December 9, 2020

"Statutory and Non-Statutory Ways to Create Individual Redress for U.S. Surveillance Activities"

Appendix 1 to U.S. Senate Commerce Committee Testimony on "The Invalidation of the E.U.-U.S. Privacy Shield and the Future of Transatlantic Data Flows"

Peter Swire[1]

This document addresses a legal issue that calls for solution to enable continued lawful basis for flows of personal data from the European Union to the United States – individual redress. In *Schrems II*, the Court of Justice for the European Union held that the lack of individual redress in the United States for persons in the EU purportedly surveilled by U.S. intelligence was a basis for finding that the Privacy Shield, as approved by the EU Commission, did not provide "adequate" protection of personal data. In this setting, individual redress refers to the ability of an individual, including an individual in the European Union, to receive a determination that their rights have not been violated by U.S. national security surveillance.

For a U.S. audience, it is important to understand that the requirement of individual redress is a constitutional requirement, under Article 47 of the EU Charter of Fundamental Rights. The European Data Protection Board (EDPB) in November published the "European Essential Guarantees" based on the jurisprudence of the European Court of Justice and the European Court of Human Rights. One of the four essential guarantees, as described by the EDPB, is that "effective remedies need to be available to the individual." This appendix to my December 9 testimony before U.S. Senate Commerce Committee seeks to identify issues and suggest possible approaches to meet the individual redress requirement. The testimony for which this is an appendix contains a summary discussion of the issue of individual redress. This appendix provides more detailed analysis and legal citations, in hopes of advancing discussion of the individual redress issue.

This appendix to my testimony to the Committee has three sections:

1. Discussion of the proposal that I published on August 13 with Kenneth Propp, entitled "After *Schrems II*: A Proposal to Meet the Individual Redress Problem." This article proposed ways that a new U.S. statute could apparently meet the EU legal standard for individual redress.
2. On October 14, European legal expert Christopher Docksey published "Schrems II and Individual Redress – Where There's a Will, There's a Way." This article found the Propp/Swire approach promising, while pointing out important aspects of EU law to be considered in any U.S. system for individual redress.
3. Discussion of non-statutory approaches for individual redress. Since August, working with others at the Cross-Border Data Forum, I have examined lawful ways to meet the goals of

[1] Elizabeth and Tommy Holder Chair of Law and Ethics, Georgia Tech Scheller College of Business; Research Director, Cross-Border Data Forum; senior counsel, Alston & Bird LLP. The opinions expressed here are my own, and should not be attributed to the Cross-Border Data Forum or any client. For comments on earlier versions of the research, I thank Théodore Christakis, Dan Felz, Robert Litt, and Kenneth Propp. Errors are my own.

the initial proposal, in the event that Congress does not pass a new statute to do so.[2] This appendix includes a number of ideas that have not previously been published.

The discussion here necessarily addresses details of multiple areas of law, including constitutional, statutory, and administrative provisions of both U.S. and EU law, and including the complex legal provisions governing U.S. national security surveillance under the Foreign Intelligence Surveillance Act (FISA) and other laws. As Christopher Docksey emphasizes, the U.S. need not have perfect "equivalence" with EU law – in our different constitutional orders, there may not be any lawful way to provide precisely the same procedures as apply under the General Data Protection Regulation (GDPR) and EU fundamental rights law. Instead, the standard announced by the CJEU is "essential equivalence," a legal term that has been the subject of extensive interpretation by the CJEU. As EU courts have stated, the "essence of the right" must be protected. The effort here is to further the discussion of how such protections might be created under U.S. law.

I. Individual Redress Proposal Based on U.S. Statutory Change

On August 13, Kenneth Propp and I published in *Lawfare* "After *Schrems II*: A Proposal to Meet the Individual Redress Problem."[3] In that case, the CJEU observed that the U.S. surveillance programs conducted under Section 702 of the Foreign Intelligence Surveillance Act (FISA) or EO 12333 do not grant surveilled persons "actionable" rights of redress before "an independent and impartial court." The Court emphasized that "the very existence of effective judicial review designed to ensure compliance with provisions of EU law is inherent in the existence of the rule of law." It added that "legislation not providing for any possibility for an individual to pursue legal remedies in order to have access to personal data relating to him or her" fails to "respect the essence of the fundamental right to effective judicial protection," as set forth in Article 47 of the EU Charter of Fundamental Rights.

