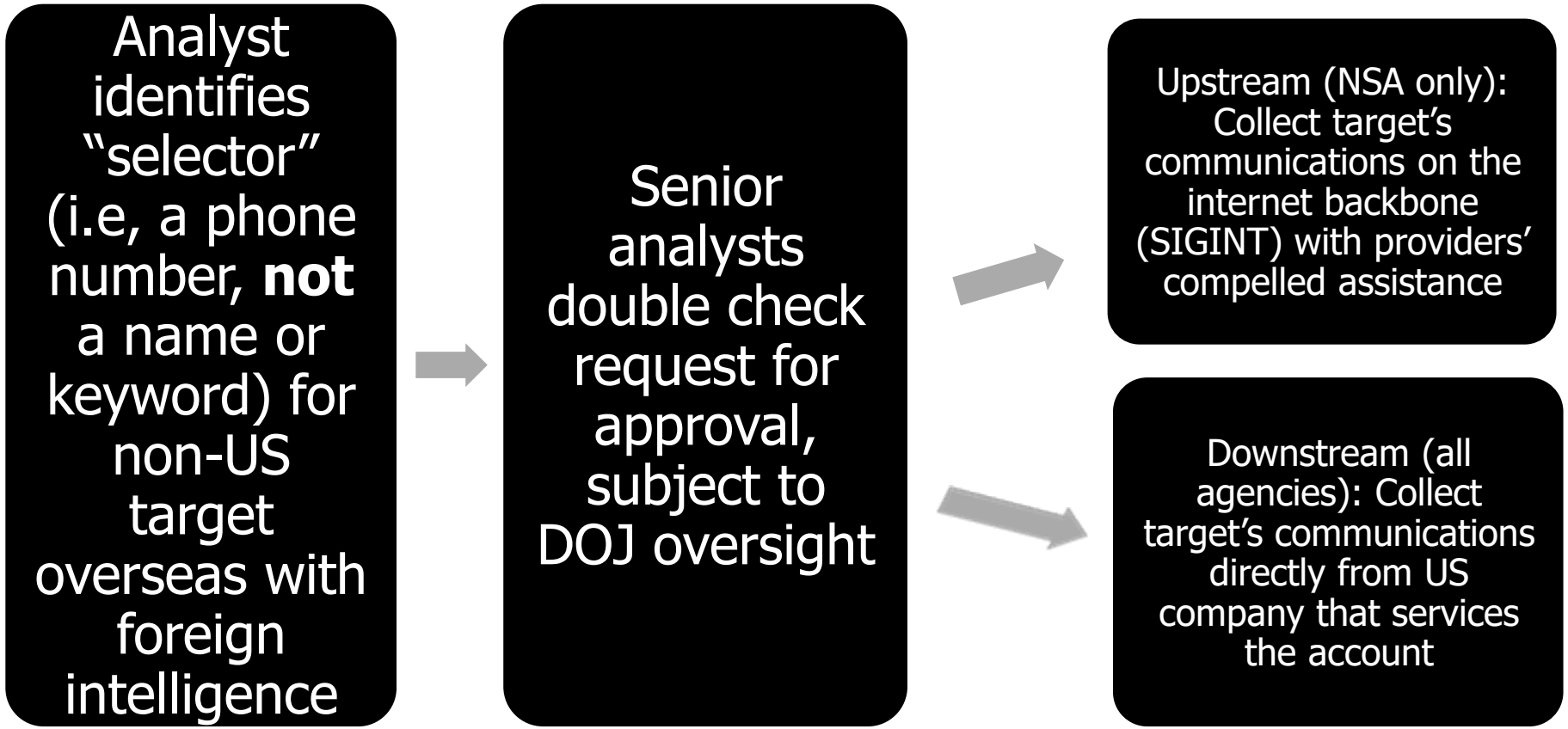
- SIGINT, originating from earlier communications intelligence (COMINT), and cryptology played a vital role in World War II and have since become crucial to foreign intelligence.
- SIGINT is not defined in the EO or the National Security Act of 1947, as amended
- While SIGINT was originally conducted by the Army and Navy, decentralization hindered collection, and in 1952 the NSA was created as a "unified organization" to control SIGINT
- The Department of Defense dictionary definition of SIGINT is:

1. A category of intelligence comprising either individually or in combination all communications intelligence, electronic intelligence, and foreign instrumentation signals intelligence, however transmitted.
2. Intelligence derived from communications, electronic, and foreign instrumentation signals.

→ **Not only the NSA is covered.**

How the Intelligence Community Collects Under Foreign Intelligence Surveillance Act Section 702?

