Testimony by Peter Swire[1]
Elizabeth & Tommy Holder Chair of Law and Ethics
Scheller College of Business
Georgia Institute of Technology

U.S. Senate Commerce Committee Hearing
"The Invalidation of the EU-U.S. Privacy Shield and the Future of Transatlantic Data Flows"
December 9, 2020

Chairman Wicker, Ranking Member Cantwell, and Members of the Committee, thank you for the opportunity to testify today on "The Invalidation of the EU-U.S. Privacy Shield and the Future of Transatlantic Data Flows."

I am Peter Swire, the Elizabeth and Tommy Holder Chair of Law and Ethics at the Scheller College of Business at Georgia Tech, and Research Director of the Cross-Border Data Forum. Since the mid-1990's I have worked intensively on the topic of data flows between the European Union (EU) and U.S., including as lead author of the 1998 book called "None Of Your Business: World Data Flows, Electronic Commerce, and the European Privacy Directive." I have worked on these issues as a government official and private citizen, and wrote expert testimony of over 300 pages for the 2017 trial in Ireland of the *Schrems II* case. A biography appears at the end of this testimony.

This hearing is important in part to create a clear public record about these complex and important issues concerning the European Union, the United States, and international flows of "personal data," which is often called PII or "personally identifiable information" in the U.S.

Part I of this testimony offers observations on legal and policy issues in the European Union. Key points include:

A. The **European Data Protection Board** in November issued draft guidance with an extremely strict interpretation of how to implement the *Schrems II* case.

B. The decision in *Schrems II* is based on **EU constitutional law**. There are varying current interpretations in Europe of what is required by *Schrems II*, but constitutional requirements may restrict the range of options available to EU and U.S. policymakers.

[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.

C. Strict EU rules about data transfers, such as the draft EDPB guidance, would appear to result in **strict data localization**, creating numerous major issues for EU- and U.S.-based businesses, as well as affecting many online activities of EU individuals.

D. **Appendix 1** to this testimony provides detailed proposals for one of the requirements of the EU Charter - **individual redress** for violation of rights in the U.S. surveillance system.

E. Along with concerns about lack of individual redress, the CJEU found that the EU Commission had not established that U.S. surveillance was "proportionate" in its scope and operation. **Appendix 2** to this testimony seeks to contribute to an informed judgment on **proportionality**, by cataloguing **developments in U.S. surveillance safeguards since** the Commission's issuance of its **Privacy Shield decision in 2016.**

F. Negotiating an EU/U.S. adequacy agreement is important in the **short term**.

G. A short-run agreement would assist in creating a better overall **long-run** agreement or agreements.

H. As the U.S. considers its own possible legal reforms in the aftermath of *Schrems II*, it is prudent and a normal part of negotiations to seek to understand **where the other party – the EU – may have flexibility to reform its own laws.**

Part II of the testimony provides observations on the U.S. political and policy landscape:

A. Issues related to *Schrems II* have largely been bipartisan in the U.S., with **substantial continuity** across the Obama and Trump administrations, and expected as well for a Biden administration.

B. **Passing comprehensive privacy legislation would help** considerably in EU/U.S. negotiations.

C. This Congress may have a **unique opportunity to enact comprehensive commercial privacy legislation** for the United States**.**

PART I: Observations on Legal and Policy Issues in the European Union

In the wake of the *Schrems II* decision very large data flows from the EU to the U.S. and other third countries may become unlawful. The likelihood and magnitude of such a blockage are uncertain, and depend significantly on how European actors interpret the *Schrems II* decision. With Kenneth Propp, I have written previously on the background of the *Schrems II* case, its holdings, and its geopolitical implications. In Part I of this testimony, I address legal and policy issues specifically about the EU.

A. The European Data Protection Board in November issued draft guidance with an extremely strict interpretation of how to implement the *Schrems II* case.

An apparently very strict interpretation of *Schrems II* appears in two documents issued, subject to public comment, by the European Data Protection Board on November 11, 2020. My discussion here draws on the clear and expert three-part commentary of Professor Théodore Christakis in the *European Law Blog*. As the body of national data protection regulators, the EDPB's views are important due to its official role in interpreting the GDPR as well as language in the *Schrems II* decision about its role in defining what supplementary safeguards are sufficient for transfers outside of the EU.

The EDPB issued its draft of the "European Essential Guarantees for Surveillance Measures" ("EEG Requirements"). This document summarized the fundamental rights jurisprudence of the European Court of Human Rights (housed in Strasbourg, and interpreting the European Convention on Human Rights) and the Court of Justice of the European Union (housed in Luxembourg, and interpreting European Union law including the EU Charter of Fundamental Rights). A key task of the EEG Requirements was to state the EDPB's understanding of what legal requirements a third country must have in order to "offer a level of protection essentially equivalent to that guaranteed within the EU." To simplify the EDPB's main point – if a third country (such as the U.S.) meets the EEG Requirements, then the country can be seen as providing "essentially equivalent" protections; if not, then the country does not provide "essentially equivalent" protections, and transfers of personal data would require additional safeguards.

Where "essentially equivalent" protections exist, then transfers to that country may be found "adequate" under EU law. This sort of "adequacy" determination was made by the EU Commission in 2016 for the Privacy Shield. Eleven countries currently have this sort of adequacy determination by the EU Commission. A new EU/U.S. agreement would presumably be based on a similar adequacy finding.

If an adequacy determination is not in place, then the *Schrems II* court stated that transfers from the EU to a third country can exist where "supplementary measures" or "additional safeguards" are in place. Along with the EEG Requirements, the EDPB released its "Recommendations on Supplementary Measures" on November 11. Prior to the EDPB guidance, the U.S. government issued its "White Paper" on "Information on U.S. Privacy Safeguards Relevant to SCCs and Other EU Legal Bases for EU-U.S. Data Transfers after *Schrems II*." Other expert commentators published detailed studies of how additional safeguards, well implemented, could create a lawful basis for continuing to use Standard Contractual Clauses or other mechanisms for transferring personal data from the EU to third countries including the U.S.

As Professor Christakis has explained, the EDPB interpreted the *Schrems II* decision to be far stricter than had the White Paper or other commentators. **The EDPB's EEG Requirements are so strict, as Christakis wrote, that "third countries might rarely if ever meet the EEG requirements." Data exporters, under the EDPB approach, would then have to rely on its Recommendations on Supplementary Measures. Christakis, however, found these are also exceptionally strict: "To sum up, the EDPB's guidance clearly indicates that no data transfer should take place to non-adequate/non-essentially equivalent countries unless the data is so**

thoroughly encrypted or pseudonymised that it cannot be read by anyone in the recipient country, not even the intended recipient."

B. <u>The decision in *Schrems II* is based on EU constitutional law. There are varying current interpretations in Europe of what is required by *Schrems II*, but constitutional requirements may restrict the range of options available to EU and U.S. policymakers.</u>

There are important and as-yet unresolved disagreements among EU experts about how to interpret the *Schrems II* decision. Disagreements about constitutional law are certainly familiar to the Senators and American lawyers. That sort of disagreement is what exists in Europe in the aftermath of *Schrems II*.

Much of the *Schrems II* decision relied on specific provisions in the EU Charter of Fundamental Rights, which came into force in 2009 along with the Treaty of Lisbon:

1. Article 47 of the Charter addresses the right to an effective remedy: "Everyone whose rights and freedoms guaranteed by the law of the Union are violated has the right to an effective remedy before a tribunal." Appendix 1 to this testimony examines issues arising under Article 47, notably what sorts of individual redress the U.S. might provide for EU persons with respect to U.S. surveillance practices.

2. Article 7 of the Charter addresses respect for privacy and family life: "Everyone has the right to respect for his or her private and family life, home and communications." This right to privacy is similar to the "right to respect for private and family life" in Article 8 of the European Convention of Human Rights, first signed in 1950.

3. Article 8 of the Charter is a data protection right. It states: "(1) Everyone has the right to the protection of personal data concerning him or her; (2) Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified. (3) Compliance with these rules shall be subject to control by an independent authority."

The EDPB guidance can illustrate the importance of how these fundamental rights protections will be interpreted after the *Schrems II* decision. To illustrate, suppose that each aspect of the draft EDPB guidance were required by the Charter of Fundamental Rights. In that instance, the European Union would have no legal authority to weaken constitutional protections, and the strict prohibitions on data transfers under the EDPB draft guidance would be required as a matter of EU constitutional law. Based on the review of that guidance by Professor Christakis, an enormous range of flows of personal data would be prohibited to the U.S., China, India and most or all other third countries in the world (except the small number with a current adequacy decision in place).

The draft EDPB guidance, in fact, would appear to be clearly stricter than constitutionally required by the *Schrems II* decision. After all, the CJEU went to considerable lengths to say that transfers using Standard Contractual Clauses remained lawful where "additional safeguards" were

in place; however, the EDPB guidance found no "additional safeguards" that would enable access to the personal data in a third country. It appears that the EDPB draft guidance would render the CJEU's discussion of additional safeguards to be a nullity.

Based on my discussions with other EU legal experts, many EU legal experts would find greater flexibility under EU constitutional law than provided by the EDPB draft guidance. Going forward, EU experts on fundamental rights will engage on what restrictions on data transfers are required by the Charter of Fundamental Rights, as contrasted with decisions of non-judicial officials.

In conclusion on EU constitutional requirements, a very strict interpretation of the decision may leave limited options open for policymakers. Going forward, EU experts on fundamental rights will engage on what restrictions on data transfers are required by the Charter of Fundamental Rights, as contrasted with decisions of non-judicial officials. Although the precise legal issues are different, the importance of constitutional doctrine is well known to U.S. lawmakers for free speech and other First Amendment issues. **Members of this Committee will therefore understand that legal, constitutional limits may affect what the EU Commission, the European Parliament, and other EU institutions can do in the wake of the *Schrems II* decision.**

C. Strict EU rules about data transfers, such as the draft EDPB guidance, would appear to result in strict data localization, creating numerous major issues for EU- and U.S.-based businesses, as well as affecting many online activities of EU individuals.

The European Union will continue its own deliberations about how strict are the limits on data flows, as a matter of either EU policy choices or fundamental rights jurisprudence. I will briefly discuss some practical effects of a strict approach, which appear considerable.

I will first address what one might call the "boy who cried wolf" theory. After all, concerns about EU cut-off of data have arisen repeatedly since the Data Protection Directive went into effect in 1998. At that time, the EU/U.S. Safe Harbor, and other practical measures, enabled commerce to proceed without great hindrance. Later, in 2015, the CJEU issued the first *Schrems* decision, and privacy experts advised companies that data flows from the EU might be cut. Then, the EU and U.S. negotiated the Privacy Shield, and commerce continued. More recently, the General Data Protection Regulation (GDPR) went into effect in 2018, along with warnings that it could shut down numerous business models. In practice, after often-considerable compliance efforts, most business has been able to continue under GDPR. After these three rounds of warnings of disaster that didn't materialize, it would be easy for people to assume that the aftermath of *Schrems II* will once again be less impactful on data transfers than doomsayers cry out.

My view, however, is that the possibility of major disruptions of data flows is far greater this time. The CJEU – the supreme court of Europe, whose decisions are binding on the member states – has reiterated its strong concerns about transferring data to countries whose surveillance systems fail to meet European standards. That same court would have the final word about any new EU-U.S. agreement, or any other legal mechanism that seeks to enable transfers to third countries. Depending on how one interprets the constitutional dimensions of *Schrems II* and the

many other high court decisions examined by the EDPB, the apparent room for policymaker discretion now seems more limited. In addition, based on my discussions with knowledgeable persons, there is a significant possibility that one or more of the largest companies in the world may come under court order to stop transfers, before the January 20 U.S. presidential inauguration. In short, this time may fit the old story, where the boy cried wolf once again, but this time the wolf was really there.

If many data transfers are cut off, then the effect would be data localization. The term "local" here would apply to the EU member states, the other countries in the European Economic Area, and the currently eleven countries that now have an adequacy determination. Transfers to the United Kingdom after the January 1, 2021 Brexit would appear to depend on the UK receiving an adequacy determination, which is currently being considered but has not been finalized.

As the possibility of data localization increases, it becomes increasingly important for organizations to determine what it would mean to implement localization, and for policymakers to understand the effects of localization. The most detailed examination of such data flows, of which I am aware, remains the book that I wrote with Robert Litan in 1998, called "None of Your Business: World Data Flows, Electronic Commerce, and the European Privacy Directive." Thanks to permission from its publisher, the Brookings Institution, that book is now downloadable from the Brookings website. Chapter 5 of the book addresses "privacy issues affecting many organizations," such as human resources, auditing, business consulting, and customer support such as call centers. Chapter 6 examines financial services in detail, and the effects on that large sector deserve careful attention. Chapter 7 looks at "other sectors with large trans-border flows", including business and leisure travel and e-commerce generally; it also looks at possible interruptions of pharmaceuticals research, which would be especially important to consider during the COVID pandemic, when sharing of personal data might be so important concerning the safety and efficacy of vaccines as well as other medical information.

Looking ahead, I plan to work with the Cross-Border Data Forum as soon as possible to update and extend the data localization analysis. I hope to publish initial pieces of that analysis in time to offer comments on the EDPB Guidelines, due December 21. Many types of data flows are the same as in 1998, but there are important new categories of data flows, perhaps most notably for cloud computing, where the personal data of individuals is often stored in a different country. Several current reports are also available that provide useful discussion of the impacts of cutting off data, including here and here. I welcome any information or suggestions about how to accurately describe the effects of data localization, such as under a strict interpretation of EU law.

Pending such additional study, I offer the following observations about the effects of a strict requirement of data localization:

1. **Companies may find it difficult or impossible to "fix" the problem themselves** – the legal problem concerns the rules for government access to personal data.

2. **Data localization would have enormous impacts on third countries other than the U.S.** *Schrems II* clarified that its rule apply to the U.S. in particular but also to all third countries that lack essentially equivalent protections.

a. Some countries, such as China, have woefully weaker safeguards against government surveillance than the U.S. does. It is therefore difficult for me to understand what additional safeguards might be taken to enable transfers to such countries. China is Germany's largest trading partner, illustrating the large effect on the EU (rather than the U.S.) of strict limits on transfers.
b. Other countries, such as Canada, are democracies with strong privacy regimes, but have not thus far received an adequacy determination. Even if the EU and U.S. reach an agreement, there will be legal uncertainty about whether and how transfers can continue to these other democracies.

