Hearing on

"The Invalidation of the EU-US Privacy Shield and the Future of Transatlantic Data Flows"

Senate Committee on Commerce, Science, and Transportation

December 9, 2020, at 10:00 a.m.
Russell Senate Office Building
Room 253
Washington, DC

Testimony of Victoria A. Espinel
President and CEO
BSA | The Software Alliance

Testimony of Victoria A. Espinel
President and CEO, BSA | The Software Alliance
Hearing on "The Invalidation of the EU-US Privacy Shield and the Future of Transatlantic Data Flows"

Good morning Chairman Wicker, Ranking Member Cantwell, and members of the Committee. My name is Victoria A. Espinel. I am President and CEO of BSA | The Software Alliance ("BSA").

BSA is the leading advocate for the global software industry.[1] Our members are at the forefront of developing cutting-edge, data-driven services that have a significant impact on US job creation and growing the global economy. I commend the Committee for holding this hearing on the important topic of transatlantic data transfers and the EU-US Privacy Shield Framework ("Privacy Shield"), and I thank you for the opportunity to testify.

Cross-border data transfers are critical to the success of a broad range of companies, of all sizes and industries, and to consumers on both sides of the Atlantic. For that reason, the issues before this Committee reach far beyond the technology sector. Companies large and small, across the entire US economy, depend on services that send data across international borders.

BSA represents the perspective of enterprise software companies. Our members create the technology products and services that help other businesses innovate and grow. Businesses trust BSA members to maintain the privacy and security of their most sensitive data, including personal information. Those businesses – in sectors as diverse as agriculture, healthcare, manufacturing, and banking – produce a broad range of products and services and are united by the need to send data across international borders. Indeed, everyday technologies like cloud storage services, customer relationship management software, human resource management programs, identity management services, workplace collaboration software, and supply chain management services all depend on the ability to transfer data across national boundaries.

Transferring data across borders is not only vital to businesses, but also to consumers and workers. In our professional lives, we transfer data when we send emails to colleagues, manage staff and budgets, attend videoconferences, and in thousands of other routine business activities. In our personal lives, we transfer data across borders when we engage in e-commerce or use messaging platforms to stay in touch with friends and relatives overseas. In each of these scenarios, we rightly expect to use global services that can connect us with others worldwide – in a manner that protects the privacy and security of our data.

These issues are even more important amid the COVID-19 pandemic, as companies across the economy rely more heavily on remote workplace tools and cloud-based technologies that help employees remain productive while working outside of their physical offices. Online tools are also opening new avenues for medical researchers, hospitals, and pharmaceutical companies to coordinate research and treatment

[1] BSA | The Software Alliance (www.bsa.org) is the leading advocate for the global software industry before governments and in the international marketplace. Its members are among the world's most innovative companies, creating software solutions that spark the economy and improve modern life. With headquarters in Washington, DC, and operations in more than 30 countries, BSA pioneers compliance programs that promote legal software use and advocates for public policies that foster technology innovation and drive growth in the digital economy. BSA's members include: Adobe, Atlassian, Autodesk, Bentley Systems, Box, Cadence, CNC/Mastercam, DocuSign, IBM, Informatica, Intel, MathWorks, Microsoft, Okta, Oracle, PTC, Salesforce, ServiceNow, Siemens Industry Software Inc., Sitecore, Slack, Splunk, Trend Micro, Trimble Solutions Corporation, Twilio, and Workday.

efforts, and for regulators to more quickly and accurately assess potential vaccines and treatments. Small businesses are increasingly serving customers not only in physical stores but also through online models that let them reach customers worldwide. As individuals, we are also shifting our lives even further online – whether it is to buy goods and services or to gather with relatives and friends.

In short, it is difficult to overstate the importance of cross-border data transfers to US consumers, businesses of all sizes and sectors, and the entire economy. That is why I want to focus my testimony on the need to ensure companies can continue transferring data across international borders, so they can provide the products and services their customers demand, in a way that respects the privacy and security of the transferred data.