- The US Intelligence Community is composed of 18 agencies (e.g., NSA, FBI, and CIA), each with defined missions, Attorney General-approved collection guidelines, and minimization procedures.



How is SIGINT collected?

Under EO 12333, governing Intelligence Activities, SIGINT:

- Is the main responsibility of the NSA
- Which supports other agencies and departments
- And may not be conducted by another agency without Defense Secretary delegation, after coordination with the NSA Director

What Would the EO Do?

Requires SIGINT be

- Necessary and
- Proportionate
- To the "advancement of validated intelligence priority"

Redress Mechanism

- EU individuals can file complaints with the Civil Liberty Protection Officer within ODNI
- Then appeal any decision to the new "Data Protection Review Court" (DPRC)
- But only if the AG designates a country as qualifying for the redress

What is Necessary and Proportionate to a Validated Intelligence Priority?

Necessity and Proportionality

- Necessity and Proportionality are found in the Charter of Fundamental Rights of the European Union and the draft California data protection regulations.
- Proportionality in EO: Achieve proper balance between the intelligence priority and "the impact on the privacy and civil liberties of all persons."

Validated Intelligence Priority

- Targeted collection must fall within one of twelve categories, like assessing terrorist organizations or global health concerns.
- Bulk collection limited to six separate categories.
- Prohibited purposes include suppressing free speech, discriminating against people based on membership in certain protected classes, or collecting trade secrets unrelated to national security.

California Consumer Privacy Act Regulations (2022)

- "A business's collection, use, retention, and/or sharing of a consumer's personal information shall be reasonably **necessary and proportionate** to achieve the purpose(s) for which the personal information was collected or processed."
- "To be reasonably necessary and proportionate, the business's collection, use, retention, and/or sharing **must be consistent with what an average consumer would expect** when the personal information was collected."

PART 3 Arguments for the EO

- Provides a much-needed **legal step towards a solution** to enable lawful transfers from the EU to the US.
- Expressly incorporates principles of **necessity and proportionality**, consistent with CJEU ruling and EU Charter of Fundamental Rights. Signals intelligence data collection may occur only for certain listed objectives (e.g., prevention of terrorism), and cannot occur for other prohibited objectives (e.g., suppressing freedom of expression).
- Expressly incorporates a **redress mechanism** for data subjects who believe their data privacy rights have been violated. Data subjects can complain to a Civil Liberties Protection Officer (in the Office of the Director of National Intelligence) and, if necessary, subsequently appeal to a new Data Protection Review Court.
- The Data Protection Review Court is **independent**. Judges must be data protection experts (prior judicial experience preferred) and cannot hold any other roles within the US Government. A special advocate will be appointed to represent the complainant's interests.

Arguments Against the EO (Overview)

Example: German Data Protection Commissioner of Baden-Württemberg, Stefan Brink:

He does not believe that the decree recently presented by U.S. President Joe Biden will stand up to the strict requirements of Schrems II.

- *"Even under the new rules, mass surveillance would still be possible"*
- *"The CJEU had demanded not only legal remedies against government spying, but a complete end to warrantless surveillance. . . However, there can be no talk of this at present . . ."The system change demanded by the CJEU is not taking place."*
- *"The EO is only an internal instruction to the government and subordinate authorities and could be amended or withdrawn at any time by the next president. . . Without a law passed by Congress, there will be no necessary legal certainty for all the parties involved."*

Arguments Against the EO: Necessity and Proportionality

Executive Order only pays lip-service to the concepts of necessity and proportionality. It still enables ongoing bulk collection of signals intelligence.

- But each IC element has its own limitations on what it can collect under EO 12333 and AG-approved guidelines, as well as minimization procedures;
- PPD 28 limits bulk collection, and now has an independent redress mechanism.
- California Consumer Privacy Act Regulations (2022) may help further clarify these concepts under US law.

Comparison: German Constitutional Court 2020 (BVerfG)

BVerfG: Foreign telecommunications reconnaissance under the Federal Intelligence Service Act (BND Act) unconstitutional

Decision of 05/1919.05.2020 - 1 BvR 2835/17

- German government's obligation to respect fundamental rights under the Basic Law is NOT limited to German territory, at least with regard to telecommunications secrecy and freedom of the press.
- Any targeted intrusion into particularly sensitive and confidential communication spaces, such as those of journalists, is only possible if a "qualified threshold" exists for the intrustion.
- If a "special sensitivity" of the data is only noticed while evaluating such data, an additional assessment of the government agency (BND) is required as to whether the relevant communication may be evaluated and used.
- The monitoring powers also require independent and continuous objective legal control, which the BND Act does not provide for.

