UNITED STATES OF AMERICA
FEDERAL TRADE COMMISSION
WASHINGTON, D.C. 20580

Office of Commissioner
Noah Joshua Phillips

Written Statement of Noah Joshua Phillips[1]
Commissioner, Federal Trade Commission

Before the U.S. Senate Committee on Commerce, Science, and Transportation

Concerning
"The Invalidation of the EU-U.S. Privacy Shield and the Future of Transatlantic Data Flows"

Washington, D.C.
December 9, 2020

Chairman Wicker, Ranking Member Cantwell, Members of the Committee, thank you for the opportunity to testify before you today.

As the agency charged with enforcing the bulk of U.S. privacy law, the Federal Trade Commission supports cross-border data flows through law enforcement, cooperation with the Department of Commerce and other agencies in international engagement, and research and advocacy concerning privacy and data security law and policy. Specifically with respect to the EU-U.S. Privacy Shield Framework ("Privacy Shield") and its predecessor, we have brought over 60 enforcement actions against companies that have failed to live up to their commitments, participated in the Privacy Shield annual review process, and worked with counterpart independent data protection authorities on a host of issues.

A free and open Internet is vital to the national interest, but it is at risk. The impact on U.S. commerce and cross-border data flows from the "*Schrems II*" decision by the European Union Court of Justice ("ECJ"),[2] and the growth of other impediments to that commerce, deserve our serious and immediate attention. This Committee has engaged actively since the ECJ's decision was rendered in August, and today's hearing marks an important, bipartisan, continuation of that effort. With terrific work ongoing by this Administration—about which you will hear today—and a presidential transition underway, your leadership in drawing attention to this issue and your support for a path forward are essential.

My testimony will address the importance of cross-border data flows, the Federal Trade Commission's role in supporting them, the impediments they nonetheless face, and some suggestions on how to move forward.

[1] My comments today are my own and do not necessarily reflect the views of the Commission or my fellow Commissioners.

[2] Case C-311/18, *Data Prot. Comm'r v. Facebook Ireland & Maximillian Schrems*, ECLI:EU:C:2020:559 (July 16, 2020) ("*Schrems II*").

The Importance of Cross-Border Data Flows

Data help power the U.S. economy. From small startups to our largest technology companies, connected cars to contact tracing, American companies are competing and winning by offering consumers and clients products and services built on data. Our businesses employ data to develop new technologies like artificial intelligence and also to help meet longstanding needs, like education, worship, health, and office work, in novel ways. The COVID-19 crisis makes this abundantly clear.

Cross-border data flows are an essential component enabling all of this. Companies of all sizes rely on these data flows to innovate, reach new customers abroad, improve efficiency, enhance security, and reduce costs,[3] permitting the expansion and innovation that draws investment capital and creates jobs at home. That is particularly true for small companies, which cannot afford to, for example, establish offices or host data centers overseas. Cross-border data flows allow these companies to gain scale more rapidly and compete internationally at lower cost and with less risk. That is doubtless why 65% percent of companies participating in Privacy Shield are small and medium businesses.[4] A 2016 study found that almost two-thirds of worldwide startups surveyed had customers or users in other countries.[5] Take Etsy, the Brooklyn-based custom craft marketplace that offers small businesses a turnkey option to reach a global customer base. In 2019, cross-border transactions made up the largest component of the 36% of business attributable to Etsy's international business.[6] Or consider that PayPal—based in San Jose and serving many