The CJEU identified two ways in which U.S. surveillance law lacks essential equivalence to EU safeguards. The first, and the focus of this article, is that the U.S. lacks an "effective and enforceable" right of individual redress. The second, which is beyond the scope of the proposal we offer here, is the finding that there is a lack of "proportionality" in the scale of U.S. intelligence activities. As discussed in the initial proposal, the CJEU thus measures U.S. surveillance law protections against an idealized, formal standard set forth primarily in EU constitutional law.

A. Lessons from *Schrems II* About Redress

The Privacy Shield was itself an iterative response to the criticisms of U.S. surveillance law voiced by the CJEU in striking down its predecessor, the Safe Harbor Framework, in 2015. In that prior ruling, the Court emphasized the importance of effective redress to protect surveilled persons, with an independent decision-maker providing protection for the individual's rights.

[2] Following the publication of the August proposal, I was asked by U.S. officials about the possibility of a non-statutory approach for individual redress. I then developed the non-statutory ideas that are published here for the first time, and described them to officials in response to their request.

[3] Kenneth Propp & Peter Swire, "After *Schrems II:* A Proposal to Meet the Individual Redress Problem."[3]

In response, the United States agreed in the Privacy Shield to designate an Ombudsperson, an Under Secretary of State, to receive requests from Europeans regarding possible U.S. national security access to their personal data, and to facilitate action by the U.S. intelligence community to remedy any violation of U.S. law. This role was built on top of the Under Secretary's previously assigned responsibilities under Presidential Policy Directive 28 as a point of contact for foreign governments concerned about U.S. intelligence activities. No change in U.S. surveillance law was needed to establish the Ombudsperson—only the conclusion of an interagency memorandum of understanding between the Department of State and components of the U.S. intelligence community.

In *Schrems II*, the CJEU disapproved of the Privacy Shield's Ombudsperson innovation. The Court observed that the Under Secretary of State was part of the executive branch, not independent from it, and in any case lacked the power to take corrective decisions that would bind the intelligence community. An inquiry conducted by an administrative official, with no possibility of appealing the result to a court, did not meet the EU constitutional standard for independence and impartiality, the CJEU held.

The implications of the CJEU's decision support the conclusion that any future attempt by the United States to provide individual redress, to meet EU legal requirements, must have two dimensions: (1) **a credible fact-finding inquiry** into classified surveillance activities in order to ensure protection of the individual's rights, and (2) **the possibility of appeal to an independent judicial body** that can remedy any violation of rights should it occur.

B. Possible Factfinders

In devising a system of individual redress for potential surveillance abuses, the first question is where best to house the fact-finding process. Our initial proposal mentioned two possible ways to conduct such fact-finding. The first is to task fact-finding to existing Privacy and Civil Liberties Officers (PCLOs) within the intelligence community, as established by Section 803 of the Implementing Recommendations of the 9/11 Commission Act of 2007. The second is to enlist the Privacy and Civil Liberties Oversight Board, and independent agency tasked with oversight of intelligence community activities. Since we wrote the proposal, as discussed below, the suggestion has also been made that fact-finding could be carried out by the Office of the Inspector General in the relevant intelligence agency.

Beyond the question of whom in the U.S. Government is best-placed to act as a factfinder, a new system of individual redress would need to define the standard for that investigation. To meet the legal standard announced by the CJEU, the system would apply at least to individuals protected under EU law; the system might also enable actions for individual redress for U.S. persons. Precise definition will require the involvement of experts within the U.S. intelligence community as well as those knowledgeable about surveillance-related redress procedures in European countries. A legal standard for all complaints, at a minimum, would likely test compliance with U.S. legal requirements, such as whether collection under FISA Section 702 was done consistent with the statute and judges' orders governing topics such as targeting and minimization. In addition, a future agreement between the U.S. and the EU or other third countries

could add provisions forming part of the investigative standard. For instance, as discussed below, there may be a way to state explicitly that the surveillance will be necessary and proportionate, which are important legal terms under the EU Charter of Human Rights and the European Convention on Human Rights. Our proposal noted that the U.S. might perhaps negotiate to ensure that the EU provide reciprocal rights for U.S. persons with respect to any surveillance conducted by EU Member States. Similarly, the new redress system might address other issues, including whether individuals would ever receive actual notice some period of time after they have been surveilled. Such notice has been an element of EU data protection law, although notice of intelligence activities appears to have been a rarity there in actual practice.

The fact-finding process would logically have two possible outcomes – no violation, or some violation that should be remedied. Where there is no violation, there would be a simple report to the individual, or perhaps to a Data Protection Authority acting in the EU on behalf of an individual. Under the Privacy Shield, the report was that there had been no violation of U.S. surveillance law or that any violation has been corrected. This sort of limited reporting about classified investigations exists for the U.K. Investigatory Powers Tribunal, which is prohibited from disclosing to the complainant "anything which might compromise national security or the prevention and detection of serious crime." As Christopher Docksey has noted, this type of reporting can also be found in Article 17 of the Law Enforcement Directive (EU) 2016/680.

