16 July 2024

**Via Email JUST-OL-INTERNATIONAL@ec.europa.eu**
Bruno Gencarelli
Head of Unit
European Commission Directorate General Justice and Consumers

Dear Mr. Gencarelli:

Thank you for seeking input from the Center for Democracy & Technology in Washington, and from CDT-Europe (collectively, "CDT") in connection with the first annual review of the EU-US Data Privacy Framework (DPF). Thank you also for inviting CDT to participate in the 9 July 2024 meeting on the same topic. You asked us to outline legislative, regulatory, administrative, and case law developments since July 2023 that are either relevant for compliance by certified U.S. companies with their obligations under the DPF, or that impact the limitations and safeguards applicable to law enforcement and intelligence-based access by U.S. authorities to personal information transferred from the EU. You also asked about the functioning of oversight and enforcement mechanisms relevant to the DPF, including the exercise of enforcement powers by the FTC and the Department of Transportation. Finally, though you asked about the functioning of the Data Protection Review Court, we focus on the other inquiries because to our knowledge, the DPRC has not yet heard a case nor issued the rules that will govern its procedures.

**Legislative Developments: Expansion and Reauthorization of FISA 702**
The most significant legislative development was the 24 April adoption by Congress of the Reforming Intelligence and Security America Act of 2024 (RISAA), which amended and reauthorized for two years Section 702 of the Foreign Intelligence Surveillance Act (FISA 702).

RISAA expanded the class of companies under U.S. jurisdiction on which FISA 702 disclosure directives could be served. Prior to RISAA, the class of companies that were "electronic communication service providers" (ECSPs) subject to FISA 702 consisted of "providers of electronic communications service" (such as Gmail and WhatsApp) and "providers of remote computing service to the public" (such as a cloud computing service with which a user might store an online "to do" list so they can add to it and cross things off, and that isn't shared with others through the service). They, and other communication service providers that have access to wire or to electronic communications in storage or in transit (50 USC 1881(b)(4)(D)), were defined as ECSPs subject to FISA 702 directives under 50 USC Section 1881a.

RISAA expanded the class of companies that could receive FISA 702 directives to include service providers who have access to equipment on which communications are stored or transmitted, with limited exceptions for restaurants, hotels, dwellings, and community facilities.

Thus, many U.S. companies that do no more than offer WiFi services to their customers are now entities that could be subjected to FISA 702 directives. Requirements in prior law that companies subject to FISA 702 directives had to provide a "communication service" no longer apply: a company that provides a different service can receive such directives. Requirements in prior law that the company be able to access the communications of its users no longer apply: access to the *equipment* on which such communications are stored or transit will suffice, even if the company never actually accesses those communications. The New York Times reported that the change in the law was meant to subject data centers in the U.S. to FISA 702 directives. While intelligence officials never publicly confirmed that reporting, data centers seem to fit squarely with the new legislative language: they have physical access to servers on which their clients — such as cloud service providers — have stored users' communications, and the data center typically does not access those communications as part of the service it offers. But many other companies would also qualify.

This change creates significant uncertainty about the reach of FISA 702. Representations that U.S. companies may have previously made that they are not subject to FISA 702 directives because they are not ECS or RCS providers, or other communications providers who can access their users' communications, can no longer be relied upon. A company asserting that it is not subject to FISA 702 directives can not have access to any equipment on which communications are stored or transmitted, but most companies have such access in one form or another.

Congress took this unfortunate step of expanding FISA 702 surveillance to a broader class of companies in response to 2022 and 2023 decisions of the FISA Court (FISC) and the FISA Court of Review (FISCR). They determined that a company that the government wanted to bring into the FISA 702 surveillance program was not an ECSP under the statute. The name and type of company that was the subject of that litigation is redacted from the opinions as classified information.

Pending legislation would narrow this expansion of the ECSPs subject to FISA 702 directives by limiting them to the type of entity at issue in the FISC and FISCR cases. That legislation, the Intelligence Authorization Act of Fiscal Year 2025, was reported unanimously by the Senate Select Committee on Intelligence in June. Section 1202 of that bill does not describe the type of company newly subjected to FISA 702 orders. Instead, it simply says that ECSPs added in April 2024 to the class of companies on which FISA 702 directives can be served encompasses only the type of company described in the secret portions of the FISC and FISCR cases. As a result, the types of companies that may be subjected to FISA 702 directives are today publicly unknown, and will remain publicly unknown even if Section1202 of the Senate Intelligence Authorization Act becomes law.

