epic.org

Electronic Privacy Information Center
1519 New Hampshire Avenue NW
Washington, DC 20036, USA

+1 202 483 1140
+1 202 483 1248
@EPICPrivacy
https://epic.org

FEEDBACK OF THE ELECTRONIC PRIVACY INFORMATION CENTER

to the

EUROPEAN COMMISSION

Regarding the

FIRST PERIODIC REVIEW OF THE EU-U.S. DATA PRIVACY FRAMEWORK

September 2, 2024

The European Commission ("Commission") adopted an adequacy decision for the EU – U.S. Data Privacy Framework ("Framework") in July 2023.[1] That decision provides for a period of public review to take place within one year of the decision.[2] The Electronic Privacy Information Center ("EPIC") submits the following response for this review.

EPIC is a public interest research center based in Washington, D.C., established in 1994 to focus public and regulatory attention on emerging privacy and human rights issues and to protect privacy, freedom of expression, and democratic values in the information age.[3] EPIC has actively engaged with previous iterations of data transfer frameworks between the U.S. and the EU.[4]

---

[1] "EU-U.S. Data Privacy Framework," available at https://www.dataprivacyframework.gov/EU-US-Framework.
[2] "EU-US Data Privacy Framework: report of the Commission on how the framework is functioning," European Commission (Aug. 9, 2024), https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/14379-EU-US-Data-Privacy-Framework-report-of-the-Commission-on-how-the-framework-is-functioning_en.
[3] EPIC, *About EPIC* (2019), https://epic.org/epic/about.html (last visited Jun. 14, 2024).
[4] *See, e.g.,* Comments of EPIC, *Privacy Shield Third Annual Review,* European Commission (July 15, 2019), https://epic.org/epic-comments-on-third-annual-privacy-shield-review/; Chris Baumohl, *New Executive Order on Signals Intelligence: A Meaningful – but Insufficient – Step Forward,* EPIC (Dec. 6, 2022), https://epic.org/new-executive-order-on-signals-intelligence-a-meaningful-but-insufficient-step-forward/.

EPIC welcomes this opportunity to contribute to the evaluation of the Framework. While EPIC recognizes the genuine effort made in creating a structure with appropriate safeguards, the core problems identified when Privacy Shield was struck down remain consistent. The United States Intelligence Community's ability to engage in mass surveillance abroad has not been meaningfully changed, and, in certain circumstances, has objectively worsened. The recent reauthorization of the Foreign Intelligence Surveillance Act ("FISA") section 702 failed to codify any protections against surveillance abuses of non-U.S. personal data and in fact meaningfully expanded the Intelligence Community's ability to engage in data collection abroad.

The Biden Administration's Executive Order 14086 (hereinafter "Executive Order")[5] also fails to fully address the surveillance activities that have plagued previous EU-US data transfer agreements. The Executive Order expressly permits bulk data collection and fails to establish an independent and effective redress mechanism for EU residents. While the Executive Order purports to grant EU residents privacy protections equivalent to those enjoyed by United States residents, the United States lacks a federal privacy law and the existing sectoral laws and regulations do not rise to the level of GDPR protections. For these reasons, EPIC does not believe the Framework rises to the level of GDPR adequacy.

I. Reauthorization of FISA Section 702

On April 20, 2024, Congress—despite broad, bipartisan support for government surveillance reform—pushed through the Reforming Intelligence and Securing America Act ("RISAA"), H.R.7888, which reauthorized FISA Section 702 for two years.[6] As EPIC, Brennan Center, and

[5] Exec. Order No. 14,086 87 Fed. Reg. 62,283 (Oct. 7, 2022) https://www.federalregister.gov/documents/2022/10/14/2022-22531/enhancing-safeguards-for-united-states-signals-intelligence-activities.
[6] Reforming Intelligence and Securing America Act, Pub. L. No 118-49, 138 Stat. 862.