Today's hearing focuses on the Privacy Shield, which until recently served as a privacy-protective way for companies to transfer data from the EU to the United States, consistent with EU legal requirements and privacy expectations of EU and US citizens. The Privacy Shield was invalidated in July, when the Court of Justice of the European Union ("CJEU") issued its decision in *Schrems II*. We applaud the swift response to that decision by policymakers on both sides of the Atlantic and their shared recognition that a new agreement is needed to replace the Privacy Shield. In particular, I would like to thank Chairman Wicker and Ranking Member Cantwell for leading a bipartisan and bicameral letter shortly after the Court's decision. Your efforts helpfully demonstrated strong congressional support for the Administration to negotiate with the European Commission to ensure data flows are not unduly disrupted. We welcome this Committee's efforts to continue supporting the important work of developing a successor to the Privacy Shield, to provide a responsible way for companies to transfer data across the Atlantic. At the same time, along with these important near-term efforts, we also encourage the Committee to think boldly about longer-term, sustainable ways to address the underlying issues about intelligence gathering and privacy – and to work toward building consensus on those issues among like-minded countries.

I. The Ability to Send Data Across International Borders is Critical to Consumers and Companies Worldwide

International data transfers are an essential part of modern-day commerce. They underpin a wide range of everyday business activities. For instance, when an employee joins a video conference with an overseas customer, shares documents with colleagues in a foreign office, sends an order to a supplier in another country, or simply communicates online with someone overseas, that person invariably engages in the cross-border transfer of data. As just one example, modern IT support offered on a 24-hour/7-days-a-week basis – which became critical for many companies even before the current pandemic – would be impossible without the ability to transfer data across borders. Robust cybersecurity likewise relies on sharing data to help companies quickly identify and respond to threats that, by their nature, do not respect national borders. Indeed, sharing information on how bad actors in one country attempted to breach a system can help companies in other countries thwart similar efforts.

International data transfers are an essential component of products and services across industries. For example:

- Detecting fraud. Cross-border data flows help stop credit card fraud on a global scale. By efficiently transmitting data across borders, banks can detect and block fraud attempts in a matter of seconds, regardless of where a purchase is attempted. This process has prevented billions of dollars in losses to online fraudsters.

- Healthcare. Cross-border data transfers allow healthcare facilities to make treatments more effective by using clinical support software that analyzes electronic medical records, insurance claims, and datasets across a large and diverse sample size. It can also enable digitized medical images to be shared with non-local specialists for consultations anywhere in the world, improving the quality of medical care regardless of where a patient lives.

- E-commerce. Cross-border data flows are at the heart of e-commerce. Retailers send data across borders when they check inventory in an overseas warehouse, accept and process customer orders, and enable customers to track shipments en route to their destination.

- Human resources management. Global companies across industries rely on cloud-based human resources systems to hire employees and conduct performance reviews, and to administer benefits and payroll across offices in different countries. The ability to send data across national borders is critical to ensuring companies can coordinate personnel management across a multi-national workforce.

In short, it is difficult to conceive of how commerce in the modern economy could continue to function without the ability to transfer data across international borders. And, in BSA's view, personal data should only be transferred – or used in any way – with real, effective privacy protections. BSA sees no tradeoff between data transfers and data privacy – both are essential. Indeed, BSA has long called for Congress to pass a clear and comprehensive national law that gives consumers meaningful rights over their personal data; imposes obligations on companies to safeguard consumers' data and prevent misuse; and provides strong, consistent enforcement. In all of these conversations, ensuring that companies handle data in privacy-protective ways that honor consumers' expectations is paramount.

Cross border data transfers are critical across all industry sectors. They are also vital to the ability of US companies to grow and compete worldwide. Although most data transfers today involve digital products and services, it would be a mistake to view international data transfers as an issue unique to technology companies. Global companies of all sizes in every industry rely on cross-border data transfers to conduct business, innovate, and compete more effectively. Data transfers are estimated to contribute $2.8 trillion to global GDP – a share that exceeds the global trade in goods and is expected to grow to $11 trillion by 2025.[2] This value is shared by traditional industries like agriculture, logistics, and manufacturing, which realize 75% of the value of the Internet.[3] US companies of all sizes and industry sectors must be able to transfer data across borders to complete in a global market.