Comparison: Intelligence Review in Germany (Overview)

§ 9 Information to the person concerned

Upon request, the Federal Intelligence Service shall provide the data subject with information about data stored about him or her pursuant to Sec. 6 in accordance with Sec. 15 of the Act on the Federal Protection of the Constitution.

§ 40 Exercise of Independent Legal Control

1. The lawfulness of technical reconnaissance and associated transmissions and cooperation by the Federal Intelligence Service on the basis of the powers granted by this Act shall be subject to legal control by the Independent Control Council.
2. Legal control shall be exercised as.
   a. Quasi-judicial legal control by the Independent Control Council; and
   b. Administrative legal control by the administrative control organ.

§ 41 Independent Control Council

1. The Independent Control Council is a supreme federal authority and, as an independent organ of control of the technical reconnaissance of the Federal Intelligence Service, shall be subject only to the law.

→ **Prior control of the legality = not a judicial body.**

Arguments Against the EO: Judicial Redress/ "Court"

The CJEU and GDPR expect data subjects to have judicial redress. However, the Protection Review Court is not a true judicial court - instead, it is a body within the Executive Branch of the US Government, and therefore insufficiently independent.

- But the EO says the DPRC "shall be guided by relevant decisions" of the Supreme Court like Article III courts.
- It has been recognized since before *Marbury v. Madison* that "it is a general and indisputable rule, that where there is a legal right, there is also a legal remedy." (Quoting Blackstone on the common law).
- Whether the DPRC is a court or administrative body is immaterial, as long as data subjects have "effective and enforceable rights" from an "independent and impartial" body that can issue binding decisions, as required in Schrems II.
- So, if the DPRC is an independent, binding authority, guided by Supreme Court precedent, as stated by the EO, it should suffice as a redress system under US law.

Arguments Against the EO: Judicial Redress/ "Court" (2)

Schrems II paragraph 194: "data subjects must have the possibility of bringing legal action before an independent and impartial court."

- But Paragraph 197 refers to the power to "provide any cause of action before a body which offers the persons whose data is transferred to the United States guarantees essentially equivalent to those required by Article 47 [EU Charter of Fundamental Rights]" (which the Privacy Shield Ombudsman did not have).
- Wording of Article 47: "independent and impartial tribunal previously established by law…"
- And administrative remedies may be better than judicial redress because procedures are less strict, less costly, faster, and offer greater expertise
- Independent experts review the matter.

Arguments Against the EO: Judicial Redress/ "Court" (3)

Regardless, the DPRC may afford more protection to non-US persons than they would receive in their own country regarding surveillance.

- For example, France's Conseil d'état (last April) validated mass telecommunications surveillance and the general retention of metadata, in contradiction to fundamental rights principles articulated by the CJEU.
- A 2017 EU Fundamental Rights Agency on surveillance by intelligence agencies report notes only 18 of 27 EU Member States have remedial bodies that can issue binding decisions.
- E.g., in Denmark, Estonia, Malta, and Spain, bodies with remedial powers over surveillance were found to have no binding decision-making power and decisions could not be reviewed.

Unanswered Question in EO: Judicial Redress/ "Court"

Can DPRC decisions be challenged in federal courts under the Administrative Procedures Act?

- The AG's regulation establishing the DPRC says it "is not intended to, and does not, modify the availability or scope of any judicial review of the decisions rendered through the redress mechanism, which is governed by existing law."
- Congress could establish a separate Article III court or amend the Foreign Intelligence Review Court's jurisdiction to allow review outside the Executive Branch.

Arguments Against the EO: Status of Data Subject

Following a complaint, data subjects are given no substantive information about any findings - and no confirmation whether they were subject to surveillance. This means the data subject has little to no ability to appeal any finding.

- But either the complainant or an IC element can apply for review.
- A special advocate will be selected to advocate in the complainant's interest.
- Risk that proceeding may be abused.

Arguments Against the EO: Not a "Statute"

The longevity of the data privacy framework protections is uncertain. Because protections are in an Executive Order, rather than legislation, they could easily be overturned by a future President.

- But EOs, like EO 12333 from the Reagan administration, can last multiple presidencies.
- Congress could still validate the EO through legislation at any time.
- The European Commission would also likely reserve the right to suspend the adequacy decision if the EO was revoked.

Arguments Against the EO: Bulk collection

Presidential Policy Directive 28 (PPD 28) may not cover all bulk collection.

- Footnote 3 PPD 28: "Unless otherwise specified, this directive shall apply to signals intelligence activities conducted in order to collect communications or information about communications, except that it shall not apply to signals intelligence activities undertaken to test or develop signals intelligence capabilities."
  - But these applications are likely limited, especially absent a validated intelligence objective.
  - CJEU: various decisions on mandatory data retention for telecoms services.