3. Particular study should focus on the **effects on EU individuals**, who may lose access to services and face reduced choice about how to live their online life. Similarly, **EU-based businesses** may face serious obstacles, beginning but not limited to how they operate with their non-EU affiliates, suppliers, and partners. Detailed study of the effect on the EU will help EU decisionmakers weigh how to protect privacy while also meeting other goals, as stated by the CJEU in *Schrems II*, that are "necessary in a democratic society."

4. During **the coronavirus pandemic**, individuals and businesses rely more than ever before on online services, many of which are operated or managed across borders. Disruptions from data localization thus would appear to be especially great until we reach a post-pandemic time.

5. **In conclusion on the effects of a strict EU approach, it is vital to consider carefully what measures can satisfy all the relevant legal constraints. New solutions quite possibly are necessary to enable continued data flows along with the legally-required improvements in privacy protection.**

D. Appendix 1 to this testimony provides detailed proposals for one of the requirements of the EU Charter - individual redress for violation of rights in the U.S. surveillance system.

This testimony will briefly summarize key points from Appendix 1, which provides details on how the U.S. might craft a new system of individual redress to address the CJEU's concerns. The Appendix has three parts:

1. Discussion of the **August 13 proposal** by Kenneth Propp and myself, entitled "After *Schrems II*: A Proposal to Meet the Individual Redress Problem." In order to provide an effective fact-finding phase, a statute could create a mandate for intelligence agencies to conduct an effective investigation when an individual (or a Data Protection Authority on behalf of the individual) makes a complaint. This mandate is similar to the Freedom of Information Act – an individual does not have to show specific injury in order to make a FOIA request, and an individual similarly would not need to show injury to request the investigation. Once the fact-finding is concluded, the statute could provide for appeal to the Foreign Intelligence Surveillance Court (FISC).

2. Discussion of the article by **European legal expert Christopher Docksey** on "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. **New material about how the individual redress system could be created, even without a new statute.** In the fact-finding phase, executive branch agencies could be required to perform an investigation pursuant to a new Executive Order or other presidential action. An independent agency, such as the Privacy and Civil Liberties Oversight Board, could sign a memorandum of understanding that would bind the agency to participate in the process. One the fact-finding is complete, complaints that concern surveillance under Section 702 FISA could then go to the FISC. The FISC has continuing oversight of actions pursuant to its annual court order concerning Section 702. It appears that the government could promise to report the outcome of an investigation to the FISC, and the FISC could then review the fact-finding investigation to determine whether it complied with its court order.

As discussed in Appendix 1, "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."

Based on my experience, the fundamental rights orientation of EU data protection law has often emphasized the importance of a mechanism for an individual to make a complaint or access request. Then, there must be a mechanism with sufficient independence and authority to review the facts and issue an order to correct any violations. As the CJEU re-emphasized in *Schrems II*, Article 47 of the Charter requires "an effective remedy before a tribunal." **After working extensively on this subject, and speaking with both European and American experts, I believe it is vital and apparently feasible to construct a new system of individual redress with respect to actions by U.S. surveillance agencies. Creating such a system would directly respond to a repeated and important criticism to date of the "essential equivalence" of U.S. protections.**

E. Along with concerns about lack of individual redress, the CJEU found that the EU Commission had not established that U.S. surveillance was "proportionate" in its scope and operation. Appendix 2 to this testimony seeks to contribute to an informed judgment on proportionality, by cataloguing developments in U.S. surveillance safeguards since the Commission's issuance of its Privacy Shield decision in 2016.

Along with lack of individual redress, the *Schrems II* court found that the principle of proportionality requires that a legal basis which permits interference with fundamental rights must "itself define 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." (¶ 180). The court held that the 2016 Privacy Shield adequacy decision by the EU Commission did not show proportionality for Section 702 and EO 12,333. (¶ 184).

Concerning the issue of proportionality, I offer six observations:

1. Appendix 2 to this testimony provides "Updates to U.S. Foreign Intelligence Law since 2016 Testimony." Appendix 2 presents updates on the U.S. legal and regulatory regime for foreign intelligence surveillance that have occurred since testimony of over 300 pages that I provided to the Irish High Court in 2016 on the same subject (the "2016 Testimony"). **Taken together, the 2016 Testimony and Appendix 2 seek to present an integrated set of references that may inform ongoing assessments**, under European Union law, **of the proportionality and overall adequacy of protection** of personal data related to U.S. foreign intelligence law.

2. A proportionality assessment is quite different than the issue of individual redress. Redress is a specific assessment – a sufficient redress provision exists or it doesn't. by contrast, **"proportionality" can be a more wide-ranging and fact-based assessment, similar to defining a term such as "reasonable."**

3. As a related point, the *Schrems II* decision cites European law that privacy and data protection rights "are not absolute rights," but instead "must be considered in relation to their function in society. (¶ 172) In addition, standard data protection clauses are lawful "where do not go beyond what is necessary in a democratic society to safeguard, inter alia, national security, defence and public security." (¶ 144). **More documentation may thus be relevant as evidence of what is "necessary in a democratic society."**

4. Appendix 1, concerning individual redress, discusses the possibility of incorporating concepts such as **proportionality** and necessity, or related terms used in U.S. law, into the **targeting procedures for Section 702** approved annually by the FISC. I make this proposal for the first time in this testimony, and so there may be classified or other persuasive reasons why such an approach is inadvisable or unlawful.

5. In considering whether and how to issue an updated adequacy opinion about the United States, the EU Commission will thus have available **a considerable record that evidences the large number and high quality of safeguards within the U.S. surveillance system.** Chapter 6 of my 2016 Testimony cited a study led by Ian Brown, then of Oxford University, that concluded that the US legal system of foreign intelligence law contains "much clearer rules on the authorization and limits on the collection, use, sharing, and oversight of data relating to foreign nationals than the equivalent laws of almost all EU Member States." The U.S. government's White Paper this fall adds particulars about current safeguards.

6. With that said, European law to date has indicated that **"essential equivalence" of a third country is judged against the standards set forth by the CJEU, rather than a comparison of U.S. practices to the practices of the EU member states.** Professor Kristina Irion this year has explained the relevant EU doctrine. Supporters of U.S. or other third country adequacy might therefore complain about hypocrisy or an unfair standard, but such arguments to date have not prevailed in European courts.

In conclusion on proportionality, it is important for the United States and the EU Commission to develop a strong record for why Section 702 and other surveillance programs currently are "proportionate," or else consider reforms that do establish proportionality.

F. Negotiating an EU/U.S. adequacy agreement is important in the short term.

There are strong reasons for the EU and the U.S. to seek agreement in the short term, so that the EU Commission can issue an adequacy decision. I highlight five points:

1. **Especially in the wake of the very strict EDPB draft guidance, there is now considerable uncertainty about the lawful basis for many transfers from the EU to third countries, including the U.S.** As mentioned above, there may well be court orders issued, even before January 20, that prohibit transfers of personal data by one or more major companies based in the U.S.

2. My understanding is that the current administration has a process in place to engage immediately with the EU. Even though a Biden administration would have available experts on these EU/U.S. data issues, **there could be a disruptive delay after January 20 if discussions are not completed by then. The immediate discussions should take account of the legal and political realities facing the EU Commission –** it will only wish to enter into an agreement with a strong case that it is acting consistent with the CJEU decision in *Schrems II*. The U.S. thus has a stronger-than-usual incentive to make its "best and final offer" quickly, because of the limited time to renegotiate before January 20.

3. **To avoid potentially large disruptions, it makes sense to achieve a short-term package even if additional reforms and agreements may be possible in the longer-run.** For instance, an adequacy decision might be for a limited time, such as one year. That would provide a new administration and the EU time to develop longer-term agreements across both data protection and other issue areas, as the EU has indicated it would like to do. A deadline, such as one year, would provide a useful incentive for all concerned to continue to work intensively toward a longer-term solution.

4. **Any short-term approach should include, if possible, clear attention to key sectors, including medical research and financial services.** During the pandemic, it would be foolhardy to interrupt the ability of medical researchers and manufacturers to develop and test for the safety and efficacy of COVID-19 treatments and vaccines. In addition, the financial services sector has historically relied primarily on Standard Contractual Clauses for transfers, rather than Privacy Shield. My understanding is that to date there has been low risk within the EU of enforcement against the financial services sector, which I believe transfers large amounts of personal data daily for business and regulatory reasons. With strict approaches such as the EDPB draft guidance, there is now increased risk of disruption of the global financial system due to possible limits on transfers of personal data from the EU to third countries.

5. **There is an important reason, from the EU perspective, to issue an adequacy decision for the U.S. in the short term, even though *Schrems II* applies to third countries generally.** The specific judicial findings in Europe have been about essential equivalence and the U.S., even though the U.S. has stronger safeguards than most or all other countries for foreign intelligence surveillance and privacy. **An adequacy decision initially concerning the U.S. thus provides the EU time to clarify its overall approach for transfers to third countries**. Enforcement actions can meanwhile proceed with respect to other third countries, such as China, to enable the EU judicial process to make findings relevant to multiple third countries, and avoid a discriminatory impact on an allied nation – the U.S. – that has many safeguards already in place.

G. A short-run agreement would assist in creating a better overall long-run agreement or agreements.

As discussed through this testimony, there are urgent short-term difficulties concerning the lawful basis for transfers of personal data from the EU to third countries. I next explain four reasons why an adequacy agreement in the near future would assist in creating a better overall set of reforms and agreements in the longer-run:

1. In this testimony, I am suggesting the desirability of seeking an adequacy agreement in the short run, such as for one year. **This sort of breathing period would enable a new administration to engage systematically to create durable approaches for agreements with the EU on data protection and other issues.**

2. A short-term agreement would **provide the Congress with time to consider any legislation that may assist in creating a durable approac**h to enabling trans-Atlantic transfers while also protecting privacy, meeting EU and U.S. legal requirements, and achieving other goals including national security. As one example, non-statutory approaches for individual redress may be possible, as explained in Appendix 1, but a subsequent statute might improve on the non-statutory approach.

3. One category of legislation to consider is for **the U.S. to codify in statute safeguards that already exist in practice.** One example would be the protections for the personal data of non-U.S. persons, as provided currently in PPD-28. More broadly, Appendix 2 to this testimony provides examples of privacy-protective practices that currently exist but are not explicitly set forth by statute. This sort of codification could address EU concerns that informal guidance or even agency policies are not "established in law" as effectively as a statute or other binding legal instrument.

4. **On an even longer time scale, there are strong reasons for the U.S., the EU, and democratic allies to engage systematically on a realistic and protective set of guidelines for government access to personal data held by the private sector.** Such a process should include input from a range of expert stakeholders, including data protection/privacy experts but also experts in areas such as national security, law enforcement, and economic policy. I understand the OECD may move forward with such

an initiative, first proposed by Japan, on "free flow of data with trust" with respect to government access to data held by the private sector. Such guidelines, among other goals, could help define what safeguards are "necessary in a democratic society," both to protect fundamental rights and achieve other compelling goals.

H. As the U.S. considers its own possible legal reforms in the aftermath of *Schrems II*, it is prudent and a normal part of negotiations to seek to understand where the other party – the EU – may have flexibility to reform its own laws.

For understandable reasons, the bulk of discussion to date has focused on what reforms the U.S. might consider in order to meet legal requirements set forth in *Schrems II* and other CJEU decisions. With that said, my testimony today discusses reasons to seek both short-term and longer-term agreements with the EU on cross-border data issues. It is normal and prudent, in any negotiation, to understand where each party may have flexibility to negotiate. As one example, my view is that the U.S. should seriously consider reforms to enable individual redress for EU citizens related to U.S. surveillance activities. Where might the EU also consider reforming any aspect of its regime?

Recognizing that views might vary about what is possible as a legal or policy matter, I offer four observations:

1. For reasons discussed above, I believe there is room, consistent with the *Schrems II* decision, for the EDPB to make changes to its draft guidance – the CJEU contemplated some continuation of transfers where additional safeguards are in place, but the draft guidance is so strict that such transfers in practice appear to be eliminated. The analysis by **Professor Théodore Christakis examines specific ways the EDPB guidance might be amended consistent with EU law.**

2. Chapter V of the GDPR governs "transfers of personal data to third countries or international organizations." Article 46 of GDPR sets forth extensive measures to enable lawful transfers to third countries that have not received an adequacy determination under Article 45. A similar approach existed under Article 26 of the Data Protection Directive, which applied from 1998 until GDPR went into effect in 2018. If the EU came to the view that Article 46 had been interpreted more narrowly than intended, then **the EU could at least contemplate a targeted amendment to GDPR to clarify its intent to allow transfers under Article 46 with defined, appropriate safeguards.** Any such amendment might be politically painful and challenging within the EU; massive disruptions of global trade would also be painful and challenging.

3. **The legal basis for transfers to the U.S. might be stronger if the U.S. and the EU negotiated a formal international agreement, such as a treaty.** I have seen draft scholarship, not yet public, that indicates that the legal basis for transfers from the EU to a third country such as the U.S. might be stronger if done pursuant to a formal international agreement, such as a treaty. The Safe Harbor and Privacy Shield were not treaties. Such a treaty would presumably not be negotiated or implemented in the short term, but may be a useful longer-term approach.

4. **By contrast, in discussions with EU experts, they have clearly stated that an amendment to the Charter of Fundamental Rights would be extremely difficult or impossible to consider.** Americans can readily understand this view – imagine if another country insisted that the U.S. amend the First Amendment free speech guarantees. It will thus be important, as a matter of EU law, to understand what is required under the Charter. The Commission, Parliament, and other EU institutions are legally bound to follow the Charter, but have room outside those requirements to make decisions within their competence.

To date, there has been little or no visible discussion within the EU about reforming its own data protection laws, such as considering any change to GDPR. In discussing possible changes, I am not seeking to tell the EU how to write its own laws. **The limited point here is that the U.S. and other third countries, in contemplating difficult reforms to their own laws, can reasonably at least consider how the EU might make reforms as well. Any eventual agreements can then be built on an understanding of what is or is not legally possible within each legal system.**

PART II: Observations on U.S. Political and Policy Landscape

A. Issues related to *Schrems II* have largely been bipartisan in the U.S., with substantial continuity across the Obama and Trump administrations, and expected as well for a Biden administration. Issues related to the Privacy Shield, *Schrems II*, and trans-Atlantic data flows have been far more bipartisan in the U.S. than for many other policy issues. I briefly highlight six aspects of continuity

1. **Privacy Shield.** The EU-U.S. Privacy Shield was signed in 2016, under President Obama. The Trump administration has uniformly supported the Privacy Shield, including working closely with EU officials in its annual reviews.

2. **Enforcement by the Federal Trade Commission.** The FTC is an independent agency, charged with enforcing violations of the Privacy Shield, as part of its general authority to protect privacy and enforce against unfair and deceptive acts. Change in administration, in my view, has not affected and will not affect the FTC's commitment to enforce company commitments to protect privacy in cross-border data flows.