Indeed, the cross-cutting importance of this issue spurred BSA to launch a new initiative earlier this year – the Global Data Alliance – bringing together companies in industries ranging from consumer goods to healthcare to aerospace technology. Members of the Global Data Alliance provide a diverse range of products and services, serve different types of customers, and operate in different geographic markets – and they all recognize the critical importance of transferring data across borders in a manner that strongly protects personal privacy.

We also should recognize the ultimate beneficiaries of enabling data to travel freely across borders are consumers. Organizations that rely on cross-border data flows produce the food we eat, the cars we

[2] OECD, *Measuring the Economic Value of Data and Cross-Border Data Flows*, 297 OECD Digital Economy Papers 24 (Aug. 2020), https://www.oecd-ilibrary.org/docserver/6345995e-en.pdf?expires=1606762530&id=id&accname=guest&checksum=E07406A96BD78AB99291D0F7D411F923.

[3] McKinsey Global Institute, *Internet Matters: The Net's Sweeping Impact on Growth, Jobs, and Prosperity* (May 2011), https://www.mckinsey.com/~/media/McKinsey/Industries/Technology%20Media%20and%20Telecommunications/High%20Tech/Our%20Insights/Internet%20matters/MGI_internet_matters_full_report.ashx.

drive, the medicines we take, the clothing we wear, and the myriad other goods and services we enjoy. Consumers also depend on these transfers when communicating with loved ones abroad, engaging in banking transactions, and purchasing goods online. The benefits to individuals of online services has been particularly apparent during the COVID-19 pandemic, with studies indicating 50% of US employees are working remotely.[4] Moreover, global collaboration between researchers, hospitals, and regulators has been critical to the development and testing of treatments and vaccines for COVID-19.

The importance of cross-border data transfers to the economy will only grow. By 2022, 60% of global GDP is expected to be digitized, with growth in every industry driven by data flows and digital technology.[5] By 2025, six billion consumers – amounting to over 75% of the world's population – are predicted to be digitally connected, through over 25 billion connected devices.[6] Ensuring data transfers can happen securely and reliably is therefore fundamental not only to current economic growth, but also to future prosperity.

Transatlantic data transfers are particularly important.[7] Data transfers to the EU account for about 50% of US data transfers, while data transfers to the United States account for an even greater share of EU data transfers.[8] These data flows are support the roughly $312 billion in annual US services exports to Europe.[9]

These numbers underscore a simple but critically important fact: maintaining stable and secure mechanisms for data transfers between the United States and the European Union is essential to the success of both economies, and to the global economy more broadly.

II. EU-US Data Transfers: The Need for Reliable, Privacy-Protective Mechanisms

The need for specific legal mechanisms to transfer data across the Atlantic is rooted in EU law, and is currently embodied in the EU's General Data Protection Regulation ("GDPR"). Under the GDPR, companies may only transfer personal data from the EU to another country if the country has been deemed to provide an "adequate" level of privacy protection, or if the data is transferred pursuant to a legal mechanism recognized by the GDPR.[10] The European Commission has only recognized twelve countries as providing an "adequate" level of protection. When data is transferred to other countries, then, companies must use another legal mechanism recognized by the GDPR.

The Privacy Shield created a way for companies to transfer data to the US under privacy-protective principles the EU deemed "adequate." By invalidating the Privacy Shield, the *Schrems II* judgment has created an urgent need for a new mechanism for transatlantic data transfers.

---

[4] Global Data Alliance, *Cross-Border Data Transfers & Remote Work* at 2 (Oct. 5, 2020), https://www.globaldataalliance.org/downloads/10052020cbdtremotework.pdf.

[5] Daniel D. Hamilton & Joseph P. Quinlan, *The Transatlantic Economy 2020* at 28 (2020), https://transatlanticrelations.org/publications/transatlantic-economy-2020/ ("The Transatlantic Economy 2020").

[6] Global Data Alliance, *Cross-Border Data Transfer Facts and Figures*, https://globaldataalliance.org/downloads/gdafactsandfigures.pdf ("GDA Facts and Figures").

[7] Recent studies indicate transatlantic cables carry 55% more data than transpacific routes, and the quantity of these transatlantic data transfers are growing rapidly. The Transatlantic Economy 2020 at 41.