Broader disclosure about classified investigations risks benefiting hostile states, terrorist groups or others. By contrast, where any violation is found, then no report could be given until the violation was remedied. For instance, if there was illegal surveillance about the person seeking redress, the personal data might be deleted or any other measure taken to remedy the violation.

C. Judicial Review in the FISC

In the initial article, we stated that the obvious and appropriate path for an appeal from the fact-finding stage would be to the Foreign Intelligence Surveillance Court (FISC). FISC judges, along with other federal judges, meet the gold standard for independence, since Article III of the U.S. Constitution ensures that they have lifetime tenure and are located outside of the executive branch. Making the FISC responsible for the adjudication of individual complaints would go in some respects go beyond the FISC's current institutional responsibilities, but the federal judges on the FISC are experienced in reviewing agency decisions in non-FISC cases. The FISC is better-suited than an ordinary Article III court would be, because of its specialized expertise in U.S. surveillance law and well-established procedures for dealing with classified matters. As discussed in more detail below, the FISC already provides judicial oversight for the FISA Section 702 program—and has a proven track record of effective oversight. In the wake of the Snowden revelations, numerous FISC decisions were declassified and made public. A detailed review of these decisions concluded: "The FISC monitors compliance with its orders, and has enforced with significant sanctions in cases of noncompliance."

A key legal issue in crafting such a system is ensuring that a plaintiff has "standing" to sue, as required by Article III of the U.S. Constitution. In the Irish High Court decision in *Schrems II*, Judge Costello wrote that "All of the evidence show that [standing] is an extraordinarily difficult

hurdle for a plaintiff to overcome" in government surveillance cases. In summary, the plaintiff must show: (1) he or she has suffered injury in fact (2) that is causally connected to the conduct complained of and (3) is likely to be redressed by a favorable judicial opinion. Under EU law, an individual such as Max Schrems can bring a successful case without proving that he was ever under surveillance by the U.S. government. By contrast, as explained by Tim Edgar in *Lawfare*, plaintiffs in the U.S. have had to clear a high hurdle to establish standing and gain a legal ruling about the lawfulness of surveillance.

To assure standing for these appeals to the FISC, a mechanism similar to the one utilized under the U.S. Freedom of Information Act (FOIA) appears feasible. Under FOIA, any individual can request that an agency produce documents, without the need to first demonstrate particular "injury." The agency is then under a statutory requirement to conduct an effective investigation, and to explain any decision not to supply the documents. After the agency completes its investigation, the individual can appeal to federal court to ensure independent judicial review. The judge then examines the quality of the agency's investigation to ensure compliance with law, and he or she can order changes in the event of any mistakes by the agency.

Analogously, when seeking individual redress on a matter relating to national security, the FISC could independently assess whether the administrative investigation met statutory requirements, and the judge could issue an order to correct any mistakes by the agency—including by correcting or deleting data or requiring additional fact-finding. This sort of judicial review of agency action is extremely common under the Administrative Procedure Act that applies broadly across federal agencies. Typically, the judge must ensure that the agency action is not "arbitrary, capricious, an abuse of discretion, or otherwise not in accordance with law." There is standing on the part of the individual—a "case or controversy"—to assess whether the agency has properly discharged its statutory duties. As with FOIA, there is no need to determine whether the complaining individual has suffered injury in fact, since the statute creates a duty on the agency to act in a defined way.

We identify three features worth considering with this approach. First, due to the classified nature of the fact-finding, there may not be any workable way for the complainant to decide whether to bring an appeal. Therefore, it may make sense to have an automatic appeal to the FISC. Second, the 2015 USA FREEDOM Act established a role for appointed amici curiae who have full access to classified information and can brief the FISC on "legal arguments that advance the protection of individual privacy and civil liberties." These amici could play a role in advocating for the rights of the complainant, so that the FISC judge can receive briefing from both the agency and an amicus assigned to scrutinize the agency investigation. Third, Congress could consider whether the right to file a complaint be extended to U.S. persons in addition to those making complaints from the EU concerning surveillance under FISA Section 702 and EO 12333. Congress should consider how to structure a meaningful right to redress while avoiding a flood of complaints. The experience from Europe, and from prior agreements such as Privacy Shield and the Terrorist Finance Tracking Program, suggests that the actual number of complaints would likely be manageable.