3. **PPD-28.** President Obama issued PPD-28, with its safeguards for non-U.S. persons in signals intelligence, in 2014. PPD-28 has remained in force under President Trump.

4. **Surveillance transparency and safeguards generally.** Appendix 2 to this testimony reports on safeguards and other developments in surveillance since the Privacy Shield was negotiated in 2016 and I provided my expert testimony in Ireland. The consistent theme in Appendix 2 is how transparency and surveillance safeguards have continued extremely similarly under the Obama and Trump administrations.

5. **Continued attention both to privacy and other goals such as national security.** As a member in 2013 of the Review Group on Intelligence and Communications Technology, I observed how seriously U.S. government officials treated both privacy and other important goals such as national security. My opinion is that similar attention to these goals has continued and will continue for each U.S. administration.

6. **A Biden administration can draw upon experts in these EU/U.S. data issues.** Another reason to expect policy continuity is that the Biden administration will have available experts in Privacy Shield and other EU/U.S. data issues. For example, key negotiators of the Privacy Shield, as signed in 2016, were Ted Dean, then in the U.S. Department of Commerce, and Robert Litt, then General Counsel for the Office of the Director of National Intelligence. Both Mr. Dean and Mr. Litt have been named as members of the Biden-Harris transition team.

In short, even though there are many differences on other policy matters, what is remarkable for EU/U.S. data issues is bipartisan agreement on issues of trans-Atlantic data flows.

B. Passing comprehensive privacy legislation would help considerably in EU/U.S. negotiations.

I believe that enactment of comprehensive commercial privacy legislation would greatly improve the overall atmosphere in Europe for negotiations between the EU and the U.S. about the effects of *Schrems II*.

This conclusion may seem counter-intuitive. After all, the CJEU holdings concerned only issues of U.S. intelligence access to personal data. By contrast, a commercial privacy statute would apply exclusively or primarily to private-sector processing of personal data. As a strict legal matter, a comprehensive commercial privacy law in the U.S. would not address the holdings in *Schrems II*.

Nonetheless, I am confident that a meaningful, protective commercial privacy bill would make an important difference. That is not only my own intuition, developed after a quarter-century of working on EU/U.S. data issues. In addition, I have asked the question to multiple European experts. **Their response has been unanimous and positive, along the lines of "Yes, that would make a big difference."**

Here are a few reasons to think enacting a comprehensive commercial privacy law would help:

1. **We have seen the link previously between U.S. intelligence surveillance and the EU reaction on commercial privacy.** The clearest example is what happened after the Snowden revelations began in June, 2013. Before that, it looked like the draft of GDPR was blocked or moving slowly through the EU Parliament. After that, GDPR was amended in multiple ways to be considerably stricter, including on the U.S.-led tech sector. GDPR passed the Parliament overwhelmingly in early 2014 by a 621-10 margin. EU Vice

President Viviane Reding, in her official statement on the vote, specifically referenced "the U.S. data spying scandals" as a reason for passage.

2. **The U.S. may soon become the only major nation globally that lacks a comprehensive commercial privacy law.** Whatever a person's views may be of the best approach to protecting privacy, the global trend is unmistakably in one direction – toward each country having a comprehensive commercial privacy law. Professor Graham Greenleaf in Australia has carefully documented these trends: "The decade 2010-2019 has seen 62 new countries enacting data privacy laws, more than in any previous decade, giving a total of 142 countries with such laws by the end of 2019." Perhaps more importantly, the four most significant recent exceptions to such a law have been the U.S., Brazil, India, and China. Brazil's new privacy law went into effect in 2020. India has nearly finished its parliamentary process to pass its law. China is also moving forward with a commercial privacy law (although its protections against government surveillance remain far weaker than in the U.S.). Simply put, unless the U.S. acts in the next Congress, the U.S. may be the only major nation globally that lacks a comprehensive privacy law.

3. **A U.S. privacy law would strengthen the hand of U.S. allies in the EU.** Currently, there are many in Brussels and throughout the EU who favor retaining a strong alliance generally with the U.S. That support for remaining allies was reflected, for instance, in the broad EU Commission draft, reported by the Financial Times, that "seeks a fresh alliance with US in face of China challenge.**"** More specifically, as seen for instance in a recent DigitalEurope study on the effects of *Schrems II*, many in Europe understand the harsh consequences to Europeans themselves of a major cut-off in data flows.

   From the European perspective, the 2000 Safe Harbor agreement and the 2016 Privacy Shield are examples of "special deals" that make transfers to the U.S. easier than transfers to the other countries in the world that lack a general adequacy finding. As the U.S. becomes an increasingly glaring exception on privacy laws, it becomes more and more difficult for those in Europe to explain why the U.S. should be a favored partner. **Put bluntly, the U.S. as the last holdout on a privacy law can look more like a "privacy pariah" than a "favored partner."** By contrast, enacting a U.S. commercial privacy law sends the message that the U.S. in general offers legal protections for privacy. With a U.S. privacy law in place, it becomes far easier in Brussels and the EU generally to complete a privacy deal with the U.S. As a related point, **serious progress on U.S. privacy legislation during the next two years, such as passage in a crucial committee such as Senate Commerce, can itself help foster progress in EU/U.S. negotiations by showing that passage of a U.S. privacy law is feasible.**

C. This Congress may have a unique opportunity to enact comprehensive commercial privacy legislation for the United States.

You as Senators have far greater insight than an outside observer can have about what is possible to enact in this Committee, the Senate, or the Congress in the next two years. With that said, **my own perspective is that the 117th Congress, convening this January, has the best chance to enact comprehensive federal privacy legislation that I have ever seen.**

I offer six reasons for believing that now is an unusual opportunity to pass privacy legislation:

1. **This Committee has already made a great deal of progress on finding areas of agreement between the political parties.** In 2020, there was significant convergence on draft legislation supported, separately, by Chairman Wicker and Ranking Member Cantwell. On the large majority of issues, the language was the same or similar. Historically, major legislation often passes after substantial work in a previous Congress. That previous work settles much of the final package. Then, there are intense and often difficult negotiations on the final issues, which for privacy appear to be federal preemption and private rights of action. Nonetheless, however difficult those two issues may be, it is far easier to come to a final deal on two issues than to try to draft an entire bill on a blank slate.

2. **Industry and all those concerned about EU/U.S. relations have a strong interest in passing comprehensive federal privacy legislation.** As just discussed above, there are compelling reasons why progress on U.S. privacy legislation would increase the possibility of a good outcome in the EU/U.S. negotiations. For the politically savvy companies that operate in both Europe and the United States, the benefit of supporting an overall U.S. law quite possibly outweighs any company-specific reasons to try to block the bill due to particular provisions in a privacy bill.

3. **Passage last month of the California privacy initiative provides business with a new, compelling reason to support federal privacy legislation.** In November, the voters in California approved a ballot initiative, called the California Privacy Rights Act (CPRA), which goes into effect on January 1, 2023. The effective date, in my understanding, is no coincidence – it gives the 117th Congress time to complete action on a federal law. CPRA, while having only mixed support from privacy and civil liberties advocates, would add new privacy restrictions, including in the area of online advertising. For this reason, online advertising companies and companies that buy online advertising have a new reason to support federal legislation. Taken together with business support due to the EU situation, the U.S. business community in general is more prepared to accept broad national privacy rules than ever before.

4. **The California privacy initiative creates the possibility of greater agreement on federal preemption.** To date, some members of this Committee have pushed for broad federal preemption of state privacy laws, for reasons including preventing business from having to comply with multiple and possibly contradictory state laws. Other members of this Committee have pushed to have the federal legislation be a floor but not a ceiling, allowing states to act first (as they have often done in the past) to enact greater protection of individual privacy. I have written three articles on preemption, about the history of federal privacy preemption, identifying key issues for preemption, and a proposal (co-authored with Polyanna Sanderson of the Future of Privacy Forum) for a process to narrow disagreement, based on case-by-case examination of the numerous existing state laws.

Building on this previous analysis, the recent passage of the CPRA creates a two-part proposal for how the differing sides on preemption can each achieve a substantial victory. First, as a win for those supporting privacy innovation in the states, the California Consumer Privacy Act, which went into effect already, would remain in effect. After all, businesses have already had to comply with that law, so the major costs associated with the law have already been spent. Second, the new federal law could preempt the CPRA, which does not go into effect until 2023. Industry would thus be spared the challenge of re-engineering their data systems again, so soon after complying with CCPA. In addition, important privacy advocates, including the ACLU of California and the Consumer Federation of California, actually came out in opposition to CPRA. There may thus be an opportunity to reach agreement on a significant example of preemption. If both sides of this fierce debate win a significant victory, then there may be more room to address remaining preemption issues as something of a technical drafting matter.

5. **A Biden administration will support federal privacy legislation.** The 2020 Democratic platform calls for enacting federal privacy legislation, and the Obama administration supported privacy legislation as part of the 2012 announcement of a "Privacy Bill of Rights." Joe Biden himself has long worked on these issues. He spoke to the European Parliament in 2010, garnering headlines such as this: "Biden vows to work with EU parliament on data privacy." In addition, a Biden administration can draw on numerous individuals who have extensive government experience on privacy, including those who worked on the Privacy Bill of Rights and negotiated the Privacy Shield.

6. **The narrow majorities in both the Senate and House likely help define the scope of the possible for federal privacy legislation.** As a resident of Georgia, I know only too well the intensity of effort for the two Senate run-off elections on January 5 – my wife and I have basically given up answering our home telephone for the duration. After those run-offs, one of the parties will have a narrow working majority in the Senate, and the margin in the House of Representatives is also unusually narrow. With such narrow margins, bipartisan cooperation will be at a premium – neither party can afford to support a privacy bill alone that would lose any of its members, so the clearest path to a majority is with bipartisan support. **Last year's proposals from the Senate Commerce Committee are the most logical starting point for negotiations.** New proposals from the wing of either party will likely have difficulty making it into the legislation, unless the proposals can garner support from a range of political viewpoints.

In conclusion on the prospects for federal privacy legislation, the stars may finally have aligned to enact meaningful privacy protections. A new federal privacy law would enshrine in law a considerable list of new privacy protections for individuals. The law would also have support from businesses who usually oppose new government regulation. **At a time when there is risk of partisan gridlock in Congress, federal privacy legislation could be a significant instance of bipartisan accomplishment.**

Background of the witness:

Peter Swire is the Elizabeth and Tommy Holder Chair and Professor of Law and Ethics in the Scheller College of Business at the Georgia Institute of Technology. He is senior counsel with the law firm of Alston & Bird, and Research Director of the Cross-Border Data Forum.

In 1998, the Brookings Institution published Swire & Litan, "None of Your Business: World Data Flows, Electronic Commerce, and the European Privacy Directive. In 1999, Swire was named Chief Counselor for Privacy in the U.S. Office of Management and Budget, the first person to have U.S. government-wide responsibility for privacy policy. Swire was the lead White House official during negotiation of the EU/U.S. Safe Harbor.

After the Snowden revelations, Swire served as one of five members of President Obama's Review Group on Intelligence and Communications Technology, making recommendations on privacy and other reforms for the U.S. intelligence community. In 2015, the International Association of Privacy Professionals awarded Swire its annual Privacy Leadership Award. In 2016 he was an expert witness in the Irish trial for *Schrems v. Facebook*, and submitted testimony of over 300 pages describing the legal safeguards for the U.S. intelligence community's use of personal data.

In 2018, Swire was named an Andrew Carnegie Fellow for his project on "Protecting Human Rights and National Security in the New Age of Data Nationalism." In 2019, the Future of Privacy Forum honored him for Outstanding Academic Scholarship.

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.

December 9, 2020

"Updates to U.S. Foreign Intelligence Law Since 2016 Testimony"

Appendix 2 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 Appendix supplements written testimony I am submitting to the Senate Committee on Commerce, Science, and Transportation for the December 9, 2020 hearing on "The Invalidation of the EU-U.S. Privacy Shield and the Future of Transatlantic Data Flows." This Appendix presents updates on the U.S. legal and regulatory regime for foreign intelligence surveillance that have occurred since testimony I provided to the Irish High Court in 2016 on the same subject (the "2016 Testimony").[2] Taken together, the 2016 Testimony and this Appendix seek to present an integrated set of references that may inform ongoing assessments, under European Union law, of the adequacy of protection of personal data related to U.S. foreign intelligence law.

My 2016 Testimony was submitted in November 2016, several months after the EU Commission adopted the finalized Privacy Shield in July 2016. At that time, I listed over twenty significant privacy-protective changes that had been made to US foreign intelligence laws since the Snowden disclosures in 2013.[3] My 2016 Testimony then discussed the systemic safeguards present in US law for foreign intelligence, including: (a) safeguards anchored in the statutes governing foreign intelligence surveillance by US agencies,[4] (b) interlocking executive, legislative, and independent oversight mechanisms that are in place for surveillance activities;[5] (c) transparency mechanisms implemented since the Snowden disclosures that offered a level of transparency into US surveillance practices unparalleled in other nations;[6] and (d) privacy safeguards implemented within the executive branch to protect personal information of non-US persons.[7] Chapter 5 of my 2016 Testimony also contained a detailed discussion of declassified opinions of the Foreign Intelligence Surveillance Court (FISC), including my assessment that the FISC has exercised careful and effective oversight over foreign intelligence surveillance.[8]

---

[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 research assistance on this appendix I thank Daniel Felz and Sara Guercio. This Appendix is based on publicly available information; I have not had access to any relevant classified information since 2016. The views expressed here are my own.

[2] PETER SWIRE, TESTIMONY OF PETER SWIRE (submitted to High Court of Ireland Nov. 3, 2016), *available at* https://www.alston.com/en/resources/peter-swire-irish-high-court-case-testimony/.

[3] *See id.* at 3-10 – 3-12.

[4] *See id.* at 3-12 – 3-26.

[5] *See id.* at 3-26 – 3-34.

[6] *See id.* at 3-34 – 3-38.

[7] *See id.* at 3-39 – 3-49.

[8] *See id.* at 5-1 – 5-53.

This Appendix highlights updates that have occurred since the 2016 period in which Privacy Shield and my Testimony was finalized. As an overview of what will be discussed in this Appendix, the following represents a summary of intervening developments that have resulted in greater safeguards, or the continued effectiveness of safeguards in place, since the 2016 period in which Privacy Shield and my prior Testimony were finalized:

1. The FISA Amendments Reauthorization Act of 2017 (FARA) introduced new safeguards for Section 702 programs, including:
   (a) mandating querying procedures for 702-acquired information,
   (b) codifying the National Security Agency (NSA) and Federal Bureau of Investigation (FBI) practice of appointing Privacy and Civil Liberties Officers,
   (c) expanding whistleblower protections to Intelligence Community (IC) contractors,
   (d) increasing disclosure and transparency requirements for Section 702 programs, and
   (e) imposing significant restrictions on the recommencement of Abouts collection.