**Legislative Developments: Other Changes RISAA Made To FISA 702**

CDT had proposed a number of steps Congress and the Administration could take to strengthen the DPF and make it more likely that the Commission's adequacy determination regarding the DPF would survive review at the Court of Justice of the European Union. In particular, we recommended in a November 2022 report and thereafter that Congress codify limits on the breadth of permissible surveillance that President Biden placed in Executive Order (EO) 14086 "Enhancing Safeguards for U.S Signals Intelligence Activities". Those limits apply to FISA 702 surveillance and to surveillance directed abroad under EO 12333. Congress declined to do this. Consequently, our concerns regarding the inconsistency of the DPF redress mechanisms with Article 47 of the Charter of Fundamental Rights and the CJEU jurisprudence fully persist.

We also recommended that Congress outlaw "about" collection, which is the collection of communications that are not to or from a person targeted for FISA 702 surveillance, but rather communications that mention the target's phone number, email address, or other identifier. This permitted the collection of communications of persons with respect to whom there was no suspicion. "About" collection had been discontinued for a number of years because, for technical reasons, it could not be conducted lawfully. FISA 702 had permitted resumption of "about" collection upon notice to Congress that the technical issues had been resolved. They never were resolved. In RISAA, Congress accepted this recommendation and outlawed "about" collection altogether. This marked an improvement in the law, tempered by the fact that the improvement had no impact on current collection activities.

RISAA made some significant changes regarding the role of the amicus in FISC proceedings. The FISC can appoint these experts in cases where it seeks assistance with technical surveillance matters and with significant matters that pose civil liberties risks. The first change is that RISAA requires the routine appointment of an amicus in cases in which a FISA 702 certification is at issue. Amicus participation at the FISC in proceedings related to these certifications is a positive development for the EU-US data privacy framework. The amicus could, for example, point out how a proposed certification falls short of statutory requirements. However, because those requirements are not exacting, the value of this addition is somewhat limited. The FISC can waive the appointment of an amicus if it chooses to do so.

RISAA also requires that the amicus involved in consideration of FISA 702 certifications must have expertise in both intelligence gathering and civil liberties. Under prior law, civil liberties experience was sufficient for an amicus chosen by the FISC to participate in a FISC proceeding. Although adding the requirement of expertise in intelligence gathering might appear useful on the surface, as a practical matter it could prevent an amicus without such experience from participating and effectively limit the pool of amici to former intelligence officials. RISAA also bars the amicus from raising issues that the FISC has not asked it to address. This is problematic because the amicus may spot an issue the FISC would otherwise miss. It calls into question the degree to which the amicus can contribute to the fairness of FISC proceedings.

Section 1201 of the Senate Intelligence Authorization Act for FY 2025 would reverse some of these changes but leave in place the problematic new requirement that the amicus have intelligence gathering expertise. It would delete the requirement that the amicus be appointed in any case involving FISA 702 certifications. And, instead of limiting the amicus to the issues the FISC has identified to it, the legislation would free the amicus to raise other privacy and civil liberties issues in all FISC proceedings, including those involving FISA 702 certifications and consideration of novel surveillance techniques or interpretation of FISA 702. The bill would also expand the ability of the amicus to gain access to information it needs to do its job, and allow the amici to consult with one another. Prospects for final approval of these changes are uncertain because it is unclear how they will be received in the House of Representatives.

**Case Law and Administrative Developments Relating to the FTC**

The Federal Trade Commission (FTC) has beefed up its staff and has been aggressively enforcing consumer protection laws that are within its mandate. The FTC's enforcement actions with respect to data brokers are important to the integrity of the DPF. This is because data brokers' sales of information and services to U.S. law enforcement and intelligence agencies can circumvent statutory restrictions that Congress has placed on the companies that collect this data. As we point out in this 2021 report, Legal Loopholes and Data for Dollars, the 1986 Electronic Communications Privacy Act restricts the ability of ECS and RCS providers to disclose metadata directly to U.S. governmental entities, including law enforcement and intelligence agencies, without appropriate legal process. However, it leaves them free to disclose metadata to non-governmental entities, including to data brokers. Those brokers are not subject to the restrictions in ECPA because, generally, they are neither ECS nor RCS providers. As a result, unlike the companies that collected the data directly, the data brokers can sell or license to U.S. law enforcement and intelligence agencies metadata that they collect on their own or purchase from ECS or RCS providers without any legal process. When they do so in a deceptive manner, the FTC can, and has, stepped in. We generally applaud it, loudly, for doing so. Its data broker decisions have been groundbreaking.