II. Assessment by European Data Protection Expert Christopher Docksey

On October 14, Christopher Docksey published in *Lawfare* an article that commented on the Propp/Swire proposal, "Schrems II and Individual Redress – Where There's a Will, There's a Way." Docksey is a leading expert in EU data protection law, after a career as senior lawyer for the EU Commission and then Director and Head of Secretariat of the European Data Protection Supervisor.

Docksey was kind enough to state that "Propp and Swire's proposal provides a valuable framework for discussions by U.S. policymakers on a durable solution to individual redress in the United States." His objective was to respond to the proposal "from a European perspective, to underline the acceptable elements of their proposal and clarify which questions remain." He said: "The key to identifying potential points of future compromise by the EU is understanding the nature of three different types of institutions: "data protection officers (DPOs), independent supervisory authorities (DPAs) and courts."

A. Fact-Finding Phase

For the fact-finding phase, we suggested either the Section 803 Privacy and Civil Liberties Officers (PCLOs) or the PCLOB. Docksey explored having the fact-finding conducted either by the Office of Inspector General (OIG) or else the PCLOB.

In assessing the PCLOs, Docksey compares them to DPO's, whom he describes as "part of the organization of the data controller but have the right and duty to act independently in carrying out their roles." Because they are within the organization itself – the federal agency – Docksey concludes they do not meet the EU requirement of "independent oversight."

Docksey examines the role of the OIG, and concludes: "It could be useful to explore whether the powers of the inspectors general could be strengthened to hear complaints referred by PCLOs and adopt binding orders for corrective action." As a potentially important factor for the EU legal analysis, OIG's have a reporting relationship to Congress – outside of the agency itself. As a legal risk of deploying the OIG's, Docksey observes that an Inspector General "can be easily removed, as recent experience shows."

Under Docksey's analysis, the PCLOB, as an independent agency, is most similar to the European institution of the data protection authority. As shown in a report by the EU Fundamental Rights Agency, national law in the EU varies in the manner of supervision. Some nations enable their usual DPA's to have oversight for national security investigations. Others, such as the Netherlands, have independent supervisory agencies specifically for intelligence activities. Docksey underscores the EU legal requirement of the right to independent supervision by a DPA, which "is enshrined as a specific element of the right to protection of personal data in Article 8(3) of the EU Charter and in Article 16(2) of the EU Treaty itself."

Assuming that the PCLOB has legal authority to conduct the investigation, therefore, the most analogous U.S. institution to a DPA, for conducting the fact-finding, would be the PCLOB.

Concerning legal authority, the statute creating the PCLOB specifically provides that it shall have the power to review and analyze actions the executive branch takes to protect the U.S. from terrorism. The PCLOB's actions, however, have not been limited only to terrorism-related activities. As shown on the agency's website, the PCLOB has taken additional actions, including under Executive Order 13636 on Improving Critical Infrastructure Cybersecurity, as well as a request from the President that the Board provide an assessment of implementation of Presidential Policy Directive 28 (PPD-28), concerning protection of privacy and civil liberties in U.S. signals intelligence activities. By statute, Congress could explicitly authorize a role for the PCLOB in the individual redress process. As discussed further below, even in the absence of a statute, there would appear to be a legal basis for the PCLOB to play a role in a new individual redress process.[4]

In conclusion on the fact-finding phase, there are multiple possible ways to create the independent fact-finding process required under EU law. In addition, as Docksey explains in detail, the EU legal standard is not "absolute equivalence"; instead the U.S. must provide "essential equivalence" to EU legal protections. Docksey in his article explains reasons, in his view, why some U.S. approach to individual redress could indeed meet this "essential equivalence" standard.

B. Judicial Review in the FISC

Once the fact-finding phase is complete, Docksey emphasized the constitutional requirement, under EU law, for judicial review. Article 47 of the EU Charter states the constitutional text – there must be a right to an "effective remedy before a tribunal."

In the *Schrems II* case, as quoted by Docksey, "the advocate general enumerated the criteria laid down by the CJEU to assess whether a body is a tribunal." The advocate general wrote that the decision hinges on "whether the body is established by law, whether it is permanent, whether its jurisdiction is compulsory, whether its procedure is inter partes, whether it applies rules of law and whether it is independent[.]" Docksey adds: "Probably the most important of these criteria is the requirement of independence. This means acting autonomously, without being subject to decisions or pressure by any other body that could impair the independent judgment of its members."

The FISC is a close fit for these announced criteria for judicial review:

1. Independence. For the most important criterion, each FISC judge meets the gold standard for independence. Decisions are made by a judge nominated by the President and confirmed by the Senate. Each judge has lifetime tenure, and cannot be removed except under the historically rare process of impeachment in the Congress.