2. The FISC has continued to annually evaluate Section 702 surveillance as required under Section 702, and its reauthorization orders have resulted in new protections for Section 702 programs.

3. As a result of FISC's continued supervision of Abouts collection the NSA (a) voluntarily terminated Abouts collection and (b) segregated and deleted all Internet transactions previously acquired through its Upstream program.

4. The Office of Director of National Intelligence (ODNI) has continued to declassify significant documents relating to Section 702 surveillance, such as publishing the Section 702 trainings that NSA provides to its internal personnel that conduct Section 702 programs on a day-to-day basis.

5. Due in part to compliance incidents reported to the FISC, NSA decided to delete three years' worth of Call Detail Records (CDRs) obtained under the USA FREEDOM Act. NSA then decided to suspend its CDR program in early 2019.

6. The Privacy and Civil Liberties Oversight Board (PCLOB) issued new oversight reports on (a) the NSA's Call Detail Records program under the USA FREEDOM Act, as well as (b) the implementation of Presidential Policy Directive 28 (PPD-28) in US intelligence agencies. PCLOB also recently announced it concluded an oversight review of the US Treasury Department's Terrorist Finance Training Program.[9]

[9] *See generally* U.S. Privacy and Civil Liberties Oversight Bd., *Press Release: Privacy and Civil Liberties Oversight Board Concludes Review of Treasury Department's Terrorist Finance Tracking Program*, (Nov. 19, 2019) *available at* https://documents.pclob.gov/prod/Documents/EventsAndPress/de7972f6-03f1-48fd-8acd-b719a658e4a0/TFTP%20Board%20Statement.pdf. PCLOB Chairman Adam Klein also issued a statement describing EU decisions to rely on TFTP instead of building its own equivalent program, and identifying privacy protective measures in place for EU citizens within TFTP, such as storage of EU bank customer data in the EU. *See* U.S. Privacy and Civil Liberties Oversight Bd., *Statement by Chairman Adam Klein on the Terrorist Finance Tracking Program*, (Nov. 19, 2020) *available at*: https://documents.pclob.gov/prod/Documents/EventsAndPress/b8ce341a-71d5-4cdd-a101-219454bfa459/TFTP%20Chairman%20Statement%2011_19_20.pdf.

7. The ODNI has continued to publish annual Statistical Transparency Reports showing numerical statistics that provide transparency on the extent to which US agencies are requesting data under FISA authorities, including Section 702 authorities.

8. The Department of Justice (DOJ) and ODNI continue to publish Semiannual Reports on the NSA's, FBI's, and CIA's compliance with Section 702 requirements, including statistics and descriptions of instances of non-compliance. These Reports continue to be created as a result of DOJ/ODNI's regular on-site reviews of the intelligence agencies.

9. US foreign intelligence law continues to permit companies to publish transparency reports. My review of leading technology companies' recent transparency reports shows that, as in 2016, US intelligence appears to affect a vanishingly small percentage of their active users.

10. ODNI has continued to publish significant quantities of declassified documents related to US foreign intelligence activities on the "IC on the Record" website. It also facilitated greater access to these documents by launching a text-searchable capability on Intel.gov.

11. FISC has continued to declassify opinions and publish statistics on its handling of government surveillance applications. The percentage of applications that the FISC has modified or denied has increased since 2016.

This Appendix discussed the above developments in eight Sections that track the structure of my 2016 Testimony: 1) updates to systemic safeguards for US foreign intelligence, 2) updates to Section 702 programs, 3) updates to the former 215 program, 4) updates to oversight safeguards, 5) updates to transparency safeguards, 6) updates to executive safeguards, 7) updates to Foreign Intelligence Surveillance Court (FISC) testimony, 8) updates to surveillance-related standing cases.

1. Updates to Systemic Safeguards for US Foreign Intelligence:

A significant portion of my 2016 Testimony discussed the systemic safeguards built into the structure of foreign intelligence in the United States.[10] The core and structure of these safeguards has remained unchanged since I testified in 2016. The US remains a constitutional democracy committed to the rule of law in conducting foreign-intelligence surveillance.[11] Further, US surveillance remains subject to an interconnected system of statutory safeguards,[12] oversight mechanisms,[13] transparency mechanisms,[14] and executive branch safeguards.[15] My detailed

[10] *See generally* SWIRE, *supra* note 2 at 3-2 – 3-49.

[11] *See id.* at 3-2 – 3-6.

[12] *See id.* 3-12 – 3-26.

[13] *See id.* at 3-26 – 3-34.

[14] *See id.* at 3-34 – 3-38.

[15] *See id.* at 3-39 – 3-49.

discussion of these safeguards can be read in my 2016 Testimony, as outlined in the introduction above.

2. Updates to Section 702 Programs.

Section 702 of FISA is the basis for significant foreign intelligence collection by US intelligence agencies, and was discussed at length in my 2016 Testimony.[16] Since 2016, the legal structure of Section 702 has remained largely unchanged. Section 702 requires the Attorney General and DNI to annually apply to the Foreign Intelligence Surveillance Court (FISC) to authorize Section 702 surveillance programs.[17] In doing so, the FISC reviews and authorizes the targeting, minimization, and (since 2018) querying procedures under which the intelligence agencies conduct Section 702 surveillance.[18] Throughout the ensuing year, the agencies' conduct of Section 702 programs is monitored by internal procedures, external audits, and regular reporting to the FISC and Congress.[19] The primary programs that exist under Section 702 remain (a) the Prism program, in which agencies such as the NSA serve directives on communications providers compelling the disclosure of communications to or from a tasked selector; and (b) the Upstream program, in which Internet backbone providers acquire communications to or from a tasked selector as they traverse the Internet.[20] My 2016 Testimony discusses the structure of Section 702 as well as its primary programs in detail.[21]

Despite broad continuity in Section 702 practice since my 2016 Testimony, a number of significant updates have occurred. This Section briefly summarizes a selection of these changes: (a) the FISA Amendments Act Reauthorization Act of 2017 and its privacy-protective aspects; (b) the FISC continues to reauthorize the Section 702 programs annually; (c) NSA terminated Upstream's Abouts collection in connection with 2017 FISC Reauthorization; (d) statistics on 702 programs continue to be released by the US government; (e) the US government continues to publish the Semiannual Assessment of compliance for 702 programs; and, (f) NSA declassified its internal guidance and training manuals for 702 programs.

a. FISA Amendments Reauthorization Act of 2017 (FARA)

In 2018, the FISA Amendments Reauthorization Act of 2017 (FARA) was passed, reauthorizing FISA for a five-year term and providing additional oversight and privacy protections.[22] Specifically, FARA i) mandated that intelligence agencies adopt querying procedures governing how they may access and use Section 702 intelligence; ii) codified the appointment of Privacy and Civil Liberties Officers in the NSA and FBI; iii) expanded whistleblower protections;

[16] *See id.* at 3-18 – 3-24.

[17] *See id.* at 3-18 – 3-21.

[18] *See id.*

[19] *See generally id.*at 3-2 – 3-49.

[20] *See generally id.*at 3-18 – 3-24.

[21] *See id.*

[22] *See* FISA Amendments Reauthorization Act of 2017, Pub. L. 115-118, (2018) [*hereinafter* "FARA"].

iv) increased agency disclosure requirements; and v) required an approval process if the NSA wishes to restart Abouts collections.[23]

i. *Mandatory Querying Procedures*

Before FARA, Section 702 mandated that intelligence agencies adopt "targeting" and "minimization" procedures, which collectively provided the standards by which individuals are targeted for foreign intelligence surveillance and how subsequently acquired communications may be retained and used. FARA added a requirement that the NSA, FBI, CIA, and NCTC adopt "querying" procedures governing how these agencies are permitted to access and search 702-acquired communications.[24] Like targeting and minimization procedures, Section 702 querying procedures must be annually submitted to the FISC for approval, and FISC must evaluate them for consistency with FISA and "the requirements of the Fourth Amendment."[25] While FARA set forth specific requirements for US person queries,[26] the querying procedures adopted by US intelligence agencies contain safeguards for all individuals regardless of nationality. For example, the NSA's 2019 Querying Procedures state that "[e]ach query of NSA systems containing unminimized content or noncontent information acquired pursuant to section 702 … must be reasonably likely to retrieve foreign intelligence information."[27] These requirements, and FISC's annual review of how they are followed by US intelligence agencies, help support proportional use of communications acquired under Section 702.

ii. *Ratification of Appointment of PCLOs within Agencies*

Under its Section 109, FARA expressly required the NSA and FBI to appoint Privacy and Civil Liberties Officers (PCLOs).[28] This change represented more of a change in law than in practice, since both NSA and FBI already had active PCLOs in place as a matter of internal policy before FARA was enacted.[29] Nonetheless, FARA's express codification of NSA's and FBI's prior practice represents Congress's approval of the IC practice of installing oversight and privacy protection offices directly within the agencies that conduct foreign intelligence surveillance.

---

[23] *See generally id.*

[24] *Id.* § 101.

[25] *Id.* § 101(a)(1)(B)(f)(1) (2018).

[26] *Id.* § 109 (2018).

[27] Nat'l Sec. Agency, *Querying Procedures Used by the National Security Agency in Connection with Acquisitions of Foreign Intelligence Information Pursuant to Section 702 of the Foreign Intelligence Surveillance Act of 1978, As Amended*, 3 (Sept. 16, 2019), *available at*: https://www.intelligence.gov/assets/documents/702%20Documents/declassified/2019_702_Cert_NSA_Querying_17Sep19_OCR.pdf.

[28] FARA § 106.

[29] Office of the Dir. of Nat'l Intelligence,, *The FISA Amendments Reauthorization Act of 2017: Enhanced Privacy Safeguards for Personal Data Transfers Under Privacy Shield*, 3 (Oct. 15, 2018) *available at*: https://www.dni.gov/files/documents/icotr/Summary-FISA-Reauthorization-of-2017---10.15.18.pdf [*hereinafter* "DNI FARA Summary"].

iii. *Expansion of Whistleblower Protections*

FARA extended available whistleblower protections to contract employees working within US intelligence agencies.[30] Prior to FARA, "contractors were protected from agency management retaliation," but not from retaliation from the contractor's direct employer.[31] FARA thus extended whistleblower protections to prohibit retaliation against a whistleblowing IC contractor by the contractor's employer.[32] As a result, IC contractors can report deficiencies or violation to the inspectors general of US intelligence agencies and, as permitted by law, to the Senate and House intelligence committees.[33]

iv. *Increased Disclosure Requirements*

FARA introduced a number of new disclosure requirements for intelligence agencies. First, FARA requires future ODNI Statistical Transparency Reports agencies to separately state the number of US persons and non-US persons that were targets of electronic surveillance.[34] Second, FARA formally mandates that agencies' Section 702 minimization procedures be published.[35] Third, FARA requires the Attorney General to provide new reporting to Congress on the number of surveillance applications and emergency authorizations,[36] and to make each report publicly available and unclassified "to the extent consistent with national security."[37]

v. *Requirements for Resuming Abouts Collections*

Abouts collection was an aspect of the NSA's Upstream program. As discussed more fully in Section 2(d) below, following significant interaction with the FISC on the lawfulness of Abouts communication, the NSA voluntarily discontinued Abouts collections in March 2017. FARA now ensures that both the FISC and Congress must be informed before Abouts collection can be revived. If the NSA wishes to resume "intentional acquisition of [A]bouts communication," several requirements must be met.[38] First, FISC must issue a certification approving the program and "a summary of the protections in place to detect any material breach."[39] Second, the NSA must notify Congress in writing 30 days before resuming Abouts collection, and cannot begin Abouts collection within that thirty-day window.[40] The FISC's order approving the recommencement of Abouts

[30] FARA § 110.

[31] DNI FARA Summary, *supra* note 29.

[32] *See id.*

[33] *See* SWIRE, *supra* note 2 at 3-28 – 3-29.

[34] FARA § 102(b).

[35] *Id.* § 104 (2018). Although agencies' minimization procedures have already been declassified and published for each year in which the corresponding Section 702 reauthorization was published, this change may result in minimization procedures being published even when the underlying reauthorization is not.

[36] *Id.* § 107.

[37] *Id.*

[38] *Id.* § 103.

[39] *Id* § 103(b)(3).

[40] *Id.* § 103(b)(2).

collection must be attached to the notice provided to Congress.[41] Third, if Abouts collection resumes after having satisfied the prior two requirements, the NSA must report all material breaches to Congress.[42] Finally, any FISC opinion certifying the recommencement of Section 702 Abouts collection will be designated as a "novel or significant interpretation of the law," thus requiring appointment of an amicus curiae during authorization proceedings, as well as public release of the opinion.[43] The presence of these requirements within the amended Section 702 adds another level of oversight to the NSA's collection of Section 702 data.

b. FISC Continued to Evaluate 702 Compliance During Annual Reauthorizations

As stated above, FISC must annually review and reauthorize Section 702 programs. Since my prior testimony, FISC has reauthorized Section 702 programs on at least three occasions: in April 2017,[44] October 2018,[45] and December 2019.[46] For each of these reauthorizations, the US government declassified and published (a) the FISC order evaluating and reauthorizing Section 702 programs; and (b) the targeting, minimization, and (starting in 2018) querying procedures approved by the FISC to govern the conduct of Section 702 surveillance.[47] For the 2016 reauthorization, the government also declassified the ODNI/Attorney General certification and the NSA Director's affidavit submitted to FISC.[48]

The FISC reauthorization opinions show the FISC conducting the careful and detailed oversight over Section 702 surveillance I discussed in my 2016 Testimony.[49] FISC continued to examine how Section 702 programs "have been and will be implemented" in practice.[50] It also crafted new requirements for compliance with Section 702. As brief examples of FISC's review:

---

[41] *Id.* § 103(b)(3).

[42] *Id.* § 103(b)(5). Material breaches include "significant noncompliance with applicable law or an order of the FISC concerning any acquisition of abouts communication," *see id.* § 103(b)(1)(B). It can be presumed that other compliance incidents, whether material or not, would be reported to the FISC, as this is the FISC's current requirement for Section 702 programs.

[43] *Id.* § 103(b)(6); *see also* USA FREEDOM Act, Pub. L. 114-23, § 602(a) (2017).