FreedomWorks found, RISAA was crafted to preserve the surveillance status quo, largely codifying current practice and procedures.[7] Worse, amendments passed in the House and included in the final bill significantly expand FISA Section 702, especially relevant for this adequacy process.[8]

First, RISAA expands the universe of businesses subject to surveillance under FISA Section 702 by amending the definition of "electronic communication service provider" to include service providers who merely have access to the equipment on which communications transit. According to the New York Times, this provision sought to cover data centers for cloud computing;[9] however, the provision itself is written in "enigmatic" language that encompasses far more than that. Senator Ron Wyden has said the provision "represents one of the most dramatic and terrifying expansions of government surveillance authority in history."[10] An individual designated by the FISA Court as permitted to draft amicus briefs for FISA Court cases has taken the rare step of publicly warning of the breadth of this provision as currently written.[11] Prior to final passage, the Information Technology Industry Council also called for the removal of this provision, citing the vast expansion of the government's warrantless surveillance capabilities, noting that it would "damag[e] the

---

[7] "RISAA: 56 'Reforms' that Preserve the Status Quo," EPIC, Brennan Center for Justice, FreedomWorks (April 2024), https://epic.org/wp-content/uploads/2024/04/RISAA-56-So-Called-Reforms-That-Preserve-the-Status-Quo.pdf; *EPIC Statement on Failed Rules Vote on RISAA,* EPIC (April 10, 2024), https://epic.org/epic-statement-on-failed-rules-vote-on-risaa/.

[8] Marc Zwillinger et al., *FISA 702 Reauthorization Amendments: The Second Time is Not the Charm,* ZwillGenBlog (April 9, 2024), https://www.zwillgen.com/law-enforcement/fisa-702-reauthorization-amendments-second-time-not-charm/.

[9] Charlie Savage, *Secret Rift Over Data Center Fueled Push to Expand Reach of Surveillance Program,* N.Y. Times (April 16, 2024), https://www.nytimes.com/2024/04/16/us/fisa-surveillance-bill-program.html.

[10] *"Wyden: 'I Will Do Everything In My Power' to Stop Bill Expanding Government Surveillance Under FISA 702,"* U.S. Sen. Ron Wyden (April 12, 2024), https://www.wyden.senate.gov/news/press-releases/wyden-i-will-do-everything-in-my-power-to-stop-bill-expanding-government-surveillance-under-fisa-702.

[11] Marc Zwillinger et al., *FISA 702 Reauthorization Amendments: The Second Time is Not the Charm,* ZwillGenBlog (April 9, 2024), https://www.zwillgen.com/law-enforcement/fisa-702-reauthorization-amendments-second-time-not-charm/.

competitiveness of U.S. technology companies large and small, and arguably imperil[] the continued global free flow of data between the U.S. and its allies."[12]

Second, RISAA codifies and expands suspicionless travel vetting using FISA Section 702.[13] In particular, RISAA requires that the Attorney General and Director of National Intelligence, for any procedures adopted by one or more of the agencies with access to FISA Section 702 information, "ensure that the procedures enable the vetting of all non-United States persons who are being processed for travel to the United States." In doing so, RISAA expands a more limited existing NSA travel vetting program using FISA Section 702 information and codifies suspicionless vetting of non-U.S. persons as a matter of law. This expansion has serious implications for EU residents seeking to travel to the U.S. for tourism, business, education, or to visit friends and loved ones.

Third, RISAA expands the definition of "foreign intelligence" to include information relating to drug trafficking, specifically information "that relates to [. . .] the ability of the United States to protect against [. . .] international production, distribution, or financing of illicit synthetic drugs, opioids, cocaine, or other drugs driving overdose deaths, or precursors of any aforementioned[.]" Although the U.S. government has already used FISA Section 702 to collect information on fentanyl trafficking, this expansion of foreign intelligence may further expand the scope of information collected under this authority.

Fourth, Section 6(g) of RISAA extends the authorized duration of surveillance conducted under Title I and Title III of FISA for non-U.S. persons from 120 days to one year. That means the government—rather than having to justify continued surveillance after an initial period of months—

---

[12] John Miller, *Expansion of FISA Electronic Communications Service Provider Definition Must Be Removed,* ITI TechWonk Blog (April 16, 2024), https://www.itic.org/news-events/techwonk-blog/expansion-of-fisa-electronic-communications-service-provider-definition-must-be-removed.