[3] *See, e.g.*, Joshua P. Meltzer & Peter Lovelock, *Regulating for a Digital Economy: Understanding the Importance of Cross-border Data Flows in Asia* 6 (Brookings Inst. Global Econ. & Dev. Working Paper No. 113) (Mar. 20, 2018), https://www.brookings.edu/wp-content/uploads/2018/03/digital-economy_meltzer_lovelock_web.pdf (discussing access to new markets and capabilities of "digital inputs such as cloud computing [which] provides on-demand access to computing power and software that was previously reserved for large companies"); ICC Comm'n on Trade & Inv. Pol'y & ICC Comm'n on the Digit. Econ., Int'l Chamber of Com., *Trade in the Digital Economy: A Primer on Global Data Flows for Policymakers* 2 (2016), https://cdn.iccwbo.org/content/uploads/sites/3/2016/09/Trade-in-the-digital-economy-A-primer-on-global-data-flows-for-policymakers.pdf ("Access to digital products and services, such as cloud applications, provides SMEs with cutting edge services at competitive prices, enabling them to participate in global supply chains and directly access customers in foreign markets in ways previously only feasible for larger companies. Indeed, the Internet is a great equalizer, enabling small companies to compete globally using the same tools as large and established companies."); Bus. Roundtable, *Putting Data to Work: Maximizing the Value of Information in an Interconnected World* 6 (2015), https://s3.amazonaws.com/brt.org/archive/reports/BRT%20PuttingDataToWork.pdf (discussing how Caterpillar uses sensor data to allow it "and its customers to remotely monitor assets across their fleets in real time"); Demetrios Marantis, *Cross-border data flows power small business recovery*, Visa, Inc. (Nov. 9, 2020), https://usa.visa.com/visa-everywhere/blog/bdp/2020/11/09/cross-border-data-flows-1604955432332.html (noting that cross-border data flows are used to improve AI the provides fraud detection).

[4] Oliver Patel & Dr. Nathan Lea, UCL Eur. Inst, *EU-U.S. Privacy Shield, Brexit and the Future of Transatlantic Data Flows* 12 (May 2020), https://www.ucl.ac.uk/european-institute/sites/european-institute/files/privacy_shield_brexit_and_the_future_of_transatlantic_data_flows_1.pdf.

[5] James Manyika & Susan Lund, *Digital Protectionism and Barriers to International Data Flows*, Bretton Woods Comm. (Jun. 25, 2018), https://www.brettonwoods.org/article/digital-protectionism-and-barriers-to-international-data-flows.

[6] Etsy, Inc., Annual Report (Form 10-K) 66 (Feb. 27, 2020), https://d18rn0p25nwr6d.cloudfront.net/CIK-0001370637/d63aa848-ac0c-474c-9350-5b18888e84bf.pdf. International business includes all transactions "where either the billing address for the seller or the shipping address for the buyer at the time of sale is outside of the United States." *Id.*

smaller businesses—has processed over $400 billion in cross border payments since 2003.[7] The list goes on.

The impact of cross-border digital commerce numbers in the trillions of dollars, adding by some estimates hundreds of billions of dollars annually to U.S. GDP.[8] And there is every reason to believe that, if allowed to do so, those numbers will continue to grow. Cross-border data flows are a critical input to our technology sector, in which American companies lead the way. Of technology firms in the Fortune Global 500, the U.S. has 12, nearly double the number of Japan, the next on the list.[9] With our increasingly data-driven economy, cross-border data flows also drive innovation and growth in other sectors as well. At the end of the day, all of that means jobs for American workers and products for consumers.

Role of the FTC

The Federal Trade Commission plays an important role in supporting the promise of the free and open Internet, including cross-border data flows.

With respect to data privacy and security, we help ensure that companies communicate honestly with their customers about their privacy and security practices and refrain from unfair privacy or security practices.

Since the enactment of the Fair Credit Reporting Act ("FCRA") in 1970, [10] the FTC has served as the primary federal agency protecting consumer privacy. With the development of the Internet as a commercial medium in the 1990s, the Commission expanded its focus on privacy to reflect the growing collection, use, and sharing of consumer data in the commercial marketplace. The Commission's main source of legal authority in the privacy and data security space is Section 5 of the FTC Act, which prohibits deceptive or unfair commercial practices.[11] Under Section 5 and other statutes such as the Gramm-Leach-Bliley Act,[12] the Children's Online Privacy Protection Act,[13] and the FCRA, the FTC has aggressively pursued cases in children's privacy, financial

---

[7] Peggy Abkemeier, *Cross-Border Trade: PayPal's $400B Business*, PayPal Holdings, Inc. (Apr. 6, 2017), https://www.paypal.com/stories/us/cross-border-trade-paypals-400b-business.