[44] *See generally Mem. Op. & Order [Redacted]*, Case Caption [Redacted] (F.I.S.C. Apr. 26, 2017) *available at*: https://www.dni.gov/files/documents/icotr/51117/2016_Cert_FISC_Memo_Opin_Order_Apr_2017.pdf [*hereinafter* "FISC 2016/2017 Reauthorization"].

[45] *See generally Order [Redacted]*, Case Caption [Redacted] (F.I.S.C. Oct. 18, 2018) *available at*: https://www.intelligence.gov/assets/documents/702%20Documents/declassified/2018_Cert_FISC_Opin_18Oct18.pdf [*hereinafter* "FISC 2018 Reauthorization"].

[46] *See generally Mem. Op. & Order [Redacted]*, Case Caption [Redacted] (F.I.S.C. Dec. 6, 2019) *available at*: https://www.intelligence.gov/assets/documents/702%20Documents/declassified/2019_702_Cert_FISC_Opinion_06Dec19_OCR.pdf [*hereinafter* "FISC 2019 Reauthorization"].

[47] *See generally* FISC 2016/2017 Reauthorization, *supra* note 44; FISC 2018 Reauthorization, *supra* note 45; FISC 2019 Reauthorization, *supra* note 46.

[48] *See generally* FISC 2016/2017 Reauthorization, *supra* note 44.

[49] *See generally* SWIRE, *supra* note 2 at 5-1 – 5-53.

[50] *Mem. Op. & Order [Redacted]*, Case Caption [Redacted], 3 (F.I.S.C. Aug. 26, 2014), *available at* https://www.dni.gov/files/documents/0928/FISC%20Memorandum%20Opinion%20and%20Order%2026%20August%202014.pdf; *See also* SWIRE, *supra* note 2 at 5-12 – 5-14.

- The 2016 reauthorization opinion is 99 pages long.[51] The FISC evaluated the NSA's reports of compliance incidents relating to Abouts collection, and the NSA's decision to terminate Abouts collection in response (discussed immediately below). Further, the FISC evaluated the NCTC receiving access to Section 702 information, NSA data deletion questions, and potential issues relating to NSA's Upstream program that had occurred in the past year. The FISC also evaluated the NSA's use of automated tools for tasking decisions; determined that reliance on these tools was not sufficient to task a selector; and required the NSA to begin reporting incidents where the NSA did not conduct post-tasking review of acquired communications to determine whether a tasking decision has been proper.

- The 2018 reauthorization opinion is 138 pages long.[52] In its most lengthy discussion, the FISC found FBI querying practices involving US person identities were inconsistent with the Fourth Amendment; this finding was appealed to the FISA Court of Review, which affirmed the FISC,[53] resulting in the FBI modifying its minimization and querying procedures.[54] Additionally, in a novel and significant decision, the FISC held that FARA restrictions on Abouts collection also applied to certain non-Abouts collection. Although the precise collection technique at issue remained redacted, FISC ordered the NSA to report each time it tasked a selector using this technique within 10 days to FISC, presumably to monitor on an ongoing basis that NSA's acquisitions complied with the restrictions of FARA.[55] For this decision, the FISC invited and received amicus briefing.

- The 2019 reauthorization opinion is 83 pages long.[56] It addressed questions about whether the NSA may share information with FBI for targeting purposes, as well as the retention period for Upstream collection after termination of Abouts collection. Additionally, FISC addressed whether 702-acquired information could be captured by intelligence agencies' "user-activity monitoring" (AUM) activities, such as insider threat protection. The FISC preliminarily

---

[51] *See* FISC 2016/2017 Reauthorization, *supra* note 44; Due to extensions granted to review Abouts collection which extended reauthorization proceedings, the 2016 reauthorization appears to have covered Section 702 surveillance in both the years 2016 and 2017. The Attorney General and ODNI filed certifications to reauthorize Section 702 surveillance on September 26, 2016. *See also Government's Ex Parte Submission of Reauthorization Certifications and Related Procedures, Ex Parte Submission of Amended Certifications, and Request for an Order Approving Such Certifications and Amended Certifications [Redacted]*, (F.I.S.C. Sept. 26, 2016) *available at:* https://www.dni.gov/files/documents/icotr/51117/2016_Certification_Cover_Filing_Sep_26_2016_part_1_and_2_-merged.pdf. In evaluating Abouts collection issues, FISC granted extensions into March 2017, at which point NSA announced it was terminating Abouts collection. FISC then issued its reauthorization order on April 26, 2017. This reauthorization thus appears to have authorized Section 702 programs for 2016 and 2017.

[52] *See* FISC 2018 Reauthorization, *supra* note 45.

[53] *See In Re: DNI/AG 702(h) Certifications 2018 [Redacted]*, Dkt. No. [Redacted] (F.I.S.A. Ct. Rev. July 12, 2019) *available at*: https://www.intelligence.gov/assets/documents/702%20Documents/declassified/2018_Cert_FISCR_Opinion_12Jul19.pdf.

[54] *See Mem. Op. & Order [Redacted]*, Case No. [Redacted] (F.I.S.C. Sept. 4, 2019) *available at*: https://www.intelligence.gov/assets/documents/702%20Documents/declassified/2018_Cert_FISC_Opinion_04Sep19.pdf

[55] *See* FISC 2018 Reauthorization, *supra* note 45 at 136-138.

[56] *See* FISC 2019 Reauthorization, *supra* note 46.

approved AUM activities, but required all agencies to provide further reporting on the extent of their AUM activities and the amount of 702-acquired information affected by it.

c. NSA Terminated Upstream's Abouts Collection in Connection with FISC's 2017 Section 702 Reauthorization

The NSA's termination of Abouts collection represents a significant development that has occurred since my 2016 Testimony and illustrates the effectiveness of the US system of safeguards for foreign intelligence surveillance. Abouts collection referred to an aspect of the NSA's Section 702 Upstream program. It acquired communications that were not to or from a tasked selector, but which instead mentioned the selector (and were thus described as being "about" that selector). An example would be the NSA receiving an email where the selector email address of the target is included in the body or text of the email, but neither sent nor received that email.[57]

Abouts collection first came to FISC's attention in 2011, when it raised concerns due to acquisition of Multi-Communication Transactions (MCTs).[58] Emails and similar communications are often not transmitted through the Internet as discrete communications, but instead as part of MCT clusters,[59] what is often called a "thread" of emails. This resulted in Upstream acquiring not just communications containing a tasked selector, but also a further cluster of attached communications in which the selector did not appear.[60] For Abouts communication, FISC found this raised heightened privacy concerns, since it resulted in the NSA acquiring communications that did not contain selectors.[61] FISC thus imposed a number of restrictions on Abouts collection, such as requiring the NSA to segregate Abouts collection from other 702-acquired data, to restrict other agencies' access to Upstream collection, to restrict NSA analysts' use of Upstream-collected data, and to purge Upstream collection on a more expedited basis than other 702-acquired information.[62] These restrictions were memorialized in NSA's Section 702 minimization beginning in 2011.[63]

It appears that in 2016, NSA's Inspector General reviewed NSA's querying of Upstream collections and identified "significant noncompliance" with the FISC's restrictions.[64] This was reported to FISC, which held a hearing and required the government to submit a report on the full extent of querying practices affecting Upstream data as well as a remediation plan.[65] The government provided several rounds of updates to the FISC; however, the FISC on several occasions

---

[57] Nat'l Sec. Agency, *NSA Stops Certain 702 "Upstream" Activities*, PA-014-18, (Apr. 28, 2017), *available at*: https://www.nsa.gov/news-features/press-room/Article/1618699/nsa-stops-certain-section-702-upstream-activities/.

[58] *See generally* SWIRE, *supra* note 2 at 5-31 – 5-34.

[59] *See Id.*

[60] *See Id.*

[61] *See Id.*

[62] *See Mem. Op. [Redacted]*, Case No. [Redacted] (F.I.S.C. Oct. 3, 2011) *available at*: https://www.dni.gov/files/documents/0716/October-2011-Bates-Opinion-and%20Order-20140716.pdf

[63] *See Mem. Op. [Redacted]*, Case No. [Redacted] (F.I.S.C. Nov. 30, 2011) *available at*: http://www.fas.org/irp/agency/doj/fisa/fisc1111.pdf

[64] FISC 2016/2017 Reauthorization, *supra* note 44 at 4.

[65] *See id.*

expressed dissatisfaction with the state of the government's investigation into how querying practices were not complying with existing FISC orders.[66]

Ultimately, on March 30, 2017, the NSA reported to FISC that it would "eliminate 'abouts' collection altogether."[67] In addition, NSA stated it would "sequester and destroy raw Upstream Internet data previously collected," and "destroy such sequestered Internet transactions as soon as practicable through an accelerated age-off process."[68] Going forward, NSA stated that any communications obtained by Upstream "that are not to or from a person targeted in accordance with NSA's section 702 targeting procedures … will be destroyed upon recognition," and that NSA "will report any acquisition of such communications to [FISC] as an incident of non-compliance."[69] The NSA proffered updated minimization procedures to the FISC that memorialized these changes to Upstream.[70]

The FISC accepted the NSA's updated minimization procedures that prohibited Abouts collection.[71] Further, as described above, FARA now requires the NSA to obtain FISC authorization, and provide notification to Congress, prior to recommencing Abouts communication.[72] The NSA also publicly announced its termination of Abouts collection.[73]

The termination of Abouts communication underscores the effectiveness of the US system of safeguards for foreign intelligence. The FISC recognized privacy risks in Abouts collection and imposed heightened requirements on the NSA. Those requirements could not be met, in part due to technical challenges . Internal reviews identified the noncompliance; and it was reported to FISC. FISC insisted on compliance with its privacy restrictions, and the NSA determined this required Abouts collection to end.

d. Statistics on 702 Programs Continue to be Released by the US Government

ODNI publishes annual Statistical Transparency Reports that identify the number of non-US persons who are the targets of tasked selectors under Section 702.[74] My 2016 Testimony referenced that in 2015, there had been 94,368 targets of Section 702 programs.[75] Since then, the

[66] *See id.* at 4-6.
[67] *Id.* at 6.
[68] *Id.* at 23-24.
[69] *Id.*
[70] *Id.* at 26.
[71] *See id.*
[72] FARA § 103.
[73] Nat'l Sec. Agency, *NSA Stops Certain 702 "Upstream" Activities*, PA-014-18 (Apr. 28, 2017), *available at*: https://www.nsa.gov/news-features/press-room/Article/1618699/nsa-stops-certain-section-702-upstream-activities/)
[74] *See* 50 U.S.C. § 1873(b)(2)(A); SWIRE, *supra* note 2 at 3-36 – 3-37.
[75] *See* SWIRE, *supra* note 2 at 3-21 – 3-24.

Statistical Transparency Reports have provided targeting statistics for subsequent years.[76] The following table provides statistics for targeting of non-US persons under Section 702 since 2016:[77]

Calendar Year	2016	2017	2018	2019
Estimated Number of Section 702 Targets for Non-US Persons	106,469	129,080	164,770	204,968

I add one comment relevant to current discussions about possible changes in US surveillance practices after *Schrems II*. One proposal I have heard would be to end the Section 702 program and have each selector be subject to the one-at-a-time prior approval by a judge under Title I of FISA, the sort of approval that applies to individuals in the US where there is probable cause that they are "agents of a foreign power."[78] There are currently 11 federal district judges on the FISC; processing over 100,000 individual orders per year would simply not be possible with anything like current staffing with the care and attention to each application that DOJ documents and a judge assesses. As discussed in my 2016 Testimony, Section 702 was created in 2008 as an increase in legal process compared to prior collection done outside of the US.[79] Adding one-at-a-time prior approval by a judge for each selector would thus appear to be a greater change to current practice than some may have realized. That is not a conclusion about what changes the US might contemplate in discussions with the EU, but instead an observation about the nature of the current 702 program.

e. The US Government Continued to Publish Semiannual Assessments of Compliance for 702 Programs

Section 702 requires the AG and ODNI to jointly assess intelligence agencies' compliance with FISA Section 702 and publish their assessment semiannually in a declassified report (the "Semiannual Assessments").[80] The AG (through its National Security Division) and ODNI conduct regular on-site reviews of NSA, FBI, and CIA on at least a bimonthly basis, and they review agencies' targeting and minimization decisions.[81] Using the results of these reviews, the Semiannual

[76] *See generally* Office of the Dir. of Nat'l Intelligence, *Statistical Transparency Report: Regarding the use of National Security Authorities for Calendar Year 2016* (Apr. 2017) *available at*: https://www.dni.gov/files/icotr/ic_transparecy_report_cy2016_5_2_17.pdf; *See generally* Office of the Dir. of Nat'l Intelligence, *Statistical Transparency Report: Regarding the use of National Security Authorities for Calendar Year 2017* (Apr. 2018) *available at*: https://www.dni.gov/files/documents/icotr/2018-ASTR----CY2017----FINAL-for-Release-5.4.18.pdf; *See generally* Office of the Dir. of Nat'l Intelligence, *Statistical Transparency Report: Regarding the use of National Security Authorities for Calendar Year 2018*, (Apr. 2019) *available at*: https://www.dni.gov/files/CLPT/documents/2019_ASTR_for_CY2018.pdf; *See generally* Office of the Dir. of Nat'l Intelligence, *Statistical Transparency Report: Regarding the use of National Security Authorities for Calendar Year 2019* (Apr. 2020) *available at*: https://www.dni.gov/files/CLPT/documents/2020_ASTR_for_CY2019_FINAL.pdf.

[77] Office of the Dir. of Nat'l Intelligence, *Statistical Transparency Report: Regarding the use of National Security Authorities for Calendar Year 2019*, 14 (Apr. 2020) *available at*: https://www.dni.gov/files/CLPT/documents/2020_ASTR_for_CY2019_FINAL.pdf [*hereinafter* "2019 Statistical Transparency Report"].

[78] 50 U.S.C. § 1801(b).

[79] *See* SWIRE, *supra* note 2 at 3-18 – 3-19.

[80] 50 U.S.C. § 1881(a)(l)(1).

[81] *See* SWIRE, *supra* note 2 at 5-20 – 5-23.

Assessments describe types, percentages, and trends of 702 non-compliance issues. The table below summarizes the overall compliance rates, as well as compliance rates for each category of non-compliance, from December 2014 to November 2017. Note that Semiannual Assessments are published on a lag, meaning that although the statistics below date back to 2014, all of the below statistics have been published since the 2016 period in which my prior Testimony and Privacy Shield were finalized.