PART 4: Next: What About the UK and Switzerland?

- The EO is designed to provide protections regardless of national origin.
- The redress mechanism is only available to **qualifying states, as determined by the US AG**, if:
  - Mutual protections exist for the protection of US persons regarding SIGINT and
  - The country will permit transfers of personal data to the US
- US CLOUD Act and US-UK government statement
- The UK and Switzerland must negotiate to become a qualifying state and appoint an authority to receive complaints for the new redress mechanism.

Qualifying States and Reciprocity

- The AG, in consultation with the Secretaries of State and Commerce, and the Director of National Intelligence may designate a country as a qualifying state for the redress mechanism if:
  - "(A) the laws of the country…require **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…;
  - (B) the country…permit, or are **anticipated to permit, the transfer of personal information for commercial purposes** between the territory of that country or those member countries and the territory of the United States; and
  - (C) such designation would **advance the national interests** of the United States."
- However, "appropriate safeguards" are not explicity defined by the EO.
- The designation, and revocation, can be effective immediately or on a date specified by the AG.

US Secretary of Commerce Raimondo's Statement

- The EU-U.S. DPF will:
  - "Update the privacy principles that companies adhere to under the EU-U.S. Privacy Shield Framework and rename them as the "EU-U.S. Data Privacy Framework Principles"."
  - "Restore an accessible and affordable data transfer mechanism for participating U.S. companies."
- The Commerce Department "will work with current Privacy Shield participants, 70% of which are small and medium enterprises, to facilitate the transition to the updated privacy principles under the EU-U.S. DPF."
- Secretary Raimondo will also submit letters and documents from relevant U.S. agencies outlining implementation to European Commissioner for Justice Reynders.

Roundtable of G7 Data Protection and Privacy Authorities (September 8, 2022)

- Paragraph 7: "With respect to transfer instruments, we recognize the importance of discussions about **several current approaches** in different regions of the world, which should be inclusive and not exclusive."
- "We therefore commit to continue working towards elements of convergence of these tools to foster future interoperability, where possible, in order to achieve a **high level of data protection** and **facilitate data free flow** with trust and create options for businesses to choose cross-border transfer tools, suitable for their business needs."
- "We […] call upon governments to continue efforts to implement effective data protection and privacy laws and to build upon existing frameworks and approaches, such as the **Convention 108+ of the Council of Europe**, the **OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data**, and the **OECD Recommendation on Cross-border Co-operation in the Enforcement of Laws Protecting Privacy**."

The Adoption Process at the EU

1. The EU Commission must draft an adequacy finding.
2. The European Data Protection Board must issue a non-binding opinion (and may request additional documents).
3. The EU Parliament may issue a formal opinion.
4. A committee composed of representatives of EU member states must approve the proposal by qualified majority.
5. The EU Commission must adopt its adequacy determination.

Possible Congressional Actions? CRS Report

- "If the CJEU determines that U.S. surveillance as authorized by Section 702 of FISA does not satisfy EU data protection law, even with the EO's safeguards in place, ensuring the legality of EU-U.S. data flows **may require amending FISA**. Section 702 of FISA is scheduled to expire at the end of 2023.
- Members of Congress have used past FISA reauthorizations to propose broader reforms to the law."
- Effect of Midterms?

A Case for Hope for Transatlantic Data Flows?

- Last paragraphs of the EO: "In the case of any conflict between this order and other applicable law, the more privacy-protective safeguards shall govern the conduct of signals intelligence activities, to the maximum extent allowed by law."
- New EU SCCs need to be in place by December 27, so there will be a legal gap from then until March 2023 when we expect the Adequacy Decision of the European Commission.
- What happens after the Adequacy Decision is unknown, however, Mr. Schrems and his organization NOYB will likely file another lawsuit.
- It remains to be seen how the redress system will work in practice and whether the CJEU would declare the protections inadequate.

Biography

Dr. Axel Spies
Rechtsanwalt, Special Legal Consultant
Washington, DC
T +1.202.373.6145
axel.spies@morganlewis.com

Dr. Axel Spies advises domestic and international clients on international legal issues, such as licensing, competition, corporate issues, and new technologies such as cloud computing in the European markets. He counsels on international data protection, international data transfers, privacy, technology licensing, e-discovery, and equity purchases. Dr. Spies is frequently quoted in the media for his telecommunications and privacy knowledge.

He is also a co-publisher of two German journals "ZD" (Journal for Data Protection) and "MMR" (Multimedia Law) and co-author on two handbooks on data privacy.