[8] BSA | The Software Alliance, *The Future of Transatlantic Data Flows* at 1 (Sept. 23, 2020), https://www.bsa.org/files/policy-filings/bsa_transatlanticdataflows.pdf ("BSA Transatlantic Data Flows").

[9] The Transatlantic Economy 2020 at iii.

[10] *See* GDPR, Chapter V. The GDPR took effect in May 2018; the EU's prior data protection law similarly restricted the transfer of personal data to third countries. *See* Directive 95/46/EC.

Transfer Mechanisms. The GDPR recognizes several legal mechanisms for transferring data across borders, including Standard Contractual Clauses ("SCCs") and Binding Corporate Rules ("BCRs").[11]

- Standard Contractual Clauses. SCCs are a standardized set of contractual obligations that companies can adopt when transferring data outside the EU. The SCCs are approved by the European Commission and reflect commitments that implement EU legal requirements to safeguard data. Companies that transfer data pursuant to SCCs typically include the Commission-approved contract language in all of their relevant contracts with suppliers and other vendors. SCCs are widely used, and they underpin transfers of personal data from the EU not only to the US, but to more than 180 countries. In 2019, one survey found that nearly 90% of companies that transferred data outside of the EU relied on SCCs.[12]

- Binding Corporate Rules. BCRs are corporate rules that govern international data transfers within a company. The GDPR sets out a list of topics that must be addressed by BCRs, which must specify how the company will apply certain data protection principles and data subject rights to the transferred data. BCRs may take several years to develop and must be approved by a data protection authority in the EU before they can take effect. Even so, their use is limited to a specific set of intra-company transfers; BCRs accordingly do not provide a basis for transferring data to third parties, such as customers, partners, or suppliers.

Privacy Shield. The Privacy Shield provided an important and cost-effective alternative mechanism for transferring data from the EU to the United States. It was negotiated by the US Government and the European Commission to allow companies to commit to privacy principles that ensured data transferred to the US was "adequately" protected. As a result, transfers under the Privacy Shield were deemed "adequate" – thus allowing companies to transfer data from the EU to the US under the Privacy Shield program without using other mechanisms such as SCCs or BCRs.

The Privacy Shield established a voluntary program for companies to transfer data – but once a company publicly committed to comply with its requirements, that commitment becomes enforceable by the Federal Trade Commission. Companies that participate in the Privacy Shield therefore commit to handle data transferred from the EU to the US in line with seven privacy-protective principles on notice, choice, onward transfers, security, data integrity and purpose limitation, access, and enforcement. Participants also adhere to sixteen supplemental principles, which address additional protections for sensitive data and dispute resolution, among other issues. To help ensure these protections remained meaningful in light of changes involving technologies and developments in EU or US law, the Privacy Shield created an internal review mechanism for the United States and the EU to update the Privacy Shield over time. Its most recent annual review, released in October 2019, confirmed that the Privacy Shield remained a trusted mechanism for companies and individuals alike.[13]

The Privacy Shield program was well-used, particularly by small- and medium-sized entities transferring data from the EU. Over 5,300 organizations, in industries ranging from manufacturing to hospitality,

[11] The other mechanisms include legally binding instruments between public authorities; codes of conduct; and approved certifications. The GDPR also permits companies to transfer data pursuant to derogations for limited, specific situations.
[12] IAPP-EY Annual Governance Report 2019 (Nov. 6, 2019), https://iapp.org/resources/article/iapp-ey-annual-governance-report-2019/ (survey of 370 companies)
[13] European Commission, Report from the Commission to the European Parliament and The Council on the Third Annual Review of the Functioning of the EU-U.S. Privacy Shield, Oct. 23, 2019, https://ec.europa.eu/info/sites/info/files/report_on_the_third_annual_review_of_the_eu_us_privacy_shield_2019.pdf.

participated in the Privacy Shield program,[14] and more than 70% of those companies were small- or medium-sized businesses.[15] Its benefits reached more broadly, though, to the networks of suppliers and customers that depended on these Privacy Shield-certified companies.

