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A. The **European Data Protection Board** in November issued draft guidance with an extremely strict interpretation of how to implement the *Schrems II* case.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

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. <u>Passing comprehensive privacy legislation would help considerably in EU/U.S. negotiations.</u>

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.