[8] James Manyika et al., McKinsey & Co., *Digital Globalization: The New Era of Global Flows* 10 (Feb. 24, 2016), https://www.mckinsey.com/~/media/McKinsey/Business%20Functions/McKinsey%20Digital/Our%20Insights/Digital%20globalization%20The%20new%20era%20of%20global%20flows/MGI-Digital-globalization-Full-report.pdf (estimating impact on global GDP of $2.8 trillion in 2014); Gary Clyde Hufbauer & Zhiyao (Lucy) Lu, *Can Digital Flows Compensate for Lethargic Trade and Investment?*, Petersen Inst. for Int'l Econ. (Nov. 28, 2018), https://www.piie.com/blogs/trade-investment-policy-watch/can-digital-flows-compensate-lethargic-trade-and-investment (estimating impact on global GDP of over $3.5 trillion in 2020); U.S. Int'l Trade Comm'n, No. 4485, *Digital Trade in the U.S. and Global Economies, Part 2*, at 13 (Aug. 2014), https://www.usitc.gov/publications/332/pub4485.pdf (estimating 2011 impact on U.S. GDP of over $500 billion).

[9] *Fortune Global 500*, Fortune (2020), https://fortune.com/global500/.

[10] Fair Credit Reporting Act, 15 U.S.C. § 1681 *et seq.*

[11] 15 U.S.C. § 45.

[12] Gramm-Leach-Bliley Act, Pub. L. No. 106-102, 113 Stat. 1338 (1999) (codified as amended in scattered sections of 12 and 15 U.S.C.); Standards for Safeguarding Customer Information, 16 C.F.R. § 314.

[13] Children's Online Privacy Protection Act, 15 U.S.C. §§ 6501-6506; Children's Online Privacy Protection Rule, 16 C.F.R. § 312.

privacy, health privacy, the Internet of Things, and beyond. In total, we have brought hundreds of data security and privacy cases and we have hosted about 75 workshops and issued approximately 50 reports in the privacy and security area, on topics from data brokers[14] to portability.[15]

Our approach emphasizes addressing harms that have a tangible, substantial impact on consumers' well-being. This allows for both innovation and enforcement. There are scores of Data Protection Authorities in nations around the world, but no agency has engaged in more, or more significant, privacy and data security enforcement than the FTC. In just the few years of my tenure and those of my fellow commissioners, we have finalized settlements with Facebook[16] and Google/YouTube[17] that mandated both substantial monetary relief and significant improvements in privacy governance practices. In early 2019, we resolved a case against TikTok, long before the company was a matter of national conversation.[18] And, just a few weeks ago, we settled a case against Zoom, including allegations regarding representations the company made about the security of stored and transferred data.[19] In my view, by any reasonable metric, our enforcement program has had a greater impact than any other in the world.

The Commission has played an important role in Privacy Shield[20] and its predecessor, the U.S.-EU Safe Harbor Framework ("Safe Harbor").[21] Under the EU's General Data Protection Regulation ("GDPR") and its predecessors, companies are required to meet certain data protection requirements in order to transfer consumer data from the EU to other jurisdictions.[22] Privacy

---

[14] *See* FTC Report, *Data Brokers: A Call for Transparency and Accountability* (May 2014), https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf.

[15] *See* FTC Workshop, *Data To Go: An FTC Workshop on Data Portability* (Sept. 22, 2020), https://www.ftc.gov/news-events/events-calendar/data-go-ftc-workshop-data-portability.

[16] *See* FTC Press Release, *FTC Imposes $5 Billion Penalty and Sweeping New Privacy Restrictions on Facebook* (July 24, 2019), https://www.ftc.gov/news-events/press-releases/2019/07/ftc-imposes-5-billion-penalty-sweeping-new-privacy-restrictions.

[17] *See* FTC Press Release, *Google and YouTube Will Pay Record $170 Million for Alleged Violations of Children's Privacy Law* (Sept. 4, 2019), https://www.ftc.gov/news-events/press-releases/2019/09/google-youtube-will-pay-record-170-million-alleged-violations.

[18] *See* FTC Press Release, *Video Social Networking App Musical.ly Agrees to Settle FTC Allegations That it Violated Children's Privacy Law* (Feb. 27, 2019), https://www.ftc.gov/news-events/press-releases/2019/02/video-social-networking-app-musically-agrees-settle-ftc.