[13] Adriel Orozco, *Congress Expands Warrantless Surveillance of Immigrants Traveling to the US,* Immigration Impact (April 26, 2024), https://immigrationimpact.com/2024/04/26/congress-expands-surveillance-immigrants-traveling-to-us/.

has an entire year to carry out surveillance of non-U.S. persons before going back to the FISA Court to justify a continued need for doing so.

Finally, RISAA's expansion of the U.S. government's surveillance powers is coupled with a near complete lack of meaningful, new safeguards for non-U.S. persons. RISAA did not contain any codification of Executive Order 14086 and actually weakens part of the existing system of checks through the operation of FISA court *amici*—legal and technical experts who aid the court in evaluating surveillance conducted pursuant to FISA. RISAA both limits the pool of individuals eligible to serve as *amici* in certain cases and limits the arguments *amici* can make to only those identified by the FISA Court.

Further, Congress did not pass any reforms of surveillance conducted pursuant to Executive Order 12333, including but not limited to the U.S. government's purchase of sensitive data. While the House ultimately passed the Fourth Amendment Is Not For Sale Act—which would prohibit intelligence agencies and law enforcement from purchasing Americans' data without a warrant if passed into law—the Act has not yet been passed by the Senate and there remain few protections for non-U.S. persons in the existing EO framework.[14]

This current lack of protection is concerning given significant evidence that the U.S. government continues to buy data in bulk with insufficient safeguards in place and that vendors of this information at times know they are collecting and selling that information in violation of EU law.[15] For example, according to a Wall Street Journal report, one location data broker—Near Intelligence—directly passed data supplied for ad placement to government agencies, allowing them

[14] Fourth Amendment Is Not For Sale Act, H.R. 4639, 118 Cong. (2023).
[15] Chris Baumohl, *ODNI Report on Intelligence Agencies' Data Purchases Underscores Urgency of Reform*, EPIC (July 7, 2023), https://epic.org/odni-report-on-intelligence-agencies-data-purchases-underscores-urgency-of-reform/.

to use the information for real-time tracking and surveillance.[16] According to the *Journal*, Near Intelligence's general counsel and chief privacy officer told leadership that "[w]e sell geolocation data for which we do not have consent to do so . . . we sell/share device ID data for which we do not have consent to do so [and] we sell data outside the EU for which we do not have consent to do so." According to the *Journal*, that same officer referred to the transfer of EU data as a "massive illegal data dump," adding that the U.S. government "gets our illegal EU data twice per day."

II. The Executive Order Does Not Sufficiently Address Problems Identified in Privacy Shield's Invalidation

The Framework suffers from many of the same independence and effectiveness defects found in Privacy Shield and Safe Harbor. The Executive Order implementing the Framework is not sufficient for a finding of adequacy under the GDPR because it permits widespread bulk collection of personal data with few limitations, created a redress mechanism with limited effectiveness for EU residents, and grants EU residents few meaningful privacy protections.

A. The Continued Existence of Bulk Data Collection

The Court of Justice of the European Union ("CJEU") has struck down two previous EU-US data transfer agreements, in large part because of bulk telephone and internet surveillance programs, and the Framework does not meaningfully address this bulk collection of personal data.[17] The Executive Order, instead, prioritizes targeted collection over bulk collection, but still allows bulk

[16] Byron Tau et al., *How Ads on Your Phone Can Aid Government Surveillance*, Wall St. J. (October 13, 2023), https://www.wsj.com/tech/cybersecurity/how-ads-on-your-phone-can-aid-government-surveillance-943bde04.