[4] The PCLOB has a staff that is small compared to employment by U.S. intelligence agencies, so a problem might arise if there are many requests for individual redress. In response, first, my understanding is that there was only one request to the Privacy Shield Ombudsman in the five years that the position existed, so staffing may not be a problem. In addition, the agency may be able to assist the PCLOB in the fact-finding, such as by "detailing" agency individuals to work on behalf of the PCLOB. This sort of "detailing" has often been used in the federal government where expertise and staffing exist in one agency, but individuals are temporarily placed under the direction of the White House or a different agency.

2. Established by law and applies rules of law. The FISC is established by law in the Foreign Intelligence Surveillance Act (FISA) and other statutes. It applies rules of law, including these statutes and its published rules of procedure.
3. Permanence. The FISC is permanent, in the sense that the authorizing statutes continue in operation unless there is a new statute passed by the Congress.
4. Compulsory jurisdiction. The FISC is a federal court, established under Article III of the U.S. constitution. A federal judge acting in the FISC has the same judicial powers as a federal judge operating generally in the federal courts. For instance, the judge issues a binding order, punishable by contempt of court, in cases of non-compliance. As with federal judges generally, the binding order can apply to a federal agency as well as to individuals.
5. Procedure "*inter partes*." The FISC originally acted *ex parte*, without opposing counsel, and now has procedures to act "*inter partes*," with counsel in addition to the government. The Review Group on Intelligence and Communications Technology explained in 2013 the reason for this change:

> "When the FISC was created, it was assumed that it would resolve routine and individualized questions of fact, akin to those involved when the government seeks a search warrant. It was not anticipated that the FISC would address the kinds of questions that benefit from, or require, an adversary presentation. When the government applies for a warrant, it must establish 'probable cause,' but an adversary proceeding is not involved. As both technology and the law have evolved over time, however, the FISC is sometimes presented with novel and complex issues of law. The resolution of such issues would benefit from an adversary proceeding."
>
> Consistent with this recommendation, Congress created a set of *amici curiae*, experts in privacy and related matters, in the USA FREEDOM Act of 2015. 50 U.S.C. § 1803(1)(i). A judge in the FISC "may appoint an individual or organization to serve as amicus curiae, including to provide technical expertise, in any instance as such court deems appropriate." As part of any negotiation with the EU, the U.S. government could consider promising to request appointment of such an amicus curiae in any case involving the rights of an EU person. With such an appointment, the FISC would meet the EU criterion of procedure *inter partes*.

In conclusion on the Docksey article, the discussion here has indicated options, consistent with EU law, for fact-finding concerning a complaint by an EU person about a possible violation of rights. Appeal then could be to the FISC, which meets the EU legal criteria for a "tribunal." Docksey himself, after completing his analysis of the proposal, concluded: "It is time to grasp the nettle. A compromise is worth the effort. And if there is the will, there is a way."

III. Non-Statutory Variations on the Proposals

Since our proposal was published in August, it has become more urgent to consider ways to establish an individual redress procedure without necessarily awaiting a statute passed by the Congress, for at least three reasons:

1. Drafting a statute on these novel issues is a complex task, which even with full agreement among members of Congress could take substantial time to complete.
2. The possibility has grown that there may soon be large cut-offs of personal data from the EU to third countries such as the U.S. As Professor Théodore Christakis has recently explained, the November guidance from the European Data Protection Board appears to conclude that it is illegal, for a very wide array of routine business practices, to transfer personal data from the EU to third countries.
3. Non-statutory approaches are worth considering even if a somewhat better system might be created by a statute. A non-statutory approach quite possibly is the best way to ensure that data flows and privacy protections exist during an interim period while legislation is being considered. Drafting a non-statutory approach can benefit from commentary from experts in the U.S. and EU legal systems, and the U.S. and EU officials working on the issue can identify and address nuanced issues about how to meet legal and policy goals for an agreement. In short, a non-statutory approach may be sufficient long-term to provide individual redress by non-statutory means, although European law emphasizes the strength of protections memorialized in a statute. Alternatively, a non-statutory approach might bridge the period until Congress enacts a statute.

As with Parts I and II above, the discussion here addresses the fact-finding phase and then the possibility of judicial review.

A. Fact-finding Phase.

The discussion here of the Docksey article mentioned possible roles in fact-finding for the Section 804 Privacy and Civil Liberties Officers in each agency, the agency Inspectors General, and the PCLOB. The analysis here suggests possible ways that each might play a role in fact-finding without statutory change.