The US Government also made significant commitments in connection with the Privacy Shield, to address the protection of data transferred under the program. These include not only the annual review mechanism discussed above, but also the establishment of an ombudsperson mechanism, which was designed to respond to requests by EU individuals regarding US signals intelligence practices.[16] Officials at the US Department of Justice and the Office of the Director of National Intelligence also described the many limitations and safeguards applicable to US government access for law enforcement and for national security purposes.[17] These include Presidential Policy Directive 28 ("PPD-28"), which was issued in 2014 to set out principles and requirements that apply to all US signals intelligence activities. In addition to these commitments, the US Privacy and Civil Liberties Oversight Board has issued oversight reports or conducted oversight reviews of many of these national security authorities.

***Schrems II* Litigation**. The *Schrems II* decision arose after a series of complaints filed by Max Schrems, who in 2013 challenged the predecessor to the Privacy Shield, which was known as the Safe Harbor. In October 2015, the CJEU annulled the Safe Harbor, creating the need for the US and EU to negotiate the Privacy Shield. Later the same year, Schrems filed a reformulated complaint challenging the ability of Facebook to transfer data from the EU to the US using SCCs. Even though the reformulated complaint centered on the use of SCCs, proceedings before both the Irish High Court and the CJEU sparked substantial discussion on the Privacy Shield.

BSA participated in the *Schrems II* litigation as an amicus curiae. We argued before the CJEU, asking it to uphold the SCCs and not address the Privacy Shield, which we felt it did not need to reach in order to decide that case. Throughout the litigation, BSA emphasized SCCs are intended to support transfers to jurisdictions the European Commission has not already deemed "adequate" – and therefore companies using the SCCs should focus on the protections provided by those clauses rather than on the protections offered by the laws of the third country to which data is exported.

In July 2020, the CJEU's *Schrems II* decision invalidated the Privacy Shield, taking away this critical mechanism for transferring data.[18] Importantly, the CJEU did not take issue with the privacy practices of companies that use the Privacy Shield. Rather, the Court based its decision on US intelligence practices it found were not consistent with the EU Charter of Fundamental Rights. The Court focused specifically on signals and intelligence collection under Executive Order 12333 and Section 702 of the FISA Amendments Act of 2008.

---

[14] Congressional Research Service, *U.S.-EU Privacy Shield* (Aug. 6, 2020), https://fas.org/sgp/crs/row/IF11613.pdf.
[15] US Department of Commerce Department, Commerce Secretary Wilbur Ross Welcomes Privacy Shield Milestone-Privacy Shield Has Reached 5,000 Active Company Participants (Sept. 11, 2019), https://www.trade.gov/press-release/commerce-secretary-wilbur-ross-welcomes-privacy-shield-milestone-privacy-shield-has.
[16] *See* John F. Kerry, Letter to Commissioner Jourova (July 7, 2016), https://www.privacyshield.gov/servlet/servlet.FileDownload?file=015t00000004q0b.
[17] *See* Bruce C. Schwartz, Letter to Justin Antonipillai and Ted Dean (Feb. 19, 2016), https://www.privacyshield.gov/servlet/servlet.FileDownload?file=015t00000004q0W; Robert Litt, Letter to Justin Antonipillai and Ted Dean (Feb. 22, 2016), https://www.privacyshield.gov/servlet/servlet.FileDownload?file=015t00000004q1F; and Robert Litt, Letter to Justin Antonipillai and Ted Dean (June 21, 2016), https://www.privacyshield.gov/servlet/servlet.FileDownload?file=015t00000004q1A.
[18] Case C-311/18, *Data Protection Commissioner v. Facebook Ireland Ltd, Maximillian Schrems* (*Schrems II*), ¶¶ 180-85, 191-92, 197-201 (July 16, 2020).