[17] Commission Decision of 16 July 2020 on the Case C-311/18 request for a preliminary ruling from the High Court (Ireland) in the proceedings Data Protection Commissioner v. Facebook Ireland Ltd, Maximillian Schrems; Commission Decision of 6 October 2015 on the Case C-362/14 request for a preliminary ruling from the High Court (Ireland) in the proceedings Maximillian Schrems v. Data Protection Commissioner.

collection in some circumstances (when the information is necessary to advance a "validated intelligence priority" that cannot be obtained through targeted collection). The Executive Order further states that the intelligence community should use "reasonable methods and technical measures" to ensure these activities collect only the information necessary to achieve these priorities. However, the language used is vague and couched in deference to the intelligence community. For example, the Executive Order authorizes signals intelligence agencies to:

- "understand[] or assess[] the capabilities, intentions, or activities of" among other foreign entities and "foreign-based political organization[s] [. . .] in order to protect the national security of the United States and of its allies and partners";
- "understand[] or assess[] transnational threats that impact global security, including climate and other ecological change, public health risks, humanitarian threats, political instability, and geographic rivalry";
- "protect[] against cybersecurity threats created or exploited by, or malicious cyber activities conducted by or on behalf of, a foreign government, foreign organization, or foreign person"; and
- "protect[] against threats to the personnel of the United States or of its allies or partners[,]" noting that personnel in this case includes any current or former member of the armed forces, any current or former U.S. official, and "any other person currently or formerly employed by or working on behalf of the United States government," as well as these same categories of individuals as they relate to allies and partners.

As written, it is unclear whether these purpose limitations actually restrict the use of bulk collection or merely memorialize the intelligence community's existing practices. In fact, these purpose limitations mirror guidance to the intelligence community published by President Obama in

Presidential Policy Directive 28,[18] which the Privacy and Civil Liberties Oversight Board ("PCLOB") found to mirror NSA's existing use of bulk data collection.[19] More importantly, the CJEU found this Directive to be inadequate in its Schrems II decision striking down Privacy Shield.[20] While this insight into how the intelligence community functions is an improvement over the Intelligence Community's typical total opaqueness, the Executive Order allows the President to update the list of authorized activities at any time without public release, which could allow for significant expansion.

B. *Fundamentally Limited Redress Mechanism*

The new redress mechanism set forth in the Executive Order remains fully within the Executive Branch, leaving both the Civil Liberties Protection Officer ("CLPO") and the newly appointed Data Protection Review Court ("DPRC") judges vulnerable to the whims of political forces. Furthermore, while the Framework is a marked improvement from previous frameworks, it fails at almost every level to provide meaningful redress. Complainants lack sufficient information or notice to file and appeal claims; it is unclear the extent to which the mechanism can provide meaningful redress and remediation even if a complainant manages to successfully plead their case; and finally, the Executive Order only contains a non-binding oversight mechanism for the CLPO and DPRC, meaning there will be few if any consequences for noncompliance to the Framework.

Lack of Independence

Both tiers of the redress mechanism exist fully within the Executive Branch. The Office of the Director of National Intelligence ("ODNI") is explicitly prohibited from interfering with the

[18] Presidential Policy Directive 28, "Signals Intelligence Activities" § 4 (Jan. 17, 2014) ("PPD-28").
[19] PCLOB, *Report to the President on the Implementation of Presidential Policy Directive 28: Signals Intelligence Activities* 6 (2018).
[20] Commission Decision of 16 July 2020 on the Case C-311/18 request for a preliminary ruling from the High Court (Ireland) in the proceedings Data Protection Commissioner v. Facebook Ireland Ltd, Maximillian Schrems.

CLPO's review or retaliating against the CLPO from carrying out its duty and the CLPO's decisions are binding on the Intelligence Community. However, the CLPO is still subject to the supervision of the Director of National Intelligence ("DNI"), i.e., the body that oversees the same surveillance activities the CLPO reviews. The DPRC judges and special advocates were appointed by the Attorney General in consultation with the Secretary of Commerce, the DNI, and the PCLOB.[21] While the Executive Order rightfully includes protections against arbitrary removal, it offers no protection against failure to renew the four-year positions as a form of retaliation.