The Section 804 PCLO's are subject to an Executive Order or similar mandates from the President. As a general matter, an Executive Order, Presidential Policy Directive, or other executive action can take effect under the President's power under Article II of the U.S. constitution to "take care" that the laws are faithfully executed. For national security matters, the President also can act as Commander-in-Chief. Expertise in the possible scope of executive power resides in the Office of Legal Counsel in the U.S. Department of Justice, working with White House Counsel and other officials. As one example, the PCLO's could be ordered by the President to cooperate in specified ways with others involved in fact-finding, such as the PCLOB.

As Docksey notes, there is a strong tradition of reporting from the Inspectors General to Congress, and IG's have a history of independence, in order to investigate and report on the

agencies within which they reside. There may be ways by Executive Order or other executive action to strengthen IG independence, as Docksey suggests may be required by EU law.

As discussed above, the PCLOB plays the role of independent supervisory agency most closely analogous to the supervisory agencies that exist in the EU. Due to its independence, I am not sure the extent to which the PCLOB would be bound by an Executive Order or other presidential action. Nonetheless, one promising approach would be if the PCLOB entered into a legally-binding Memorandum of Understanding (MOU) with an executive branch agency. This MOU would be a public commitment by the PCLOB and the executive branch agency to act in agreed-upon ways to conduct fact-finding. To the extent that the EU has questions about the legal enforceability in court of such an MOU, any agreement with the U.S. leading to adequacy could be conditional on the MOU remaining in force. As with other adequacy determinations, the EU would periodically assess how procedures are working in practice, and the EU could therefore withdraw its adequacy finding if the MOU were not followed.

In conclusion on the fact-finding phase, there would appear to be considerable scope for executive action and/or agreements between agencies to put in place effective fact-finding mechanisms for individual redress. Drafting of such measures can be informed by the insights offered by Christopher Docksey in his articles, and from other experts.

B. Judicial Review by the FISC

As described in the Propp/Swire proposal, Congress can provide by statute for an appeal to go to the FISC. The discussion here suggests a legal approach, without the need for a statute, that may also enable appeal to the judges in the FISC. The basic idea is that the U.S. Government could request review by the FISC, as part of the court's inherent authority to review implementation of its Section 702 orders. The U.S. Government could promise, such as in an agreement with the EU, that it will petition the FISC to review each complaint under the redress system in this manner. As a result, independent federal judges would provide judicial review of the complaints, and have authority to issue binding orders in the event of violations.

The approach discussed here has not been published previously, so I offer it as an initial public draft, with relatively detailed citations to relevant authorities.

1. FISC Oversight of Section 702 Orders

The proposed approach would build on existing FISC supervision of national security surveillance. Judges in the FISC issue binding legal orders about how requirements apply for any surveillance under Section 702. FISC authorizes Section 702 surveillance each year by entering an order that evaluates the conduct of the 702 program over the past year, imposes new restrictions or requirements as appropriate, and approves targeting, querying, and minimization procedures for U.S. intelligence agencies. 50 U.S.C. § 1881a(j)(3) (requiring FISC to "enter an order" authorizing 702 program if government's annual certification meets statutory and constitutional requirements); *see also, e.g.*, *In re Government's Ex Parte Submission of Reauthorization Certifications and Related Procedures*, Case caption redacted (Foreign Int. Surv. Ct. Dec. 6, 2019), available here (order authorizing 2019 Section 702 intelligence programs).

In the U.S. legal system, federal judges have "inherent authority" under Article III of the Constitution to take judicial action in order to ensure compliance with judicial orders. FISC has Article III authority. *See, e.g.*, *In re: Certification of Questions of Law to the Foreign Intelligence Court of Review*, No. FISCR 18-01, at 8 (FISA Ct. Rev. Mar. 16, 2018), available here ("FISC's authority … is cabined by – and consistent with – Article III of the Constitution). Further, FISA expressly ensures FISC can exercise this authority in regards to FISC's own orders, stating that "[n]othing in [FISA] shall be construed to reduce or contravene the inherent authority of [FISC] to determine or enforce compliance with an order or … a procedure approved by [FISC]."

Under the proposed approach, the U.S. Government would essentially ask the FISC to do no more than exercise its inherent authority as an Article III court, to review that 702 intelligence activities conducted in regards to a specific individual complied with the FISC's own 702 authorization order and applicable law.