At the same time, the CJEU upheld the validity of SCCs. While we agree with the European Commission and the US Government that the safeguards and commitments contained in the Privacy Shield should have been sufficient, we were pleased the Court affirmed the validity of SCCs. Like BCRs, SCCs can create commercial privacy protections beyond those included in the Privacy Shield, because companies may use them to make additional binding commitments.[19] For companies using SCCs, the CJEU stressed the need to determine, on a case-by-case basis and in light of all the circumstances of the transfer, including any additional safeguards that parties may add to SCCs, whether the data can be protected adequately. We agree with that approach. In October, BSA published a set of principles to guide companies in developing additional safeguards for EU-US data transfers. The principles can be turned into specific clauses appropriate to the specific nature of the transfer.[20]

Last month, the European Data Protection Board ("EDPB"), which comprises representatives of the national data protection authorities within the European Union, published draft recommendations for the use of SCCs for transferring data. We understand the concern many companies have raised about whether the recommendations would effectively prohibit transfers to the US. We appreciate that the EDPB has opened its recommendations to public comment. We also respect the difficulty of providing examples that account for all of the circumstances of all data transfers. We remain optimistic the draft recommendations can be revised to better reflect the CJEU's judgment, which envisions greater flexibility and use of additional safeguards to protect privacy. For example, the CJEU's decision directs companies to consider "all" circumstances of a transfer in determining whether additional safeguards are appropriate to supplement SCCs. The full set of relevant circumstances may include the nature of the data transferred and the likelihood of government access to that data, yet the range of these circumstances are not fully reflected in the current draft recommendations.

Despite the widespread use of SCCs, we should not forget that the use of SCCs creates burdens, particularly on smaller businesses that may be forced to re-negotiate all of their relevant contracts to include terms of SCCs. This option should therefore not be viewed as a replacement for the Privacy Shield. Given the breadth and diversity of companies that rely on transatlantic data transfers, it is imperative to ensure there are multiple practical and privacy-protective ways for companies to transfer data.

III. There is Broad Support for the US Government and the European Commission to Develop an Enhanced Privacy Shield

We commend the US Government and the European Commission for recognizing the need for a new agreement to improve on the Privacy Shield. Shortly after the CJEU's judgment, the Department of Commerce and the European Commission jointly announced the initiation of discussions to evaluate the potential for an enhanced Privacy Shield framework.[21] In doing so, both governments "recognize[d] the vital importance of data protection and the significance of cross-border data transfers to our citizens and economies," and stressed their mutual commitment to supporting privacy, the rule of law, and the close economic relationship between the United States and Europe.[22]

---

[19] In fact, BSA members were making commitments beyond what is included in Commission-approved SCCs before the *Schrems II* case began.
[20] BSA | The Software Alliance, *Principles: Additional Safeguard for SCC Transfers* (Oct. 2020), https://www.bsa.org/files/policy-filings/10222020bsascctransfers.pdf.
[21] *Joint Press Statement from U.S. Secretary of Commerce Wilbur Ross and European Commissioner for Justice Didier Reynders* (Aug. 10, 2020), https://www.commerce.gov/news/press-releases/2020/08/joint-press-statement-us-secretary-commerce-wilbur-ross-and-european.
[22] *Id*.

These efforts have strong bipartisan, bicameral support. Again, we very much appreciate the letter Chairman Wicker and Ranking Member Cantwell sent after the *Schrems II* decision to the Commerce Department and the Federal Trade Commission, along with your counterparts on the House Energy and Commerce Committee, encouraging them to work closely with the European Commission to develop a new data transfer mechanism to replace the Privacy Shield.[23]

All sectors of the US economy have also demonstrated support for this effort to reach an improved agreement. BSA and the US Chamber of Commerce led a letter signed by dozens of trade associations spanning a broad range of industries, which together encouraged the US Government to work collaboratively with its EU counterparts to develop a stable and sustainable mechanism to replace the Privacy Shield.[24]

The US Government and the European Commission have also repeatedly expressed their support for the Privacy Shield framework. Prior to the Court's judgment in *Schrems II*, European regulators described the Privacy Shield as a "success story," that offered strong privacy protections to EU data subjects and exemplified the productive partnership between the EU and US governments.[25] In the *Schrems II* litigation, both the US Government and the European Commission argued in support of the Privacy Shield, stressing its importance to both sides of the Atlantic. As an amicus in *Schrems II* and in a separate challenge to the Privacy Shield, BSA argued in support of the Commission and of the Privacy Shield. Moreover, at BSA, we have a longstanding relationship with the European Commission and are committed to working collaboratively and closely with them to address the need for robust data transfer mechanisms and find long-term solutions.