[19] *See* FTC Press Release, *FTC Requires Zoom to Enhance its Security Practices as Part of Settlement* (Nov. 9, 2020), https://www.ftc.gov/news-events/press-releases/2020/11/ftc-requires-zoom-enhance-its-security-practices-part-settlement.

[20] *See* FTC Business Guidance, *Privacy Shield* (2020), https://www.ftc.gov/tips-advice/business-center/privacy-and-security/privacy-shield. While I focus here on the U.S.-EU agreements, there was previously a U.S.-Swiss version of Safe Harbor that was replaced by a U.S.-Swiss version of Privacy Shield. The Swiss data protection authorities recently reached a similar decision as the court in *Schrems II*. Mark Smith, *ANALYSIS: Swiss-U.S. Privacy Shield Suffers from Schrems, Too*, Bloomberg L. (Sept. 10, 2020), https://news.bloomberglaw.com/bloomberg-law-analysis/analysis-swiss-u-s-privacy-shield-suffers-from-schrems-too.

[21] *See* FTC Business Guidance, *Federal Trade Commission Enforcement of the U.S.-EU and U.S.-Swiss Safe Harbor Frameworks* (2016), https://www.ftc.gov/tips-advice/business-center/guidance/federal-trade-commission-enforcement-us-eu-us-swiss-safe-harbor.

[22] Regulation (EU) 2016/679 of the European Parliament and of the Council, Art. 45, General Data Protection Regulation, 2016 O.J. (L 119) 1, 41.

Shield and Safe Harbor are voluntary mechanisms ensuring compliance with European requirements that have provided legal bases for companies to transfer data from Europe to the United States.[23]

The FTC can bring enforcement actions against companies that misrepresent their participation in or compliance with Privacy Shield. We have brought over 60 cases enforcing companies' commitments under Safe Harbor and Privacy Shield. We also fill a similar role with the APEC Cross-Border Privacy Rules system, designed to protect privacy and data flows in the Asia-Pacific region.[24]

Even though the court declared the Privacy Shield invalid, which I discuss below, the FTC continues to expect companies to comply with their ongoing obligations with respect to transfers made under Privacy Shield. If companies do not keep their promises, we will enforce the law against them. We also encourage companies to continue to follow robust privacy principles, such as those underlying Privacy Shield, and to review their privacy policies to ensure they describe their privacy practices accurately, including with regard to cross-border data transfers. The Commission remains committed to working with the Department of Commerce to help support the free flow of data across borders.

Schrems II

Notwithstanding these efforts, the privacy protections U.S. law provides U.S. citizens and non-citizens, and the tremendous work this Administration and the prior one have done with their counterparts on the European Commission (the Executive Branch of the EU), transatlantic data flows are threatened.

In 2016, the European Commission deemed Privacy Shield "adequate", thus permitting transfers to the U.S. under the framework.[25] In its recent ruling in *Schrems II*, the ECJ struck down Privacy Shield. The court expressed concerns about U.S. protections described in the European Commission's Privacy Shield Adequacy Decision, including the independence of the Ombudsman mechanism established in the U.S. Department of State and the perceived lack of redress for EU data subjects.[26] Additionally, the court required companies that rely on Standard Contractual Clauses ("SCCs") to assess the level of protection in the importing country for all of their transfers, raising questions about SCCs as a legal basis for transfers to the U.S.[27]

---

[23] Privacy Shield is not the only mechanism for transferring data to the U.S. from the EU. As discussed below, GDPR permits transfers made using Standard Contractual Clauses and Binding Corporate Rules.

[24] *See* FTC Press Release, *FTC Becomes First Enforcement Authority in APEC Cross-Border Privacy Rules System* (July 26, 2012), https://www.ftc.gov/news-events/press-releases/2012/07/ftc-becomes-first-enforcement-authority-apec-cross-border-privacy.

[25] Eur. Comm'n, *Commercial Sector: EU-US Privacy Shield*, https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/eu-us-data-transfers_en#:~:text=The%20adequacy%20decision%20on%20the,United%20States%20for%20commercial%20purposes.

[26] *Schrems II*, *supra* note 2, ¶¶ 186-198.