This approach would fit with FISC's general monitoring of the intelligence community's compliance with its orders and U.S. surveillance laws. The FISC Rules of Procedure already require the government to report any noncompliance with a FISC order. *See* FISC Rule of Procedure 13(b) (requiring the government to report all cases where "any authority or approval granted by [FISC] has been implemented in a manner that did not comply with [FISC's] authorization or applicable law"). The FISC itself has not hesitated to monitor and, if warranted, aggressively enforce compliance with its orders. Examples include the FISC's questioning the NSA's compliance with FISC orders governing the post-9/11 Internet metadata program, ultimately leading to the program's termination, or the FISC's more recent orders requiring the government to respond to the DOJ Inspector General's findings relating to the Carter Page and other FISA warrant cases, both of which are discussed in Appendix 2 to today's testimony.

Put another way, this approach fits well within the joint, ongoing system of oversight for 702 surveillance that the FISC and the U.S. Government already work together to provide. The Government subjects 702 surveillance to a range of oversight mechanisms, including day-to-day supervision within intelligence agencies, supervision by the Oversight Section in DOJ's National Security Division (NSD), and regular joint on-site audits of 702 surveillance by NSD and ODNI. *See, e.g., Joint Unclassified Statement to the H. Comm. on the Judiciary*, 114th Cong. 4 (2016), available here. Existing FISC orders also require the government to report violations of 702 authorization orders. *See* PCLOB 702 Report at 29-30 (referencing a still-classified 2009 FISC opinion imposing reporting requirements). All compliance incidents identified through these processes are reported to the FISC. The FISC reviews these compliance incidents as part of its annual 702 reauthorization. This review can give rise to FISC requiring remediation or imposing new restrictions on intelligence activities in its 702 authorization orders.

The approach also seems to fit within procedural, jurisdictional, and national-security constraints under which the FISC operates:

- The U.S. Government is entitled to ask FISC for relief. The FISC Rules of Procedure generally require "the government" or "a party" to file pleadings requesting relief from FISC. *See, e.g.*, FISC Rules of Procedure 6(a)-(b) (permitting "the government" to request

certain relief); 6(c)-(d) (permitting "a party" to request certain relief); 19(a) (permitting "the government" to file show-cause motions); 62(a) (permitting "a party" to move for publication of FISC decisions). If an individual were to file a petition with the FISC, this could give rise to questions about whether she is "a party" entitled to request relief. But it would seem clear that a motion from the U.S. Government would be from "the government" as contemplated under FISC rules.

- The U.S. Government should not face standing hurdles. When non-governmental parties have requested relief from FISC in the past, FISC has required them to plead Article III standing. *See, e.g., In re Opinions & Orders of this Court Addressing Bulk Collection of Data under [FISA]*, Misc. 13-08 (Foreign Int. Surv. Ct. Nov. 9, 2017), available here (chronicling litigation over whether ACLU had Art. III standing to request that FISC publish orders relating to Section 215 programs). In contrast, the U.S. Government is already entitled to obtain 702 authorization orders from FISC in *ex parte* proceedings, without needing to show standing. The Government should thus also be able to ask FISC to review and enforce compliance in connection with those same 702 orders.

- National security interests remain protected. In recent decisions, the FISA Court of Review has reasserted the FISC's "unique" national-security need to maintain secrecy. *See, e.g.*, *In re: Certification of Questions of Law to the Foreign Intelligence Court of Review*, No. FISCR 18-01, at 3 (FISA Ct. Rev. Mar. 16, 2018), available here (emphasizing that "[t]he very nature of [FISC's] work … requires that it be conducted in secret," and that FISC orders "often contain highly sensitive information" whose release "could be damaging to national security"). The proposed approach would not require FISC to disclose classified information, or otherwise impair the secrecy under which FISC normally operates.

2. What would the FISC Review?

A non-statutory proposal would need to define the scope of oversight the FISC can and would review. The statutory text of Section 702 states that the FISC oversees the targeting, querying, and minimization procedures of intelligence agencies. Based on that text, the FISC would have oversight at least over those procedures, but perhaps not more broadly. The EU potentially could seek very broad oversight, along the lines of "full compliance with all the rights of a data subject" under EU law. Defining the scope of oversight would quite possibly be an important subject of negotiation between the U.S. and EU.

Scope of FISC's subject-matter jurisdiction. The FISC can only operate within its subject-matter jurisdiction. Recent decisions of the FISA Court of Review have discussed the FISC's defined subject-matter jurisdiction, which may prevent non-parties from requesting relief that merely "relates to the FISC or the FISA," as opposed to relief expressly authorized by FISA. *See, e.g., In re Opinions & Orders by the FISC Addressing Bulk Collection of Data under [FISA]*, FISCR 20-01 at 18-19 (FISA Ct. Rev. Apr. 24, 2020), available here (holding FISCR did not have subject-matter jurisdiction to adjudicate ACLU request to declassify portions of Section 215 orders). The proposed approach, however, would merely ask FISC to confirm compliance with its own orders, which FISA expressly authorizes FISC to do.