However, the national security exception the FTC included in its recent settlement agreement with X-Mode seemed inconsistent with the FTC's role in enforcing the DPF. X-Mode is a data broker that sold precise location information to federal government contractors for national security purposes without disclosing such sales to consumers. The FTC entered into a settlement agreement with X-Mode to address this practice. But, the settlement agreement excluded location information collected outside the U.S. that was used for national security purposes and other security purposes. In our letter objecting to the security exemption, we pointed out that the FTC has jurisdiction over conduct that occurs abroad but that deceives people in the U.S. We argued that the security exemption in the X-Mode settlement agreement was unclear because it turned on the place where location information was "collected," which is often unclear. We also pointed out that it ran contrary to the assurances the FTC Chair had provided the Commission in a June 9, 2023 letter: When the FTC acts to address deceptive acts that are reasonably likely to cause foreseeable injury in the U.S., remedial action it can take to

protect domestic consumers can inure to the benefit of foreign consumers. In the X-Mode settlement, the FTC came up short in benefiting consumers outside the U.S. when it had the opportunity to do so.

The Supreme Court's June 28, 2024 decision in *Loper Bright Enterprises v. Raimondo* could have an adverse impact on the ability of the FTC to play the role contemplated for it in the DPF. In *Loper Bright*, the Supreme Court put an end to the deference federal courts used to be required to show agency interpretations of their authority under ambiguous federal statutes. This deference had been a key feature of U.S. administrative law since the Supreme Court established it in *Chevron v. Natural Resources Defense Council* forty years ago. Court deference to agency interpretations of vague laws can help agencies more aggressively police company misconduct and deception. Instead of deferring to the interpretations of law made by expert agencies such as the FTC, *Loper Bright* invites the lower courts to reach their own determinations of proper agency authority without deferring to the agency. This may increase concern of regulatory agencies like the FTC that their more aggressive efforts to carry out their regulatory mandates will be thwarted in the courts, and may make them more cautious.

**Case Law and Administrative Developments Relating To Intelligence Agencies**
The Supreme Court's decision in *Loper Bright* will probably not impact the actions of agencies charged with national security responsibilities such as the NSA, CIA, and the DOJ National Security Division.They are unlikely to be impacted by this case because courts grant their decisions deference under precedents other than *Chevron* that recognize the special expertise of the executive branch in national security matters.

The Director of National Intelligence took a significant positive step in July 2023 by declassifying the number of certifications that govern FISA 702 collection and the categories of information that each of them covers. CDT had been calling for declassification of the FISA 702 certifications for more than ten years. The DNI revealed that there are three certifications and that they cover, (1) foreign governments and related entities, (2) counterterrorism, and (3) combating proliferation. These are very general categories and their disclosure does not shed an enormous amount of light on the nature of FISA 702 surveillance, but they are a step in the right direction for more transparency about that surveillance.

Finally, we also wanted to bring to the Commission's attention the issue of vacancies at the Privacy and Civil Liberties Oversight Board (PCLOB). PCLOB plays a key role in overseeing U.S. intelligence surveillance to protect privacy and civil liberties. In particular, its reports on FISA 702 have revealed extremely helpful information about the operation of that program, and of the benefits, risks, and scope of the surveillance conducted under it. EO 14086 requires intelligence agencies to revise their policies and procedures to make them consistent with the enhanced safeguards in the EO. PCLOB has agreed to the President's invitation in the EO to review those policies and procedures to ensure that they comply with the requirements of the EO.

A full complement of members would help PCLOB complete this review. However, there is one vacant seat on the PCLOB for which President Biden recently made a nomination on which the Senate has not yet acted. In addition, the term of the Chair of the PCLOB has expired and the period during which she can remain will expire in January unless she is reappointed. CDT and fourteen other NGOs have called for reappointment of the Chair. Another Board member's term ends in January. If three of the five seats on the PCLOB become vacant, the staff for PCLOB will continue to do its work, but the PCLOB may be unable to complete this review and issue a report that is based on it. There is a risk that other priorities of the President and of Congress in this election year will crowd out efforts to ensure that all the seats at the PCLOB are filled.

**Conclusion**

Thank you again for seeking CDT's input in connection with your first annual review of the EU-US Data Privacy Framework. We hope that the information we have provided will be useful to you, and that you feel free to direct any additional questions to us as the review continues.

Sincerely,

Silvia Lorenzo Perez
Programme Director,
Security, Surveillance and Human Rights
CDT-EU
sperez@cdt.org

Greg Nojeim
Director,
Security and Surveillance Project
CDT Global
gnojeim@cdt.org