[27] *Schrems II*, *supra* note 2, ¶ 142. To be sure, it is the view of many, including the Commerce Department, that SCCs are still available, at least for some transfers. But even where SCCs may still be available, the complexity and risk of using them has increased. *See* Dep't of Com. et al., *Information on U.S. Privacy Safeguards Relevant to SCCs and Other EU Legal Bases for EU-U.S. Data Transfers after Schrems II* (Sept. 2020),

The *Schrems II* decision and recent recommendations from the European Data Protection Board,[28] the coordinating body of local data protection authorities under the GDPR, create substantial legal uncertainty and risk for cross-border data transfers. Those costs are borne disproportionately by small companies, which cannot afford the more expensive options, and for that reason constitute the bulk of companies that participate in Privacy Shield.

The court's decision concerned national security access to personal data, not consumer privacy in the sense that we enforce at the FTC. Meaning, what was at issue in *Schrems II* was not the absence of a GDPR-like national consumer privacy law in the U.S.

Looking at how the court considered U.S. national security access to personal data, three things strike me. *First*, U.S. law and practice incorporate civil liberty protections against government surveillance that are substantial, including statutes such as the Electronic Communications Privacy Act[29] and the Judicial Redress Act[30] and executive actions like Presidential Policy Directive 28.[31] *Second*, as researchers in the U.S. and Europe have found, U.S. law and practice are *at least* as protective of privacy as the domestic laws of many of our European allies.[32] The court, however, deemed European domestic laws irrelevant, focusing instead on what Professor Peter Swire has referred to as "an idealized, formal standard set forth primarily in EU constitutional law", rather than the national security laws and practices of members states.[33] *Finally*, as Adam Klein, Chairman of the Privacy and Civil Liberties Oversight Board recently noted, those allies regularly partner with the U.S. to assist in their collection of valuable intelligence data.[34]

Schrems II is not the only risk factor for cross-border data flows. Both before and since the decision, sometimes under the rubric of "data sovereignty", a number of prominent European

---

https://www.commerce.gov/sites/default/files/2020-09/SCCsWhitePaperFORMATTEDFINAL508COMPLIANT.PDF.

[28] Eur. Data Prot. Bd., *Recommendations 01/2020 on Measures That Supplement Transfer Tools to Ensure Compliance with the EU Level of Protection of Personal Data* (Nov. 10, 2020), https://edpb.europa.eu/sites/edpb/files/consultation/edpb_recommendations_202001_supplementarymeasurestransferstools_en.pdf.

[29] Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (codified as amended in scattered sections of 18 U.S.C.).

[30] Judicial Redress Act, 5 U.S.C. § 552a note.

[31] Presidential Policy Directive 28– Signals Intelligence Activities, 1 Pub. Papers 46 (Jan. 17, 2014), https://www.govinfo.gov/content/pkg/PPP-2014-book1/pdf/PPP-2014-book1-doc-pg46.pdf.

[32] *See, e.g.*, Jacques Bourgeois et al., Sidley Austin LLP, *Essentially Equivalent: A Comparison of the Legal Orders for Privacy and Data Protection in the European Union and United States*, at iv (Jan. 2016), https://www.sidley.com/-/media/publications/essentially-equivalent---final.pdf (arguing that "the US legal order for privacy and data protection embodies fundamental rights consistent with the Charter, principles of proportionality, and checks and balances in both form and substance, and that these protections of privacy and data protection rights are essentially equivalent to those in the EU").

[33] Kenneth Propp & Peter Swire, *Geopolitical Implications of the European Court's Schrems II Decision*, Lawfare (July 17, 2020), https://www.lawfareblog.com/geopolitical-implications-european-courts-schrems-ii-decision.

[34] Adam Klein, Chairman, Priv. & C.L. Oversight Bd., Statement on the Terrorist Finance Tracking Program (Nov. 19, 2020), https://documents.pclob.gov/prod/Documents/EventsAndPress/b8ce341a-71d5-4cdd-a101-219454bfa459/TFTP%20Chairman%20Statement%2011_19_20.pdf.

voices[35] have called for data localization requirements in Europe—that is, for all data about Europeans to be kept in Europe.