We are confident the US Government and the European Commission can work together to develop an enhanced successor to the Privacy Shield. In its decision invalidating the Privacy Shield, the CJEU focused on concerns around two specific US intelligence-gathering programs, including whether those programs appropriately safeguard privacy and fundamental rights, whether they are subject to independent oversight, and whether they provide EU data subjects with rights to judicial redress. Given the targeted nature of the Court's concerns, we are optimistic the US Government and European Commission can work together to address them. Indeed, it is important to recognize the CJEU expressed no concerns about the adequacy of the privacy protections imposed on commercial entities by the Privacy Shield. Developing an enhanced Privacy Shield should not require a complete overhaul of the existing model but instead should address the specific concerns highlighted in the *Schrems II* judgment. We fully support those efforts and stand ready to provide whatever assistance we can.

IV. Over the Long Term, Countries Must Work Together to Recognize Shared Values on Appropriate Safeguards for Intelligence Practices

The ongoing work by the Administration and the European Commission to develop an enhanced Privacy Shield is urgent, and we appreciate their constructive approach and this Committee's focus on the issue. Creating a new and enhanced mechanism for such transfers is vital to the continued prosperity of both the United States and Europe.

---

[23] *Letter from Senator Roger Wicker et al. to Secretary Wilbur Ross & Chairman Joseph Simons* (Aug. 5, 2020), https://energycommerce.house.gov/sites/democrats.energycommerce.house.gov/files/documents/FTC.DOC.2020.8.5.%20Letter%20re%20Privacy%20Shield%20ECJ%20Decision.CPC_.pdf. In addition, several members of the House of Representatives, led by Representatives Welch, LaHood, and DelBene, have echoed this support. *Letter from Representative Peter Welch et al. to Secretary Wilbur Ross & Chairman Joseph Simons* (Oct. 2, 2020), https://www.bsa.org/files/policy-filings/10022020congresslettersupportprivacyshield.pdf

[24] *Letter from BSA | The Software Alliance et al. to Secretary Wilbur Ross* (July 17, 2020), https://www.bsa.org/files/policy-filings/07172020multiindustryresponselettertoschremsii.pdf.

[25] European Commission, *EU-U.S. Privacy Shield: Third Review Welcomes Progress While Identifying Steps for Improvement* (Oct. 23, 2019), https://ec.europa.eu/commission/presscorner/detail/en/IP_19_6134.

We also urge this Committee, the US Government, and all like-minded democratic societies interested in both security and civil liberties to think boldly about longer-term approaches to security safeguards. Even the CJEU recognizes some amount of signals intelligence is necessary in a democratic society to ensure safety and security. The question is what guardrails and safeguards are needed.

The US Government has, to its credit, publicly released significant guidance about safeguards and oversight mechanisms. It is well positioned to lead a conversation with other governments about the appropriate use of safeguards to protect privacy and fundamental rights, the level of independent oversight, and the ability of individuals to obtain redress for violations. A common understanding on best practices will improve transparency among America's allies and decrease future transatlantic data conflicts.

We have full confidence the US Government and the European Commission can address these issues in the context of developing a successor to the Privacy Shield. At the same time, we recognize commitments and agreements addressing such practices are more durable when they reflect a broader consensus of America and its allies on the appropriate scope of intelligence-gathering practices.

We accordingly encourage the US Government to work with like-minded democratic countries to build a mutual recognition that many countries already share a set of values on the appropriate safeguards for intelligence-collection activities. For example, we support the US Government working toward diplomatic agreements with countries that share our commitment to democracy and the rule of law, to set out a mutual understanding of the types of safeguards appropriate for intelligence-gathering activities to ensure respect for the privacy and fundamental rights of individuals. We do not underestimate the potential magnitude of such an effort, or the challenges it might present. But we believe US leadership on this issue will both strengthen US economic interests, and ensure the United States and its allies can are aligned in promoting economic growth based on the principles of freedom, security, democratic values, and human rights across the globe.

* * *

Thank you again for the opportunity to testify at today's hearing. BSA looks forward to working with the Committee on promoting reliable and secure mechanisms for international data transfers.