Lack of Effective Judicial Remedy

First, complainants lack sufficient information to either file the initial complaint or appeal decisions from the CLPO and DPRC. Surveillance programs are, by necessity, cloaked in secrecy and subjects of surveillance are often unable to gather evidence identifying how they were surveilled and by whom. The redress mechanism itself also relies on the complainant engaging several authorities, including the correct competent authority in the EU member state who then submits qualifying complaints to the CLPO for review. After investigating, the CLPO then provides a summary notice to the complainant that neither confirms nor denies that the complainant was subject to U.S. signals intelligence surveillance. The CLPO would only be required to state that it either found no covered violations or that the DPRC "issued a determination requiring appropriate remediation." This does not give sufficient information to a complainant as to whether the decision should be appealed.

Furthermore, complainants are not included in the CLPO or DPRC proceedings, instead forcing complainants to rely on a Special Advocate appointed by the DPRC who will not have an attorney-client relationship with the complainant. In cases where the Intelligence Community

[21] *The Data Protection Review Court*, Off. Of Priv. and Civ. Liberties Dep't. of Just. (last updated Jun. 11, 2024), https://www.justice.gov/opcl/redress-data-protection-review-court.

appeals the DPRC decision, the Special Advocate is specifically prohibited from communicating with the complainant.

Second, even if complainants successfully navigate the redress mechanism, the "appropriate remediation" the Executive Order calls for must be specific to the complainant and "narrowly tailored to redress the covered violation." If a complainant is part of a larger class, such as a foreign-based political organization, the remediation would be specific to that complainant rather than addressing the systemic violation identified.

Third, and finally, the only oversight of the CLPO and DPRC's decisions allowed by the Executive Order is review by the PCLOB, a non-binding body that oversees the Intelligence Community. While the PCLOB provides crucial reporting on non-compliance with U.S. law, the Intelligence Community has repeatedly failed to follow the PCLOB's recommended remediations in other contexts, like the FISA Court.[22] The Framework does not provide any reassurances that the CLPO and DPRC, already suffering from serious conflicts of interest, would be subject to liability for non-compliant decisions.

C. EU Residents Will Receive Few Privacy Protections Under the Framework

The Intelligence Community operates its signals intelligence work outside of the typical Fourth Amendment framework and the Executive Order does not confer EU residents GDPR equivalent protections. The U.S. famously does not have a federal privacy law and the Intelligence Community, in particular, skirts traditional warrant requirements and the existing FISA process to

[22] *See, e.g.*, *In re [REDACTED], No. [REDACTED]*, at 58 (FISA Ct. Nov. 6, 2015) (criticizing the government's failure to timely purge improperly collected information); *In re [REDACTED]*, Mem. Op. & Order, No. [REDACTED] 87–89, 94–95 (FISA Ct. Apr. 26, 2017), https://www.dni.gov/files/documents/icotr/51117/2016_Cert_FISC_Memo_Opin_Order_Apr_2017.pdf (reprimanding the FBI and CIA for violating their respective purging requirements).

engage in surveillance abroad.[23] This leaves even U.S. residents with little to no protections beyond occasional post-hoc judicial review for collections and few internal controls on use and dissemination of personal data. By creating a clear framework for redress for EU residents, the Executive Order grants EU residents more rights than U.S. residents are entitled to—and those rights are still insufficient to meet GDPR standards.

III. Conclusion

While the Framework and Executive Order reflect sincere efforts to address the problems identified in Schrems I and II, they still fail to meet the necessary requirements for adequate protections under the GDPR and we have seen nothing in the past year to remediate these inadequacies. Until the U.S. Intelligence Community is meaningfully reigned in, any data transfer agreement between the European Union and the United States will be plagued by structural failures.

Respectfully submitted,

Calli Schroeder
Calli Schroeder
EPIC Senior Counsel and Global Privacy Counsel

[23] *Foreign Intelligence Surveillance Court (FISC)*, EPIC, https://epic.org/foreign-intelligence-surveillance-court-fisc/ (last visited Jun. 14, 2024) (describing the FISC's circumscribed review of Section 702 targeting and minimization procedures).