By no means are data localization concerns unique to Europe. By some estimates, localization efforts have grown fourfold since 2000, including many sector-specific rules requiring that certain data be processed or maintained in-country.[36] Countries that have, or are considering, localization requirements include India, Vietnam, Australia, and Turkey.[37]

Adopting data localization around the world poses a threat to U.S. commerce as well as the free and open Internet. To do business in multiple countries, companies will need servers, local staff, and so on. For smaller companies and startups, this may spell the end of cross-border commerce. The result will negatively impact not only American companies looking to grow but American consumers who benefit from products improved by cross-border data flows.

For larger firms that can add processing capacity overseas, there still are downsides. For instance, localization inhibits the global backup and redundancy that a distributed network allows, and the privacy and security that come with it.[38] Even something as uncontroversial as bug and error reporting from individual computers—which allows companies to analyze and correct software issues—may become a local function deprived of critical inputs. And research institutions will feel the impact, with cross-border collaboration in areas like medicine and computer science—where access to large and global data sets are essential—newly subject to digital boundaries.[39]

Data localization requirements are nothing new but historically have more often been associated with alternative visions of internet governance in countries like China and Russia. The hallmark of this alternative is state control: the opposite of a free and open Internet. China uses technical

---

[35] *See, e.g.*, Vincent Manancourt, *Europe's data grab*, Politico (Feb. 12, 2020), https://www.politico.eu/article/europe-data-grab-protection-privacy/; Thierry Breton, Comm'r, *Europe: The Keys To Sovereignty*, Eur. Comm'n (Sept. 11, 2020), https://ec.europa.eu/commission/commissioners/2019-2024/breton/announcements/europe-keys-sovereignty_en.

[36] Christian Ketels & Arindam Bhattacharya, *Global Trade Goes Digital*, Bos. Consulting Grp. (Aug. 12, 2019), https://www.bcg.com/publications/2019/global-trade-goes-digital; Jennifer Huddleston & Jacqueline Varas, *Impact of Data Localization Requirements on Commerce and Innovation*, Am. Action F. (June 16, 2020), https://www.americanactionforum.org/insight/impact-of-data-localization-requirements-on-commerce-and-innovation/#ixzz6YgQOlW4C ("The data covered by these laws can range from all personal data to only specific types of data such as health or financial information.").

[37] Pablo Urbiola et al., Inst. of Int'l Fin., *Data Flows Across Borders: Overcoming Data Localization Restrictions* 1, 2 (Mar. 2019), https://www.iif.com/Portals/0/Files/32370132_iif_data_flows_across_borders_march2019.pdf; David Meyer, *Here's Why PayPal Is About to Suspend Operations in Turkey*, Fortune (May 31, 2016), https://fortune.com/2016/05/31/paypal-turkey-suspension/.

[38] For example, data may be divided into shards, with any individual's data split up across multiple machines across the world. H Jacqueline Brehmer, *Data Localization: The Unintended Consequences of Privacy Litigation*, 67 Am. U. L. Rev. 927, 967-986 (2018), https://digitalcommons.wcl.american.edu/cgi/viewcontent.cgi?article=2009&context=aulr; Dillon Reisman, *Where Is Your Data, Really?: The Technical Case Against Data Localization*, Lawfare (May 22, 2017), https://www.lawfareblog.com/where-your-data-really-technical-case-against-data-localization.

[39] *See, e.g.*, PHG Found., *Impact of Schrems II on Genomic Data Sharing* (2020), https://www.phgfoundation.org/documents/schrems-ii-discussion-paper.pdf (noting how *Schrems II* impacts genomic research).

controls (its "great firewall") and legal controls to filter what is available to Chinese citizens.[40] There is active censorship at the national level, such that you can't type Winnie the Pooh—a reference used by critics of President Xi—into Weibo without it being deleted.[41] And, not surprisingly, China also requires that substantial amounts of data be stored on servers in China.[42] Data stored locally are accessible to the government upon request, and without due process.[43]

Russia also maintains strict data localization laws (though not always enforced);[44] allows for blacklisting of Internet sites;[45] and has experimented with creating, in effect, its own internet, with exclusively in-country routing, DNS, and the like.[46]

Let me stress that the liberal democracies of Europe are nothing like China and Russia, but impeding cross-border data flows and erecting unnecessary barriers—the "Splinternet", as Stanford Law Professor Mark Lemley refers to it in a recent article[47]—will reverberate. In many

---

[40] Elizabeth C. Economy, *The great firewall of China: Xi Jinping's internet shutdown*, Guardian (June 29, 2018), https://www.theguardian.com/news/2018/jun/29/the-great-firewall-of-china-xi-jinpings-internet-shutdown.