Intelligence Agencies Compliance Statistics	Report 14 (Dec. 2014 - May 2015)[82]	Report 15 (June 2015 - Nov. 2015)[83]	Report 16 (Dec. 2015 - May 2016)[84]	Report 17 (June 2016 - Nov. 2016)[85]	Report 18 (Dec. 2016 - May 2017)[86]	Report 19 (June 2017 to Nov. 2017)[87]
Overall Non-Compliance Rate	0.35%	0.53%	0.45%	0.88%	0.37%	0.42%
Tasking Non-Compliance Rate	42.3%	58.%	50.8%	35.3%	24.9%	28.7%
Detasking Non-Compliance Rate	24.3%	21.5%	13.7%	5.9%	7.5%	7.3%
Notification Non-Compliance Rate	8.7%	5.2%	6.4%	6.8%	11.2%	22.1%
Documentation Non-Compliance Rate	4.9%	2.2%	12.9%	7.5%	14%	23.6%
Minimization Non-Compliance Rate	14.8%	9.9%	14.3%	42.5%	39.1%	17.3%

[82] Dir. of Nat'l Intelligence & US Att'y Gen., *Semiannual Assessment of Compliance with Procedures and Guidelines Issued Pursuant to Section 702 of the Foreign Intelligence Surveillance Act*, 26-30 (Feb. 2016), available at here: https://www.dni.gov/files/documents/icotr/14th-Joint-Assessment-Feb2016-FINAL-REDACTED.pdf

[83] Dir. of Nat'l Intelligence & US Att'y Gen., *Semiannual Assessment of Compliance with Procedures and Guidelines Issued Pursuant to Section 702 of the Foreign Intelligence Surveillance Act*, 27-31 (Nov. 2016), found here: https://www.dni.gov/files/documents/icotr/15th-702Joint-Assessment-Nov2016-FINAL-REDACTED1517.pdf

[84] Dir. of Nat'l Intelligence & US Att'y Gen., *Semiannual Assessment of Compliance with Procedures and Guidelines Issued Pursuant to Section 702 of the Foreign Intelligence Surveillance Act*, 27-31 (Aug. 2017), found here: https://www.dni.gov/files/icotr/16th_Joint_Assessment_Aug_2017_10.16.18.pdf

[85] Dir. of Nat'l Intelligence & US Att'y Gen., *Semiannual Assessment of Compliance with Procedures and Guidelines Issued Pursuant to Section 702 of the Foreign Intelligence Surveillance Act*, 26-30 (Dec. 2017), found here: https://www.dni.gov/files/icotr/17th_Joint_Assessment_Dec_2017_10.16.18.pdf

[86] Dir. of Nat'l Intelligence & US Att'y Gen., *Semiannual Assessment of Compliance with Procedures and Guidelines Issued Pursuant to Section 702 of the Foreign Intelligence Surveillance Act*, 28-32 (Oct. 2018); found here: https://www.dni.gov/files/icotr/18th_Joint_Assessment.pdf [*hereinafter* "Semiannual Report 18"].

[87] Dir. of Nat'l Intelligence & US Att'y Gen., *Semiannual Assessment of Compliance with Procedures and Guidelines Issued Pursuant to Section 702 of the Foreign Intelligence Surveillance Act*, 30-36 (Dec. 2019)., found here: https://www.intelligence.gov/assets/documents/702%20Documents/declassified/19th%20Joint%20Assessment%20for%20702%20Dec%202019%20-%20Final%20for%20release%20(002)OCR.pdf [*hereinafter* "Semiannual Report 19"].

Intelligence Agencies Compliance Statistics	Report 14 (Dec. 2014 - May 2015)[82]	Report 15 (June 2015 - Nov. 2015)[83]	Report 16 (Dec. 2015 - May 2016)[84]	Report 17 (June 2016 - Nov. 2016)[85]	Report 18 (Dec. 2016 - May 2017)[86]	Report 19 (June 2017 to Nov. 2017)[87]
Miscellaneous/Other Non-Compliance Rate	4.9%	2.5%	2%	1.9%	0.9%	0.7%
Overcollection Non-Compliance Rate	Not reported	Not reported	Not reported	0.1%	Not reported	0.3%

Overall, AG/ODNI concluded in each Semiannual Assessment that "the agencies have continued to implement [targeting and minimization] procedures and follow [applicable] guidelines in a manner that reflects a focused and concerted effort by agency personnel to comply with the requirements of Section 702."[88] Only two incidents of intentional non-compliance were identified in the six Semiannual Assessments that have been published since my 2016 Testimony, each of which was remedied.[89] The Semiannual Assessments enable transparency into the conduct of foreign intelligence surveillance that, to the best of my knowledge, remains unique among leading nations.

f. NSA Declassified its Internal Training Manuals for 702 Programs

Since my 2016 Testimony, NSA has released internal guidance and training documents related to Section 702.[90] The documents show the multi-level training NSA provides to personnel on Section 702 compliance. They include trainings NSA provides to analysts who task selectors to be used in Section 702 surveillance, detailing the process through which NSA analysts must document their rationale for targeting a selector and submit it to an NSA "Adjudicator" for review.[91] The documents also include trainings provided to Adjudicators on reviewing analyst requests to task

[88] This conclusion is from the October 2018 Semiannual Assessment, but is representative of the conclusion of prior Semiannual Assessments. *See, e.g.*, Semiannual Report 18, *supra* note 86 at 48, ("[T]he agencies continued to implement the procedures and follow the guidelines in a manner that reflects a focused and concerted effort by agency personnel to comply with the requirements of Section 702.").

[89] In Semiannual Report 19, there were two issues of intentional non-compliance. The first issue involved FBI running batch queries under proposed, but unapproved, query procedures. These query procedures were eventually approved, but this incident still counted as intentional non-compliance. The second issue involved traditional intentional non-compliance where an FBI analyst queried his name and the name of his co-worker in the FBI database. This analyst was fired, and his security clearance was terminated. *See* Semiannual Report 19, *supra* note 87.

[90] *See* Office of the Dir. of Nat'l Intelligence, *IC on the Record: IC on the Record Guide to Posted Documents*, ICONTHERECORD.TUMBLR.COM, (Oct. 2020), *available at*: https://www.intel.gov/ic-on-the-record/guide-to-posted-documents.

[91] *See* Nat'l Sec. Agency, *Updated FAA 702 Targeting Review Guidance [Redacted]*, (May 15, 2017), *available at*: https://www.dni.gov/files/icotr/ACLU%2016-CV-8936%20(RMB)%20000911-001000%20-%20Doc%2010.%20NSA%E2%80%99s%20702%20Targeting%20Review%20Guidance.pdf; NSA's Practical Applications Training. *See also* Nat'l Sec. Agency, *CRSK1304: FAA Section 702 Practical Applications [Redacted]*; https://www.dni.gov/files/icotr/ACLU%2016-CV-8936%20(RMB)%20000911-001000%20-%20Doc%2011.%20NSA%E2%80%99s%20702%20Practical%20Applications%20Training.pdf

specific selectors, and the checklists used in selector evaluations.[92] Finally, NSA published a comprehensive Section 702 training covering aspects of NSA personnel's compliance duties relating to collecting, processing, analysis, retention, and dissemination of 702-acquired information, as well as obligations to immediately report compliance incidents.[93]

As one comment on possible reforms that may address EU legal concerns, the US government might consider codifying training requirements and other aspects of compliance. Such codification might be done through either statutory or non-statutory means, to address European legal concerns that Section 702 and other safeguards be "required by law."

3. Updates to the Former 215 Program.

In my 2016 Testimony, I discussed "[p]erhaps the most dramatic change in US surveillance law" since the Snowden disclosures: The termination of a bulk telephone record collection program that had been operated under Section 215 of the USA PATRIOT Act, and its replacement with a targeted call records program.[94] This change began when President Obama's Review Group, in which I participated, reviewed the 215 program and found it "not essential to preventing attacks."[95] The USA FREEDOM Act was passed soon thereafter, and prohibited bulk collection under Section 215, as well as under pen register, trap-and-trace, and national security letter authorities. NSA terminated the bulk phone records program on November 29, 2015.[96]

The USA FREEDOM Act thus introduced a targeted telephone call detail records program (the "CDR Program") that operated as I described in my 2016 Testimony.[97] The government had to identify a specific selector that is reasonably suspected of being associated with terrorism (such as a phone number), and obtain a FISC order requiring a communications provider to produce records associated with that selector. The government could only obtain records that were no more than two "hops" from the identified selector.

Since my 2016 Testimony, the NSA voluntarily terminated the CDR Program due to compliance and data-integrity issues it did not believe could be resolved. This section briefly describes the significant events relating to the CDR Program: (a) the NSA's deletion of years' worth

---

[92] *See* Nat'l Sec. Agency, *FAA702 Adjudicator Training [Redacted]*, *available at*: https://www.dni.gov/files/icotr/ACLU%2016-CV-8936%20(RMB)%20000911-001000%20-%20Doc%2012.%20NSA%E2%80%99s%20702%20Training%20for%20NSA%20Adjudicators.pdf; Nat'l Sec. Agency, *FAA 702 Adjudication Checklist [Redacted]*, *available at*: https://www.dni.gov/files/icotr/ACLU%2016-CV-8936%20(RMB)%20001001-001049%20-%20Doc%2013.%20NSA%E2%80%99s%20702%20Adjudication%20Checklist.pdf

[93] *See* Nat'l Sec. Agency, *OVSC1203: FISA Amendments Act Section 702 [Redacted]*, *available at*: https://www.dni.gov/files/icotr/ACLU%2016-CV-8936%20(RMB)%20001001-001049%20-%20Doc%2017.%20NSA%E2%80%99s%20Training%20on%20FISA%20Amendments%20Act%20Section%20702.pdf

[94] SWIRE, *supra* note 2 at 3-16 – 3-18.

[95] *See id.*

[96] *See* Office of the Dir. of Nat'l Int., *ODNI Announces Transition to a New Telephone Metadata Program*, (Nov. 27, 2015), *available at*: https://www.dni.gov/index.php/newsroom/press-releases/press-releases-2015/item/1292-odni-announces-transition-to-new-telephone-metadata-program.

[97] *See* SWIRE, *supra* note 2 at 3-16 – 3-18.

of CDRs, followed by its decision to terminate the CDR Program, and (b) the PCLOB's ensuring report on the CDR Program. These NSA actions are another example of the oversight and correction mechanisms built into the US legal system governing foreign intelligence.

a. NSA Voluntarily Deleted 3 Years' Worth of USA FREEDOM Act CDRs, then Discontinued the CDR Program Altogether

The CDR Program was affected by a number of compliance issues that resulted in the NSA deciding to delete years' worth of CDR Program data, then to discontinue the program. Between 2016 and 2019, the NSA provided a number of notices to FISC detailing issues of non-compliance and data-integrity issues.[98] Generally, the non-compliance issues included information omitted from FISA applications, providers transmitting CDRs on expired orders, and training and access incidents involving NSA personnel.[99] The data-integrity issues generally involved the NSA receiving erroneous data from certain telecom providers.[100] NSA notified FISC of these incidents, and deleted CDRs associated with these incidents.

In a further incident, when a provider produced inaccurate data, NSA searched for "anomalous data from the other providers," and found data-accuracy issues distributed across providers.[101] Further discussions by the NSA with another provider confirmed it also provided inaccurate data.[102] Ultimately, NSA determined "the providers could not identify for NSA all the affected records, and NSA had no way to independently determine which records contained inaccurate information."[103]

In response, starting on May 23, 2018, the NSA began deleting all CDRs obtained since 2015.[104] As required under FISA, the NSA also notified the PCLOB, Department of Justice (DOJ), and Congressional Oversight committees of its decision.[105] In June 2018, NSA released a statement notifying the public that it had deleted all of its call records under the CDR program due to "technical

---

[98] *See* Privacy and Civil Liberties Oversight Bd., *Report on the Government's Use of the Call Detail Records Program Under the USA Freedom Act*, 20 (Feb. 2020), *available at*: https://documents.pclob.gov/prod/Documents/OversightReport/87c7e900-6162-4274-8f3a-d15e3ab9c2e4/PCLOB%20USA%20Freedom%20Act%20Report%20(Unclassified).pdf [*hereinafter* "PCLOB CDR Report"].

[99] *See id.* at 21.

[100] First, a telecom provider pushed "inaccurate first-hop numbers to the NSA," which the NSA's system could not detect. "Instead, [the system] requested second-hop records using the erroneous first-hop response." Subsequently, the provider fixed the issue and the NSA purged the CDRs containing inaccurate numbers. Second, a telecom provider pushed produced a number of CDRs with inaccurate data to the NSA. The NSA took immediate action to stop receipt of CDRs from the provider. The NSA also found there were four FISA applications that relied on the inaccurate information, which it quickly reported to the FISC. The NSA then deleted associated CDRs and "recalled one disseminated intelligence report generated based on inaccurate CDRs." *Id.* at 22.

[101] *Id.* at 23.

[102] *See id.*

[103] *Id.* at 24.

[104] *See* Nat'l Sec. Agency, *NSA Reports Data Deletion*, Release No: PA-010-18, (June 18, 2018), *available at*: https://www.nsa.gov/news-features/press-room/Article/1618691/nsa-reports-data-deletion/

[105] The DOJ subsequently notified FISC. *See id.*

irregularities in some data received from telecommunications service providers" that had resulted in the NSA having access to some CDRs that NSA was not authorized to receive.[106]

Shortly after, in early 2019, the NSA allowed its last FISC order authorizing CDR collection to expire, thus discontinuing the CDR Program under the USA FREEDOM Act.[107] This decision was based on a balancing of "the program's relative intelligence value, associated costs, and compliance and data-integrity concerns."[108] Accordingly, the number of CDRs collected by the NSA fell from over 434 million in 2018 to approximately 4.2 million in 2019.[109]

b. PCLOB Assessed the USA FREEDOM Act CDR Program

In February 2020, the PCLOB issued a report reviewing the CDR program under the USA Freedom Act (the "CDR Program Report").[110] Since the CDR program had been discontinued by the time the PCLOB's Report was issued, the PCLOB made no recommendations regarding the Act, but did issue five key findings. First, the Board found that the CDR program had been constitutional, and second, that the NSA's collection of two hops of CDR data on an ongoing basis was statutorily authorized.[111] Third, PCLOB found no agency abuse of the CDR Program prior to the NSA's decision to stop CDR collection, and, fourth, no evidence that the NSA received statutorily prohibited categories of information such as name, address, or financial information related to a selector. [112] Finally, the Board found the NSA did not use its authority granted under the USA Freedom Act to attempt to gather certain kinds of metadata (the specifics of which remain redacted).[113] More broadly, the PCLOB agreed with the NSA's decision to stop CDR collection.[114]

In March 2020, Congress reauthorized the USA FREEDOM Act, extending it through December 2023.[115] Thus, there is the possibility that NSA could revive the CDR Program in the future. However, to do so, the NSA would have to obtain FISC orders authorizing the collection of CDRs, and the FISC – as it does in other contexts – could impose safeguards on CDR collection based on the past experience of the now-discontinued CDR Program.