Possibly build agreement with the EU into the scope of the targeting, querying, and minimization procedures. One potentially fruitful path is to include EU-relevant provisions in the annual authorizations by the FISC of Section 702. For instance, the targeting procedures might adopt language responsive to EU legal concerns, such as stating that targeting shall be done only as necessary and proportionate. If the FISC order concerning 702 required necessity and proportionality – key terms within EU law – then the FISC presumably could oversee implementation of those necessity and proportionality requirements. The U.S. Government would have the ability to request such language, or other language negotiated with the EU, in the targeting procedures, as part of its regular legal submissions to the FISC. The FISC could issue binding requirements on U.S. agencies to ensure compliance with its Section 702 orders

Due to the defined subject matter jurisdiction of the FISC, the court quite possibly would not have judicial authority to rule on the legality of surveillance under EO 12,333. The FISC review above is predicated on the FISC's authority to oversee implementation of Section 702 orders, but the FISC has no similar statutory authority over an executive order, such as EO 12333.

I offer five observations about EO 12,333:

- First, the fact-finding phase, potentially including intelligence agencies and the PCLOB, could apply to both Section 702 and EO 12,333. Perhaps legal theories could be developed about how the FISC could review, as an ancillary matter, the portion of the record pertaining to EO 12,333. My tentative conclusion, however, is that review of EO 12,333 surveillance would be outside of the scope of the FISC's authority, absent statutory change.

- Second, EO 12,333 surveillance may be sufficiently protected by the procedural steps before the complaint gets to the FISC. The PCLOB or an agency procedure, for instance, could be the final arbiter on EO 12,333 issues. Docksey specifically presents arguments about why a PCLOB decision might meet EU legal requirements.

- Third, the Commerce Department White Paper contains multiple arguments about why no further legal protections should be required for companies using standard contractual clauses. Importantly, for instance, the White Paper states that it is unclear how companies can "consider any U.S. national security data access other than targeted government requirements for disclosure such as under FISA 702." Under these approaches, the U.S. government has thus articulated reasons why the scope of individual redress should match Section 702, rather than including EO 12,333.

- Fourth, in practice, many companies are addressing EO 12,333 by taking additional safeguards with respect to secure communications when personal data leaves the EU, such as to come to the U.S. There is ongoing discussion among European actors about the extent to which use of strong encryption answers EU legal concerns about EO 12,333 surveillance. If such use of encryption turns out to meet EU legal requirements, then individual redress can apply to the cases where it is relevant, under Section 702.

- Fifth, and if the previous observations do not apply, I present as another possible approach the following analysis of why an effective regime of individual redress may meet the EU

legal standard of "essential equivalence," even if EO 12,333 is outside of that regime. In recent cases concerning data retention, the CJEU highlighted its jurisdiction where a government achieves surveillance via private actors, such as companies subject to a judicial order. By contrast, the CJEU did not say that it had jurisdiction, in the face of the national security exception to its jurisdiction, where a government performs surveillance directly (not through a private company). Judicial orders to private companies apply to Section 702, but not to government activities under EO 12,333. With the disclaimer that I am a U.S. lawyer, perhaps it is worth considering whether the EU "essentially equivalent" regime of individual redress, to that offered by the EU Member States, might apply only to judicially ordered actions by companies, that is, to Section 702. With the same disclaimer, the same limit on "national security" jurisdiction does not apply to the European Court of Human Rights, and potentially its jurisprudence would apply to the direct government actions under EO 12,333.

Conclusion

This document has attempted to set before this Committee and the public research to date about how to create a system of individual redress under U.S. law. Standing doctrine, under Article III of the U.S. constitution, can block many proposed ideas for offering individual redress to an individual. The Propp/Swire proposal explained how the analogy to FOIA can require an agency to act, with a court then empowered to review the agency action. Christopher Docksey has supplemented the initial proposal with his expert insights about EU legal requirements. The new discussion here then presents ways that valid individual redress might be created by the U.S. government, even before Congress is able to enact a statute.

Members of this Committee and other U.S policymakers may doubt whether it is desirable as a policy matter to create such systems of individual redress for EU citizens. In response, there is this simple point – the highest court of the European Union has stated, apparently as a matter of its constitutional law, that such individual redress is required. Absent a valid system of individual redress, any future agreement between the U.S. and EU will be subject to great risk of invalidation. Faced with that reality, the proposals here seek to present possible solutions. Creative alternative proposals are most welcome, and the task is important.