[41] Yuan Yang, *Winnie the Pooh blacklisted by China's online censors*, Fin. Times (July 16, 2017), https://www.ft.com/content/cf7fd22e-69d5-11e7-bfeb-33fe0c5b7eaa.

[42] Yuxi Wei, *Chinese Data Localization Law: Comprehensive but Ambiguous*, Henry M. Jackson Sch. of Int'l Stud., Univ. of Wash. (Feb. 7, 2018), https://jsis.washington.edu/news/chinese-data-localization-law-comprehensive-ambiguous/ (localization requirements in China are comprehensive but also confusing and ambiguous).

[43] Afef Abrougi, *Chinese law and state security requirements stunt companies' progress in 2019 RDR Index*, Ranking Digit. Rts. (July 17, 2019), https://rankingdigitalrights.org/2019/07/17/chinese-law-and-state-security-requirements-stunt-companies-progress-in-2019-rdr-index/ (Chinese law requires "to keep user activity logs and relevant data for six months and to hand it over to the authorities when requested without due process"); Martina F. Ferracane & Hosuk Lee-Makiyama, Eur. Ctr. For Int'l Pol. Econ., *China's Technology Protectionism and its Non-negotiable Rationales* 3 (June 2017), https://ecipe.org/wp-content/uploads/2017/06/DTE_China_TWP_REVIEWED.pdf ("[T]he State Security Law (passed in 1993) provides the state security organs with access to any information or data held by an entity in China whenever they deem it necessary. Without doubt, the scope of the State Security Law has grown exponentially in the digitalisation era."); Adrian Shahbaz, Freedom House, *The Rise of Digital Authoritarianism* (2018), https://freedomhouse.org/report/freedom-net/2018/rise-digital-authoritarianism ("China was once again the worst abuser of internet freedom in 2018.").

[44] Vera Shaftan, *Russian Data Localization law: now with monetary penalties*, Data Prot. Rep. (Dec. 20, 2019), https://www.dataprotectionreport.com/2019/12/russian-data-localization-law-now-with-monetary-penalties/#:~:text=By%20way%20of%20recap%2C%20in,using%20databases%20located%20in%20Russia ("[I]n 2015, Russia introduced a data localization law, requiring "data operators" to ensure that recording, systematisation, accumulation, storage, refinement and extraction of personal data of Russian citizens is done using databases located in Russia.").

[45] Freedom House, *Freedom on the Net 2019, Russia* (2019), https://freedomhouse.org/country/russia/freedom-net/2019 ("The government gives several state bodies—including Roskomnadzor, the Prosecutor General's Office, the Federal Service for Surveillance on Consumer Rights Protection and Human Wellbeing (Rospotrebnadzor), the Federal Drug Control Service, and, most recently, the Federal Agency for Youth Affairs—the authority to block various categories of online content.").

[46] Isabelle Khurshudyan, *Russia is bolstering its internet censorship powers – is it turning into China?*, Independent (Feb. 3, 2020), https://www.independent.co.uk/news/world/europe/russia-internet-censorship-norway-putin-a9306666.html (observing that a 2019 law "aims to route Russian web traffic and data through points controlled by state authorities and to build a national domain name system. This, supporters claim, would give Russia greater control of internet content and traffic.").

[47] Mark A. Lemley, *The Splinternet* (Stan. Law & Econ. Olin Working Paper No. 555, 2020), http://dx.doi.org/10.2139/ssrn.3664027. Professor Lemley is not the first to use this term.

parts of the world, including nations with which the U.S. does substantial commerce, which path to follow remains an open question. Liberal democracies should be uniting—not dividing—to light the better path.