---

[106] PCLOB CDR Report, *supra* note 98 at 24.

[107] As a part of the discontinuation, the NSA deleted remaining data collected under the CDR Program, but not data "that had been used in disseminated intelligence reporting or data that was considered 'mission management related information.'" PCLOB CDR Report, *supra* note 98 at 24.

[108] PCLOB CDR Report, *supra* note 98 at 24.

[109] Semiannual Report 19 *supra* note 87 at 32.

[110] *See generally* PCLOB CDR Report, *supra* note 98.

[111] Some of the members of the Board did not join on the constitutional analysis provided in the report. *See id.* at 70-77.

[112] *See* PCLOB CDR Report, *supra* note 98 at 2.

[113] *See id.*

[114] *See* Privacy and Civil Liberties Bd., *Fact Sheet: Report on the NSA's Call Detail Records Program Under the USA Freedom Act*, 2, *available at*: https://documents.pclob.gov/prod/Documents/OversightReport/e37f0efb-c85d-4053-b4c1-4159ccbf100f/CDR%20Fact%20sheet%20FINAL.pdf

[115] *See* USA FREEDOM Reauthorization Act of 2020, H.R. 6172, 116th Congress (May 14, 2020), *available at*: https://www.congress.gov/bill/116th-congress/house-bill/6172/text

4. Updates to Oversight Safeguards.

My 2016 Testimony describes a comprehensive oversight system for foreign intelligence, including Senate and House intelligence committees, agency Inspectors General, Privacy and Civil Liberties offices in the agencies, and ongoing review by the independent Privacy and Civil Liberties Oversight Board.[116] The structure of these oversight safeguards remains unchanged since 2016. This section briefly discusses updates occurring within the existing oversight framework: (a) PCLOB issuing its PPD-28 report, and (b) activities by Inspectors General.

a. PCLOB Issued its PPD-28 Report

On October 16, 2018, PCLOB published its report on Presidential Policy Directive 28 (PPD-28) (the "PPD-28 Report").[117] To produce the Report, PCLOB reviewed the PPD-28 targeting procedures of the CIA, NSA, and FBI, reviewed ODNI reports on changes to signals intelligence under PPD-28,[118] took comments from the public and NGOs, and held classified briefings and discussions with IC elements. PCLOB found PPD-28 resulted in greater memorialization and/or formalization of privacy protections that had inhered in existing practices.[119] For example, prior to PPD-28, NSA had limited its uses of signals intelligence collected in bulk to the six permissible purposes listed in PPD-28 (such as espionage and threats to US armed forces); PPD-28 resulted in these limitations being memorialized and codified.[120] Additionally, PPD-28 resulted in extending protections previously reserved for US persons to all individuals regardless of nationality. For example, NSA and CIA used PPD-28 procedures to refocus on protecting "personal information of all individuals regardless of nationality."[121] Similarly, NSA, CIA, and FBI minimization procedures now require that "personal information of non-US persons shall only be retained if comparable information of US persons may be retained pursuant to" EO 12333.[122]

Based on its review, PCLOB issued four recommendations for PPD-28's implementation:

1) The National Security Council (NSC) and ODNI should issue criteria for determining which activities or types of data will be subject to PPD-28 requirements;

---

[116] *See* SWIRE, *supra* note 2 at 3-26 – 3-34.

[117] This report was issued on the basis of Section 5 PPD-28, which encouraged PCLOB to provide a report on any matters within PCLOB's mandate, such as the implementation of executive branch regulations or policies like PPD-28. *See* Privacy and Civil Liberties Bd., *Report to the President on the Implementation of Presidential Policy Directive 28: Signals Intelligence Activities*, (Oct. 16, 2018), *available at*: https://documents.pclob.gov/prod/Documents/OversightReport/16f31ea4-3536-43d6-ba51-b19f99c86589/PPD-28%20Report%20(for%20FOIA%20Release).pdf [*hereinafter* "PCLOB PPD-28 Report"].

[118] *See* Office of the Dir. of Nat'l Intelligence, *A Status Report on the Development and Implementation of Procedures Under Presidential Policy Directive 28*, (July 2014), *available at*: https://www.dni.gov/files/documents/1017/PPD-28_Status_Report_Oct_2014.pdf; *See also* Office of the Dir. of Nat'l Intelligence, *2016 Progress Report on Changes to Signals Intelligence Activities* (Jan. 22, 2016), *available at*: https://www.intelligence.gov/index.php/ic-on-the-record-database/results/12-odni-releases-2016-signals-intelligence-reform-progress-report.

[119] *See generally* PCLOB PPD-28 Report, *supra* note 117.

[120] *See id.* at 6.

[121] *Id.* at 6-7.

[122] *Id.* at 7-8.

2) IC elements should consider both the mission and privacy implications of applying PPD-28 to multi-sourced systems;
3) NSC and ODNI should ensure that any IC elements obtaining first-time access to unevaluated signals intelligence update their PPD-28 use, retention and dissemination practices, procedures, and trainings before receiving such data; and
4) To the extent consistent with the protection of classified information, IC elements should promptly update their public PPD-28 procedures to reflect any pertinent future changes in practices and policy.[123]

These recommendations were later reviewed by ODNI's Office of Civil Liberties, Privacy, and Transparency (CLPT) in an October 2018 report on the status of implementation of the PCLOB's PPD-28 Report.[124] The CLPT found that the agencies had already implemented all four of these recommendations to the extent possible to maintain national security.[125]

b. Inspectors General

My 2016 Testimony described federal inspectors general (IGs) as an oversight component that provides a well-staffed and significant safeguard to ensure that federal agencies comply with internal administrative privacy mandates, including exercising privacy watchdog responsibilities[126]. Since my 2016 Testimony, as is widely known, the Department of Justice Inspector General issued a report on traditional FISA warrants issued in connection with an FBI investigation into a US citizen associated with the Trump campaign;[127] however, this report was not related to Section 702 or surveillance targeting non-US persons. The IG for the ODNI has continued to issue semiannual reports relating to the IC as a whole.[128] The IGs for surveillance agencies have also issued semiannual reports to Congress,[129] and have published on an ongoing basis reports on various investigations relating to intelligence agency activities.[130]

---

[123] *See id*. at 12-18.

[124] *See* Office of the Dir. of Nat'l Intelligence, *Status of Implementation of PPD-28: Response to the PCLOB's Report*, (Oct. 2018), *available at*: https://www.dni.gov/files/icotr/Status_of_PPD_28_Implementation_Response_to_PCLOB_Report_10_16_18.pdf [*hereinafter* "CLPT PPD-28 Implementation Report"].

[125] *See id*.

[126] *See* SWIRE, *supra* note 2 at 3-26 – 3-28.

[127] *See* Office of the Inspector Gen., *Review of Four FISA Applications and Other Aspects of the FBI's Crossfire Hurricane Investigation*, US Dept. of Justice, (Dec. 2019), *available at* https://www.justice.gov/storage/120919-examination.pdf

[128] *See* Office of the Dir. of Nat'l Intelligence, *ICIG Semiannual Report*, *available at*: https://www.dni.gov/index.php/who-we-are/organizations/icig/icig-publications/icig-all-reports

[129] *See, e.g.* Office of the Inspector Gen., *Semiannual Report to Congress*, National Security Agency, (Oct. 1, 2019 to Mar. 31, 2020), *available at*: https://oig.nsa.gov/Portals/71/Reports/SAR/OCT-MAR%202020%20OIG%20SAR.pdf?ver=2020-09-02-094002-550

[130] For a sample of reports from the NSA's Office of Inspector General, see, e.g., Office of the Inspector Gen. of the Nat'l Sec. Agency, OFFICE OF INSPECTOR GENERAL: REPORTS, *available at*: https://oig.nsa.gov/reports/.

5. Updates to Transparency Safeguards.

My 2016 Testimony discussed how, in the wake of the Snowden disclosures, the US government focused on increasing transparency measures relating to US surveillance, both for companies subject to orders and for government agencies that have requested orders.[131] The transparency safeguards I identified in 2016 have remained in place, and continue to provide valuable information about how foreign intelligence surveillance is conducted by US agencies. This section discusses transparency efforts since 2016: (a) additional releases of Statistical Transparency Reports, (b) continued corporate transparency reporting, (c) the creation of a second, text-searchable IC on the Record database, and (d) continued public release of declassified IC documents.

a. Additional Releases of Statistical Transparency Reports.

As discussed in Section 2(e) above, ODNI produces annual Statistical Transparency Reports that cover the IC's use of multiple types of intelligence.[132] Above, I discussed the numbers of Section 702 targets discussed in Statistical Transparency Reports. I note here that Statistical Transparency Reports go well beyond Section 702 and disclose statistics on the number of governmental requests made under other FISA foreign-intelligence authorities, including traditional individual FISA warrant authorities for electronic surveillance or physical searches, pen-register and trap-and-trace authorities, the "business records" authorities used to obtain Call Detail Records, and national security letter authorities. These reports also disclose the number of criminal proceedings in which a notice was provided that the government intended to use or disclose FISA-acquired information. The Statistical Transparency Report is also unique in that it explains the development of US surveillance programs, limitations placed on programs by FISC, and even instances of the NSA discontinuing programs – such as the 2020 Statistical Transparency Report describing the NSA's decision to suspend the CDR Program.[133]

b. Continued Corporate Transparency Reporting

My 2016 Testimony highlighted corporate transparency reporting as an important transparency safeguard that arose shortly after the Snowden disclosures.[134] Five leading US technology companies (Facebook, Google, LinkedIn, Microsoft, and Yahoo!) filed suit with the FISC to gain rights to provide transparency reporting, resulting in a DOJ policy change permitting

---

[131] *See* SWIRE, *supra* note 2 at 3-34 – 3-38.

[132] *See generally* Office of the Dir. of Nat'l Intelligence, *Statistical Transparency Report: Regarding the use of National Security Authorities for Calendar Year 2016*, (Apr. 2017) *available at*: https://www.dni.gov/files/icotr/ic_transparecy_report_cy2016_5_2_17.pdf; Office of the Dir. of Nat'l Intelligence, *Statistical Transparency Report: Regarding the use of National Security Authorities for Calendar Year 2017*, (Apr. 2018) *available at*: https://www.dni.gov/files/documents/icotr/2018-ASTR----CY2017----FINAL-for-Release-5.4.18.pdf; Office of the Dir. of Nat'l Intelligence, *Statistical Transparency Report: Regarding the use of National Security Authorities for Calendar Year 2018*, (Apr. 2019) *available at*: https://www.dni.gov/files/CLPT/documents/2019_ASTR_for_CY2018.pdf; Office of the Dir. of Nat'l Intelligence, *Statistical Transparency Report: Regarding the use of National Security Authorities for Calendar Year 2019*, (Apr. 2020) *available at*: https://www.dni.gov/files/CLPT/documents/2020_ASTR_for_CY2019_FINAL.pdf.

[133] *See* 2019 Statistical Transparency Report, *supra* note 77 at 29 - 30.

[134] *See* SWIRE, *supra* note 2 at 3-37 - 3-39.

reporting on ranges of governmental foreign intelligence requests. The USA FREEDOM Act codified the right of companies to issue transparency reports.

Since my 2016 Testimony, corporate transparency reporting has continued as permitted under the USA Freedom Act, with large companies regularly publishing reports on government access requests.[135] As in my 2016 Testimony, this Appendix examines the most recent transparency reports of Facebook and Google – the percentages of users whose records were accessed in the most recent six-month period is smaller than in 2016. In total, the number of customer accounts accessed by the US government for national security in the most recent time period is no more than (1) 118,997[136] for Facebook, out of approximately 2.5 billion[137] active users per month; and (2) approximately 109,497[138] for Google, out of approximately 1.17 billion[139] active users per month. The charts below, similar to the ones provided in my 2016 Testimony, reflect the current data above.

I make the following observation – these percentages are very, very small. Government surveillance requests are far from "pervasive" or "unlimited," as some have suggested.

Facebook	# of Users Accessed in 6 months	Accounts Specified	Percentage based on Users Per Month
Non-Content Requests	0-499	0-499	.0000002%
Content Requests	0-499	117,000-117,499	.000047%
National Security Letters	0-499	500-999	.0000004%

[135] *See id.*

[136] For the time period from July 2019 - December 2019, Facebook received the following: 0-499 non-content requests (affecting the same number of accounts); 0-499 content requests (affecting between 117,000 and 117,499 accounts); and 0-499 national security letters (affecting the same number of accounts). *See* FACEBOOK, *United States Law Enforcement Requests for Data*, GOVERNMENT REQUESTS REPORT (2020), https://govtrequests.facebook.com/country/United%20States/2015-H1.

[137] *See* STATISTA, *Number of Monthly Active Facebook Users Worldwide as of 4th Quarter 2019* (2020), https://www.statista.com/statistics/264810/number-of-monthly-active-facebook-users-worldwide/#:~:text=With%20over%202.7%20billion%20monthly,the%20biggest%20social%20network%20worldwide.

[138] For the time period from January 2019 - June 2019, Google received the following: 0-499 non-content requests (affecting the same number of accounts); 0-499 content requests (affecting between 107,000 and 107,499 accounts); and 500-999 national security letters (affecting between 1000 and 1499 accounts). *See* GOOGLE, *Transparency Report – United States* (2020), https://transparencyreport.google.com/user-data/us-national-security?hl=en.

[139] *See* Craig Smith, *365 Google Search Statistics and Much More (2020)*, EXPANDEDRAMBLINGS.COM (Nov. 30, 2020), http://expandedramblings.com/index.php/by-the-numbers-a-gigantic-list-of-google-stats-and-facts.