Next Steps

All of this demonstrates the need to foster transatlantic data flows, and international ones more broadly.

First, we need to find a path forward after *Schrems II*, to permit transfers between the U.S. and EU. I want to recognize the efforts of U.S. and EU negotiators to find a replacement for Privacy Shield. While no doubt challenging, I have confidence in the good faith and commitment of public servants like Jim Sullivan, with whom I have the honor of appearing today, and our partners across the Atlantic. I have every hope and expectation that protecting cross-border data flows will be a priority for the incoming Administration, and I ask for your help in ensuring it is.

Second, we must actively engage with nations evaluating their approach to digital governance, something we at the FTC have done, to share and promote the benefits of a free and open Internet. There is an active conversation ongoing internationally, and at every opportunity—whether in public forums or via private assistance—we must ensure our voice and view is heard.

Third, we should be vocal in our defense of American values and policies. While we as Americans always look to improve our laws—and I commend the members of this committee on their important work on privacy legislation and other critical matters—we do not need to apologize to the world. When it comes to civil liberties or the enforcement of privacy laws, we are second to none. Indeed, in my view, the overall U.S. privacy framework—especially with the additional protections built into Privacy Shield—should certainly qualify as adequate under EU standards.

Fourth, as European leaders call to strengthen ties with the U.S., we should prioritize making our regimes compatible for the free flow of data. This extends to the data governance regimes of like-minded countries outside of Europe as well. Different nations will have different rules, but relatively minor differences need not impede mutually-beneficial commerce.[48] We need not and should not purport to aim for a single, identical system of data governance. And we should remind our allies, and remind ourselves, that far more unites liberal democracies than divides us.[49]

Fifth and finally, if we must draw lines, those lines should be drawn between allies with shared values—the U.S., Europe, Japan, Australia, and others—and those, like China and Russia, that offer a starkly different vision. I am certainly encouraged when I hear recognition of this distinction from Europe. European Data Protection Supervisor Wojciech Wiewiórowski recently noted that the U.S. is much closer to Europe than is China and that he has a preference for data

[48] *See, e.g.*, Remarks of Jennifer Daskal, *Debate: We Need to Protect Strong National Borders on The Internet*, 17 Colo. Tech. L.J., 13, 27 ("[T]he goal is to figure out a way to mediate, and manage, those differences, without yielding a fractured Internet.").

[49] For one model of how to bridge the divide, consider the CLOUD Act, which provides for U.S. law enforcement access to data stored overseas while recognizing and respecting the citizens and laws of the hosting country. *See, e.g.*, Alan Charles Raul, *Global Overview*, Privacy, Data Prot. and Cybersecurity L. Rev., 1, 2 (Alan Charles Raul ed., 2020), https://www.sidley.com/-/media/publications/the-privacy-data-protection-and-cybersecurity-law-review-2020-global-overview.pdf?la=en; Daskal, *supra* note 48, at 29.

being processed by countries that share values with Europe.[50] Some here in the U.S. are even proposing agreements to solidify the relationships among technologically advanced democracies, an idea worth exploring in more detail.[51]

However we proceed will require vision and leadership, and that is why I am so glad that this committee is prepared to engage thoughtfully with these challenges.

Again, thank you for inviting me today, and I look forward to your questions.

[50] Peter Swire, '*Schrems II' backs the European legal regime into a corner — How can it get out?*, IAPP (July 16, 2020), https://iapp.org/news/a/schrems-ii-backs-the-european-legal-regime-into-a-corner-how-can-it-get-out/.

[51] *See, e.g.*, Robert K. Knake, Council on Foreign Rels., *Weaponizing Digital Trade: Creating a Digital Trade Zone to Promote Online Freedom and Cybersecurity* (Sept. 2020), https://cdn.cfr.org/sites/default/files/report_pdf/weaponizing-digital-trade_csr_combined_final.pdf; Jared Cohen & Richard Fontaine, *Uniting the Techno-Democracies*, Foreign Affs., Nov.-Dec. 2020, https://www.foreignaffairs.com/articles/united-states/2020-10-13/uniting-techno-democracies (suggesting an informal group of technologically advanced states which would hold regular meetings).