Google	# of Users Accessed in 6 months	Accounts Specified	Percentage based on Users Per Month
Non-Content Requests	0-499	0-499	.0000004%
Content Requests	0-499	107,000-107,499	.00009%
National Security Letters	0-499	1000-1499	.0000012%

c. The Government Has Launched New Transparency Websites

In 2013, the ODNI created "IC on the Record," a website on which ODNI posts declassified documents relating to United States foreign intelligence surveillance practices. In doing so, the US government became the first government in the world to maintain a running repository of declassified documents from its foreign intelligence agencies and oversight organs.[140] Since its appearance in 2013 and my 2016 Testimony, IC on the Record has accumulated a substantial amount of NSA internal records, FISC opinions, and other documents and records relating to foreign intelligence surveillance. The IC states that it has disclosed hundreds of documents comprising thousands of pages, including "hundreds of documents relating to Section 702."[141]

Further, since 2016, the publicly-available online channels through which the public has access to intelligence-related documents and court decisions has increased. For one, the FISC maintains an online "Public Filings" database containing a substantial number of its declassified opinions and orders, which has added usefulness in being searchable by docket number.[142] Second, ODNI has created "Intel.gov," a new repository on an official IC website that creates the capability to conduct full text searches on all documents posted on IC on the Record.[143] These resources make the transparency offered by the US government significantly more actionable for researchers, civil-rights organizations, and civil society in monitoring how foreign intelligence surveillance is being conducted.

6. Updates to Executive Safeguards

a. Presidential Policy Directive 28 (PPD-28)

My 2016 Testimony discussed Presidential Policy Directive 28 (PPD-28) as a significant new safeguard that creates an extensive system of privacy protection for signals intelligence activities involving non-US persons.[144] Since my prior testimony, PPD-28 has remained unchanged in substance. As discussed above, PPD-28 has resulted in intelligence agencies codifying PPD-28

[140] *See* SWIRE, *supra* note 2 at 3-36 - 3-37.

[141] Office of the Dir. of Nat'l Intelligence, *IC on the Record Guide to Posted Documents*, INTEL.GOV, (Oct. 2020), *available at*: https://www.intel.gov/ic-on-the-record/guide-to-posted-documents.

[142] *See* U.S. Foreign Intelligence Surveillance Ct., *Public Filings – US Foreign Intelligence Surveillance Court*, *available at*: https://www.fisc.uscourts.gov/public-filings. [*hereinafter* "FISC Public Filings Website"].

[143] *See* INTEL.GOV, *IC on the Record Database*, *available at*: https://www.intel.gov/ic-on-the-record/guide-to-posted-documents [*hereinafter* "Intel.gov"].

[144] *See* SWIRE, *supra* note 2 at 3-41 - 3-46.

protections into targeting and minimization procedures governing their conduct of signals intelligence. More significantly, PPD-28 remained in place during the transition between the Obama and Trump administrations.[145] The Biden administration is reportedly expected to continue or increase current protections under PPD-28.[146] This demonstrates significant continuity among US presidential administrations to maintain the United States' commitment to PPD-28 and the protections it offers to non-US persons.

b. Privacy Shield

My 2016 Testimony discussed Privacy Shield as a significant safeguard for the protection of data relating to EU citizens, since it introduced commitments from the US government to provide remedies to EU citizens, to act promptly and effectively to address EU data protection concerns, and to subject compliance to an ongoing review process.[147] After the *Schrems II* judgment, Secretary of Commerce Ross stated that the Department of Commerce would "continue to administer the Privacy Shield program," and that the ECJ decision "does not relieve participating organizations of their Privacy Shield obligations."[148] This indicated the US government continues to require Privacy Shield organizations to apply Privacy Shield protections to data received under the Shield until the data is deleted.

7. Updates to Foreign Intelligence Surveillance Court (FISC) Testimony.

Chapter 5 of my 2016 Testimony contained an evaluation of the significant number of FISC opinions that had been declassified following the Snowden disclosures, in a number of cases at the FISC's own order. My assessment reached four primary conclusions:

1. The newly declassified FISC materials support the conclusion that the FISC today provides independent and effective oversight over US government surveillance.
2. The FISC monitors compliance with its orders and has enforced with significant sanctions in cases of noncompliance.
3. In recent years, both the FISC on its own initiative and new legislation have greatly increased transparency.
4. The FISC now receives and will continue to benefit from briefing by parties other than the Department of Justice in important cases.

Since my prior testimony, additional FISC opinions have been published, but I am not aware of any reason to alter these conclusions. This section briefly describes updates that have occurred since 2016 and support the above conclusions: (a) FISC decisions continue to be declassified and

[145] *See* CLPT PPD-28 Implementation Report, *supra* note 124 at 4.

[146] *See* Kristen Bryan et. al., *Election 2020: Looking Forward to What a Biden Presidency May Mean for Data Privacy and Data Privacy Litigation*, NATIONAL LAW REVIEW, (Nov. 12, 2020), *available at*: https://www.natlawreview.com/article/election-2020-looking-forward-to-what-biden-presidency-may-mean-data-privacy-and

[147] *See* SWIRE, *supra* note 2 at 3-49.

[148] U.S. Dept. of Commerce, *US Secretary of Commerce Wilbur Ross Statement on Schrems II Ruling and the Importance of EU-US Data Flows* (July 16, 2020), *available at* https://www.commerce.gov/news/press-releases/2020/07/us-secretary-commerce-wilbur-ross-statement-schrems-ii-ruling-and.

published; (b) the FISC and FISA Court of Review have issued further decisions in ACLU litigation discussed in my prior Testimony; and (c) FISC transparency statistics continue to show FISC exercising considerable oversight over government surveillance applications.

a. New and Significant FISC Opinions Continue to be Declassified and Published

The transparency in regard to FISC opinions that I discussed in my 2016 Testimony has continued to the present. Opinions have been published under the USA FREEDOM Act's requirement to publish every FISC "decision, order, or opinion" that contains "a significant construction or interpretation of any provision of law" to the greatest practicable extent.[149] Others have been published in connection with litigation pursued by civil-rights organizations.[150] On the whole, a considerable quantity of FISC opinions have been published and can be accessed through IC on the Record,[151] the FISC's own "Public Filings" website,[152] and in text-searchable form on the Intel.gov repository.[153]

b. Updates to ACLU Litigation Discussed in Prior Testimony

My 2016 Testimony discussed litigation brought by the ACLU following the Snowden disclosures in which the ACLU requested that FISC publish its opinions authorizing the bulk telephone records program under Section 215.[154] The FISC found that the ACLU had Article III standing to seek publication of FISC opinions, and ordered the publication of certain Section 215 program authorizations. Since my 2016 Testimony, the FISA Court of Review confirmed that the ACLU and similar public-interest organizations have Article III standing to bring petitions for publication of FISC opinions.[155] However, in a subsequent decision, FISCR held that the FISC does not have subject-matter jurisdiction to hear challenges by public-interest organizations to the withholding of redacted, nonpublic materials in those opinions.[156]

---

[149] 50 U.S.C. § 1872.

[150] *See, e.g.*, IC ON THE RECORD, *Release of the FISC Opinion Approving the 2016 Section 702 Certifications and Other Related Documents* (May 11, 2017), available at: https://icontherecord.tumblr.com/post/160561655023/release-of-the-fisc-opinion-approving-the-2016 (listing "Other FISA Section 702 and Related Documents" produced in response to Freedom of Information Act litigation).

[151] *See* IC ON THE RECORD, *available at*: https://icontherecord.tumblr.com/.

[152] *See* FISC Public Filings Website., *supra* note 142.

[153] *See* Intel.gov, *supra* note 143.

[154] *See* SWIRE, *supra* note 2 at 5-39 – 5-41.

[155] *See In Re: Certification of Questions of Law to the Foreign Intelligence Surveillance Court of Review*, No. 18-01 (F.I.S.C. Mar. 16, 2018), https://www.fisc.uscourts.gov/sites/default/files/FISCR%2018-01%20Opinion%20March%2016%202018.pdf.

[156] *See In Re Op.s & Orders by the FISC Addressing Bulk Collection of Data Under the Foreign Intelligence Surveillance Act*, No. 18-02 (F.I.S.A. Ct. Rev. Mar. 24, 2020), *available at*: https://www.fisc.uscourts.gov/sites/default/files/FISCR%2020%2001%20Opinion%20200424.pdf.

c. FISC Transparency Statistics

My 2016 Testimony assessed a description of the FISC, in the wake of the Snowden disclosures that FISC acted as a "rubber stamp" for government surveillance requests.[157] The FISC itself had disputed this characterization, stating in a letter to the Senate that "24.4% of matters submitted ultimately involved substantive changes to the information provided by the government or to the authorities granted as a result of Court inquiry or action."[158] The USA FREEDOM Act permitted the Administrative Office of US Courts to issue new statistics on FISC practice that – unlike prior DOJ reporting – did not merely state the number of applications that FISC had denied in full, but rather accounted for all applications that FISC procedures significantly modified, denied in part, or denied in full.[159] This reporting enabled a more complete view of the extent to which FISC subjects government surveillance requests to scrutiny resulting in changes or denial. My 2016 Testimony evaluated the first of these new FISC reports and found that "the FISC either rejected or modified just over 17% of all surveillance applications it received in the latter half of 2015."[160]

Since 2016, the FISC has continued to publish its statistics on the number of applications and certifications for surveillance it modifies or denies.[161] These reports show the FISC modifying or denying a greater percentage of governmental surveillance requests than it did during my prior review. The following table summarizes the FISC statistics for each year since my 2016 Testimony:

Year	Total Number Applications Modified	Total Number of Applications Denied in Part	Total Number of Applications Denied	Sum of Applications Modified, Denied in Part, and Denied	Total Number of Applications and Certifications	Percentage of Applications Modified or Denied by FISC
2017[162]	391	50	26	**467**	**1,614**	**29%**
2018[163]	261	42	30	**333**	**1,318**	**25%**
2019[164]	234	38	20	**292**	**1,010**	**29%**

[157] SWIRE, *supra* note 2 at 5-9 – 5-18.

[158] Letter dated July 29, 2013 from Reggie B. Walton, FISC Chief Judge, to Patrick J. Leahy, Chairman of the US Senate Judiciary Committee 2, http://www.fisc.uscourts.gov/sites/default/files/Correspondence%20Grassley-1.pdf.

[159] *See* SWIRE, *supra* note 2 at 5-43 – 5-48.

[160] *Id.* at 5-14 – 5-17.

[161] *See* U.S. COURTS, *Director's Report on Foreign Intelligence Surveillance Courts' Activities, available at* https://www.uscourts.gov/statistics-reports/analysis-reports/directors-report-foreign-intelligence-surveillance-courts.

[162] Admin. Office of U.S. Cts., *Report of the Director of the Administrative Office of the U.S. Courts on Activities of the Foreign Intelligence Surveillance Courts for 2017*, 4, (Apr. 25, 2018), *available at* https://www.uscourts.gov/sites/default/files/ao_foreign_int_surveillance_court_annual_report_2017.pdf

[163] Admin. Office of U.S. Cts., *Report of the Director of the Administrative Office of the US Courts on Activities of the Foreign Intelligence Surveillance Courts for 2018*, 4, (Apr. 25, 2019), *available at* https://www.uscourts.gov/sites/default/files/fisc_annual_report_2018_0.pdf.

[164] Admin. Office of U.S. Cts., *Report of the Director of the Administrative Office of the US Courts on Activities of the Foreign Intelligence Surveillance Courts for 2019*, 4, (Apr. 27, 2020), *available at* https://www.uscourts.gov/sites/default/files/fisc_annual_report_2019_0.pdf.

8. Updates to Surveillance-Related Standing Cases

My 2016 Testimony briefly discussed the role that Article III standing may play in attempts to challenge surveillance programs before US courts.[165] This section briefly describes the state of select US cases seeking court review of surveillance programs.

a. Civil Challenges – The two primary attempts to file a civil challenge to Section 702 programs are both actively appealing dismissals on standing grounds.[166] In each case, the plaintiffs were granted discovery to prove they had standing and proffered either documents or experts as evidence. However, both suits were ultimately dismissed on standing ground because plaintiffs could not show a significant probability, or show evidence the government would authenticate, that the plaintiffs' communications had been affected by 702 programs or their predecessors. My understanding is that both proceedings are currently on appeal to a federal circuit court.

b. Challenges in Criminal Cases – In at least two criminal cases, defendants have asserted challenges to the constitutionality and lawfulness of Section 702 programs when 702-obtained evidence was proffered against them.[167] The challenges have been heard and adjudicated, in each instance with Section 702 programs being found lawful. In each instance, the defendant was a US person whose communications had been incidentally collected via 702 programs. In both cases, the lawfulness of incidentally acquiring communications of US persons via Section 702 programs was affirmed on at the appellate level.[168] In one case, following this appellate finding, the case was remanded to the district court to evaluate whether any querying of databases containing such incidentally-acquired Section 702 information by the government was constitutional.[169]

[165] *See* SWIRE, *supra* note 2 at 5-9 – 5-10. .

[166] *See Jewel v. NSA*, No. C 08-04373, 2019 U.S. Dist. LEXIS 217140 (N.D. Cal. 2019); *Wikimedia Found. v. NSA/Central Sec. Serv.*, 427 F. Supp. 3d 582 (D. Md. 2019).

[167] *See U.S. v. Hasbajrami*, 945 F.3d 641 (2d Cir. 2018); *U.S. v. Mohamud*, 843 F.3d 420 (9th Cir. 2016).

[168] *See U.S. v. Hasbajrami*, 945 F.3d 641 (2d Cir. 2018); *U.S. v. Mohamud*, 843 F.3d 420 (9th Cir. 2016).

[169] *See .S. v. Hasbajrami*, 945 F.3d 641 (2d Cir. 2018) (finding that incidental acquisition of US person communications through Section 702 is lawful, but remanding to district court to determine if querying of databases containing 702-acquired information by the government occurred and if so, whether it violated the defendant's constitutional rights).

Annex to Swire Testimony:
Acronyms used in this Appendix

ACLU	American Civil Liberties Union
AG	Attorney General
DNI	US Director of National Intelligence
DOD	US Department of Defense
DOJ	US Department of Justice
DOJ NSD	US Department of Justice, National Security Division
EU	European Union
FBI	US Federal Bureau of Investigation
FISA	Foreign Intelligence Surveillance Act
FISC	US Foreign Intelligence Surveillance Court
FISCR	US Foreign Intelligence Surveillance Court of Review
FTC	US Federal Trade Commission
IC	US Intelligence Community
IG	Inspector General
ISP	Internet Service Provider
MCT	Multiple Communication Transactions
NSA	US National Security Agency
NSD	National Security Division
NSL	National Security Letters
OCR	US Department of Health and Human Services Office for Civil Rights
ODNI	US Office of the Director of National Intelligence
OIG	US Office of the Inspector General
PCLOB	Privacy and Civil Liberties Oversight Board
PPD	Presidential Policy Directive
SIGINT	Signals Intelligence
US	United States of America
USA FREEDOM	Uniting and Strengthening America by Fulfilling Rights and Ending Eavesdropping, Dragnet-collection and Online Monitoring
USA PATRIOT	Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism