ITIF | INFORMATION TECHNOLOGY & INNOVATION FOUNDATION

‘Schrems II’: What Invalidating the EU-U.S. Privacy Shield Means for Transatlantic Trade and Innovation

NIGEL CORY, DANIEL CASTRO, AND ELLYSSE DICK I DECEMBER 2020

The EU-U.S. Privacy Shield’s demise affects thousands of firms that relied on it to transfer data. Policymakers should realize the enormous trade and innovation stakes involved—both bilateral and global—and build an improved framework for data protection and digital trade.

KEY TAKEAWAYS

- Transatlantic data flows allow firms from all sectors to benefit from data-driven innovation, strengthen trade, and increase consumer access to a growing range of digital and digitally enabled goods and services.
- Privacy Shield was a critical bridge between two different data protection regimes for thousands of mainly small and medium-sized firms. Given the cost and complexity of alternatives, they will be disproportionately impacted by its demise.
- The political challenge ahead is reconciling different government surveillance systems, both between the EU and United States and among EU member states. This problem is not one the private sector can solve on its own.
- The role and importance of transatlantic data flows and data protection will only grow. Policymakers need to recognize this and ensure it is supported through further cooperation and new data-transfer mechanisms.
- Europe and the United States share more in common than they often admit, especially compared to authoritarian powers such as China. Severing digital trade ties would hurt both sides by fragmenting of the global digital economy.

INTRODUCTION

The July 2020 decision by the European Court of Justice (ECJ) to invalidate the EU-U.S. Privacy Shield will have an immediate and potentially long-term impact on the thousands of organizations that relied on it to legally transfer data abroad for operations, customer service, communications, research and development, and human resources. Data transfers are a necessity for trade and innovation in the global digital economy, especially during the COVID-19 pandemic. These organizations—mostly small and medium-sized businesses, from diverse sectors and countries—face considerable uncertainty about their alternatives for managing data transfers, as these options are more costly and complicated, and themselves now on shaky legal grounds. The other choice—de facto forced local data storage in Europe—is also costly and complicated for firms, and would divert resources from more meaningful steps organizations could take to protect data. Policymakers on both sides of the Atlantic need to realize what is at stake and urgently work together to establish a new legal framework.

A clear, predictable, and accessible legal framework for data protection makes it easier for organization to manage and transfer data. Transatlantic data flows allow firms from all sectors to benefit from data-driven innovation, strengthen trade between countries in a growing range of digital and digitally-enabled goods and services, and expand consumers' access to a growing variety of goods and services.[1] The EU-U.S. Privacy shield was especially important to enable small and medium-sized enterprises (SMEs) on both sides of the Atlantic to transfer data abroad because they don't have the resources or expertise to use other more costly and complicated legal mechanisms.

If policymakers do not create an alternative to the EU-U.S. Privacy Shield, firms from a broad range of sectors on both sides of the Atlantic will suffer—just as COVID-19 accelerates the digital transformation of our society and economy.

Attempts at reconciling the EU and U.S. approaches to data protection have long been deviled by concerns over surveillance and implicit protectionism. While both sides have agreed on legal tools to establish transatlantic data flows—initially the U.S.-EU Safe Harbor in 2000, and more recently the EU-U.S. Privacy Shield—EU courts have now undermined these efforts twice with the *Schrems I* and *Schrems II* rulings. Though the latest setback is no doubt frustrating for EU and U.S. policymakers, it has hopefully clarified where further work is needed to resolve the outstanding issues in order to develop a cooperative, integrated, and stable transatlantic relationship on digital policy. If policymakers do not create an alternative to the EU-U.S. Privacy Shield, firms from a broad range of sectors on both sides of the Atlantic will suffer—just as COVID-19 accelerates the digital transformation of our society and economy.

It's an especially challenging context for EU-U.S. negotiations and any potential new agreement. Many policymakers' views are shaped by recent bilateral trade and political tensions. There's also a tendency for some to view digital policy through a singular lens that only focuses on leading American technology firms. Policymakers are also understandably preoccupied by other pressing issues, including the COVID pandemic's health and economic impacts and preparing for an incoming Biden administration. This means that there's a real risk that policymakers may not recognize the immediate and long-term consequences if this critical component of the

transatlantic economic relationship is not quickly repaired or replaced. While creating a new solution will be challenging and require substantial work by both sides, thankfully, a history of good faith engagement, an openness to new ideas, and shared values provides a foundation for the EU and United States to create something that is mutually beneficial.

This brief provides an overview of the EU-U.S. Privacy Shield, who uses it, and the impacts its invalidation could have on individual firms and digital innovation more broadly. Ultimately, policymakers need to realize what is at stake and prioritize creating a solution.

'SCHREMS II' AND EU-U.S. PRIVACY SHIELD: SEVERING A CRITICAL CONNECTION

In *Schrems II,* the ECJ found that the data surveillance laws and compliance requirements for data processors in the United States made it impossible for firms to ensure that, once transferred, individuals' data in the United States received equivalent protections to those in the EU. Specifically, the court identified Section 702 of the Foreign Intelligence Surveillance Act (FISA) and Executive Order 12333, which allow U.S. intelligence agencies to collect data on foreign nationals, as inconsistent with rights guaranteed in the EU Charter.

The U.S. government disputes the merits of the ECJ's ruling, arguing that the court did not consider many of the oversight functions in place, some of which have been made recently. For example, the U.S. Foreign Intelligence Surveillance Court actively monitors whether U.S. intelligence agencies properly target individuals to obtain intelligence information.[2] In addition, U.S. laws, including FISA and the Administrative Procedures Act, allow foreign individuals to seek redress for violations in U.S. courts through civil lawsuits.

Moreover, there are serious questions about the rationale of the ECJ's decision. The simple fact is that the vast majority of companies that used the EU-U.S. Privacy Shield have no data of relevance to national security, and are unlikely to ever be subject to a FISA-related request. Regardless, all participants in the EU-U.S. Privacy Shield have lost the ability to transfer data under this program even though it may be an unrealistic concern for most.

The simple fact is that the vast majority of companies that used the EU-U.S. Privacy Shield have no data of relevance to national security, and are unlikely to ever be subject to a FISA-related request.

The ECJ's ruling invalidated the European Commission's adequacy decision that allowed firms to self-certify under the EU-U.S. Privacy Shield. As a result, organizations are no longer able to use this framework to transfer personal data, and must use alternative transfer mechanisms. The *Schrems II* ruling upheld the validity of Standard Contractual Clauses (SCCs) with "supplementary measures" to ensure adequate protections. The European Data Protection Board's (EDPB) recommendations on these measures provide some guidance, but considerable uncertainty remains in how to implement them alongside European Commission policy advice, past and upcoming ECJ rulings related to SCCs, and how each EU member state's Data Protection Authority (DPA) will interpret and enforce all of these changes.[3] However, there is still a lack of clarity around SCCs and what constitutes supplementary measures and sufficient data protection in the absence of an adequacy decision. Exporters can also use other legal alternatives, such as Binding Corporate Rules (BCRs) and derogations, to ensure compliance.

THE EU-U.S. PRIVACY SHIELD: A BRIDGE BETWEEN DIFFERENT APPROACHES TO DATA PROTECTION

The EU and United States use bridging mechanisms—firstly, Safe Harbor, and most recently, Privacy Shield—as they manage data protection very differently, yet both realize the importance of data transfers for trade and innovation. The United States uses a risk- and accountability-based approach wherein firms remain legally responsible for managing data wherever they transfer and store it, whereas the EU uses a more rigid, compliance-based approach that restricts international data transfers to a small list of countries it says provide the same protection as the EU's General Data Protection Regulation (GDPR).[4] In making these determinations, the European Commission considers both the levels of legal protections in an importing country and the potential impacts of stopping data flows to that country. These determinations don't allow onward transfer of EU personal data to third countries (unless they're also deemed adequate or another legal tool is used). Because the EU does not deem the United States to have met its adequacy test, it has worked with the United States to establish a program to address the differences. U.S. firms, and EU firms with U.S. subsidiaries, must abide by these additional legal mechanisms to receive EU personal data.

Privacy Shield was a critical bridge in providing the additional safeguards that EU law required for transferring personal data from the EU to the United States. It provided an element of trust to EU consumers, a system of recourse, and an easier pathway to transfer EU personal data.

The EU-U.S. Safe Harbor framework, established in 2000, provided this bridge initially. After the ECJ invalidated Safe Harbor following the *Schrems I* decision, the United States and EU negotiated the Privacy Shield framework in 2016. Privacy Shield was developed to provide a more robust interoperability mechanism to manage transfers of EU personal data between the United States and EU. The agreement was welcomed on both sides of the Atlantic, with then-vice president of the commission Andrus Ansip noting that "[EU] businesses, especially the smallest ones, have the legal certainty they need to develop their activities across the Atlantic."[5] Likewise, then U.S. Federal Trade Commission (FTC) chairwoman Edith Ramirez stated that it was essential to "[ensuring] consumer privacy is protected on both sides of the Atlantic."[6]

Privacy Shield was a critical bridge between the two regimes in providing the additional safeguards that EU law required for transferring personal data from the EU to the United States. Privacy Shield provided an element of trust to EU consumers, a system of recourse, and an easier pathway to transfer EU personal data. Under Privacy Shield, organizations that intended to transfer data could self-certify adherence to a set of principles through the U.S. Department of Commerce, such as by including additional privacy and protection measures in their data transfer policies and practices.[7] Organizations must continue to adhere to these principles in order to remain in compliance with EU law. Organizations paid an annual fee to participate in Privacy Shield. The annual fee was based on an organization's annual revenue, which started at $250 for organizations with up to $5 million in revenue and ended with $3,250 for organizations that had over $5 billion in revenue.[8] Thus, Privacy Shield was affordable, and thus accessible, to a broader range of smaller firms.

While affordable, Privacy Shield was not necessarily easy or cheap. It was much more than just a box-ticking exercise, as many firms invested considerable money, time, and effort to build new data protection policies and procedures as part of self-certification (and to maintaining compliance). For example, identifying and renegotiating contracts with outside vendors (to embed data handling requirements) involves considerable complexity and administrative costs. Unless firms were already subject to specific U.S. data privacy laws (such as the U.S. Health Insurance Portability and Accountability Act), they may not have had to do an inventory of their data and build out their data protection practices for EU personal data. Firms also had to provide a readily available independent recourse mechanism to hear individual complaints (at no cost to the individual).

While electing to self-certify is voluntary, the principles are legally binding, ensuring the framework provides consistent and universal safeguards for transatlantic data transfers. The FTC monitors compliance and has the authority to take legal action against companies that falsely claim Privacy Shield participation or compliance. In April 2019, the Department of Commerce started a system to do 30 spot-checks on firms each month to proactively ensure firms are in compliance with their commitments.[9] In the first half of 2020, the FTC finalized settlements with at least 12 companies that misrepresented their participation in Privacy Shield or failed to comply with the Privacy Shield principles.[10] Privacy Shield also provided an option for EU citizens to invoke binding arbitration to determine whether an organization has violated the agreement. The U.S. Department of Commerce set up a fund that all Privacy Shield organizations contribute to in order to cover arbitration costs (the fund and arbitration itself was managed by the International Centre for Dispute Resolution-American Arbitration Association).[11]

Privacy Shield had a significant impact on the data privacy practices of many firms involved in transatlantic trade and innovation. It led many new, especially smaller, firms to allocate more resources and attention to data compliance, which left them better positioned to meet future data compliance requirements in Europe and elsewhere. Thus, the EU-U.S. Privacy Shield established a higher baseline for transatlantic data flows. EU and U.S. policymakers should recognize that this was a good-faith effort by the many firms involved in Privacy Shield, and a positive overall outcome in terms of improved commercial data privacy and digital trade. This is the progress they should aim to build on.

WHATEVER THE LEGAL TECHNICALITIES, DATA TRANSFERS ARE NECESSARY AND BENEFICIAL TO TRANSATLANTIC TRADE AND INNOVATION

The increased digitalization of organizations, driven by the rapid adoption of technologies such as cloud computing and data analytics, has increased the importance of data as an input to trade and commerce, impacting not just information industries, but traditional industries as well.[12] Data flows are critical to the $7.1 trillion transatlantic trade and innovation relationship.[13] The development, adoption, and consumption of data-driven goods and services is central to improved productivity and innovation, and thus standards of living, in the United States and European Union.[14]

As the Information Technology and Information Foundation (ITIF) outlined in "Promoting European Growth, Productivity, and Competitiveness by Taking Advantage of the Next Digital Technology Wave," the EU has an opportunity to make major strides in the next wave of digital transformation, especially in areas where it has competitive advantage, such as smart

manufacturing and technology-enabled business services.[15] But it will require the EU and the United States to put in place the right policies to allow the transfers of data that support the mutually beneficial movement and use of data, while obviously accounting for their respective approaches to data privacy.

The amount, type, and flow of data continues to grow exponentially. Companies collect and analyze personal data to better understand customers' preferences and willingness to pay, and adapt their products and services accordingly. It is a simple fact that international trade involving consumers cannot take place without collecting and sending personal data—such as names, addresses, billing information, etc.—across borders. Likewise, modern innovation often requires the transfer of personal data, such as for clinical trials. But personal data is just one part of a broader flow and use of data. Organizations increasingly rely on data to monitor production systems, manage global workforces, monitor supply chains, and support products in the field in real time.

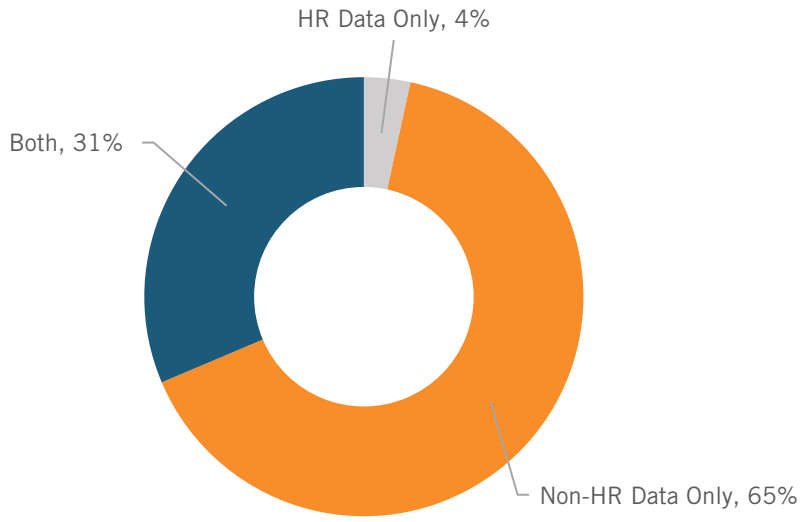
However, personal information is often intertwined with non-personal data. Thus, a restriction on personal data can act as a restriction on the use and transfer of the rest of the information contained in the data. Segregating different categories of information within particular data and within truly global cloud storage and data analytics systems is not straightforward. The Organization for Economic Cooperation and Development (OECD) report "Trade and Cross-Border Data Flows," which surveyed 259 firms (headquartered in 48 countries, but mainly in the EU, Japan, and the United States) showed that it is costly and complicated for firms from all sectors to split personal and non-personal data.[16]

Without the Privacy Shield framework, it'll become more costly and complicated for organizations figuring out what safeguards are necessary. For SMEs, the additional cost of additional legal compliance and operational changes to IT systems may reach a tipping point that changes the cost/benefit ratio of transatlantic trade, thus leading them to withdraw.

WHO USED PRIVACY SHIELD, AND WHAT THE IMPACT WOULD BE IF THERE'S NO FRAMEWORK FOR DATA TRANSFERS

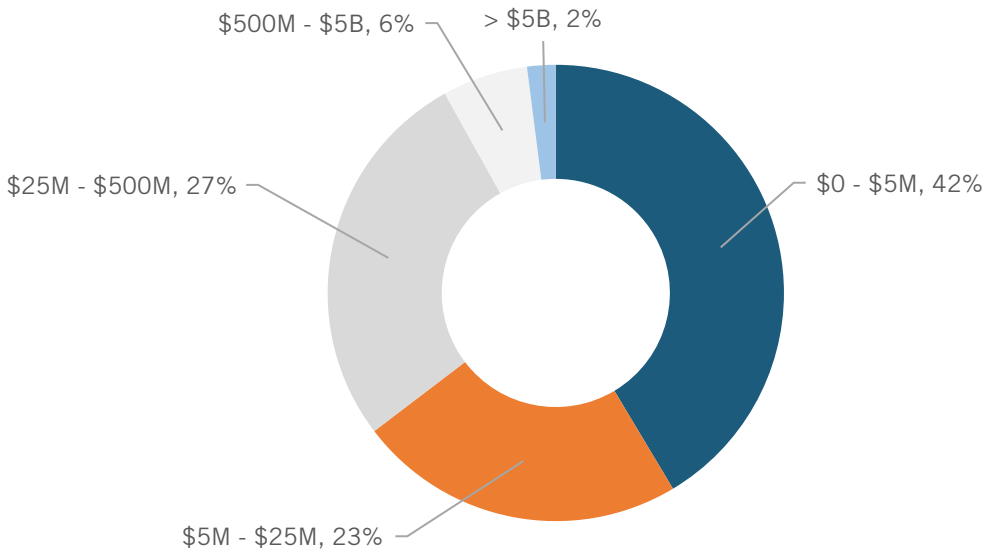
The death of Privacy Shield will be felt across industries in both the United States and the EU. These firms represent virtually all segments of the global digital economy well beyond those considered "tech." Privacy Shield's growing importance is a direct reflection of the increasingly critical role of data and data flows to transatlantic trade and innovation. As of October 2020, 5,211 firms were actively self-certified under the Privacy Shield. Previous studies by The Future of Privacy Forum show that membership has grown significantly since its inception: from 2,177 in September 2017 to 3,703 firms in September 2018 (70 percent growth) to 5,348 in June 2019 (44 percent growth).[17] The ECJ's decision has likely contributed to the recent fall in active firms listed under Privacy Shield. Over 1,500 organizations used it to transfer human resources (HR) data (see figure 1).[18]

Figure 1: Privacy Shield use by data category[19]



Privacy Shield was one of the most popular legal mechanisms for firms, especially SMEs, seeking to transfer data and engage in digital trade between Europe and the United States. Privacy Shield was one of the most popular legal mechanisms for firms, especially SMEs, seeking to transfer data and engage in digital trade between Europe and the United States. According to a 2019 survey by the International Association of Privacy Professionals (IAPP), 60 percent of privacy professionals said their firms used Privacy Shield compliance as a legal safeguard for data transfers.[20] It was mainly used by SMEs—in September 2019, the U.S. Department of Commerce reported that more than 70 percent of Privacy Shield firms at that time were SMEs.[21] This is contrary to the popular conception that it and data flows in general are simply a tool of "big tech" (see figure 2). SMEs don't have the resources and expertise to use other more onerous and complicated legal tools, such as SCCs. Privacy Shield was also attractive in that while SMEs may have had customers on either side of the Atlantic, they did not necessarily have operations and subsidiaries (nor could they afford setting up a physical presence) in all markets.

Figure 2: Privacy Shield participants by revenue (of 5,000-plus firms, 2019)[22]



Privacy Shield Was Used in Europe—and the World

Privacy Shield was used by firms across the United States and European Union. While the Department of Commerce's list specifies where firms are based in the United States, it does not specify where firms operate in the EU. However, many firms are headquartered or have offices there. Previous Future of Privacy Forum studies show that there were 114 EU headquartered or co-headquartered firms participating in Privacy Shield in 2017, which increased to 202 in 2018 (a 77 percent increase), and to 259 EU in June 2019 (a 28 percent increase).[23]

Examples of European firms (and their sector) that used Privacy Shield include Adjust (market research services, Germany), Agfa Health (Belgium), Aldi (retailer, Germany), Allergan (biopharmaceuticals, Ireland), Ascendia (material handling, France), Avania (scientific and technical services, Netherlands), Axialent (education services, Spain), Barilla (grains, Italy), BTS (corporate training, Sweden), CluePoints (health data analytics, Belgium), Dailymotion (media and entertainment, France), Deutsche Boerse (financial technology, Germany), eFront Financial Solutions (France), Funcom (toys and games, Finland), HalioDx (health care, France), Bauer Xcel Media (book publishing, Germany), Eaton Corporation (management company, Ireland), Euronext (financial services, Netherlands), Johnson Controls (equipment and machinery, Ireland), Global Shares (financial services, Ireland), I.K. Hofmann (employment services, Germany), International Drug Development Institute (Belgium), Jazz Pharmaceuticals (Ireland), Lidl (food retailer, Germany), Salzburg Global Seminar (higher education, Austria), Siemens Digital Industry Software (Germany), Ulrich Medical (surgical instruments, Germany), and Valneva (vaccine development, France).[24]

Highlighting the global need for interoperable data transfer mechanisms such as Privacy Shield to manage data flows, it was also used by many non-U.S. and non-EU firms. For example, 99Designs (marketing services, Australia), AscendantFX Capital (banking, Canada), Blackline Safety (industrial safety and security, Canada), EML Payments (financial services, Australia), Gan and Lee Pharmaceuticals (China), Lululemon (clothing retailer, Canada), M3 USA (book publisher and

marketing, Japan), Pokémon Company International (video games, Japan), Prodalim (fruit products, Israel), Shiseido (cosmetics and toiletries, Japan), Showbie (education technology, Canada), and Teva Pharmaceuticals (Israel). Dozens of firms from the United Kingdom also used Privacy Shield, such as activpayroll (accounting services), Adelphi Communications (business services), Advanced Travel Partners International (travel), EIMS (marketing), PCI Pal (telecommunications), Safe Passage International (corporate training), Sonnedix USA Services (solar energy), and the Planning Shop (professional services).

Privacy Shield Was Used Throughout the U.S. Economy

Privacy Shield was used by firms in sectors throughout the U.S. economy—30 U.S. states were home to more than 20 firms that used it. (See table 1.) Unsurprisingly, California (1,357) and New York (587) were home to the most firms, but hundreds more firms through many other states use it too.

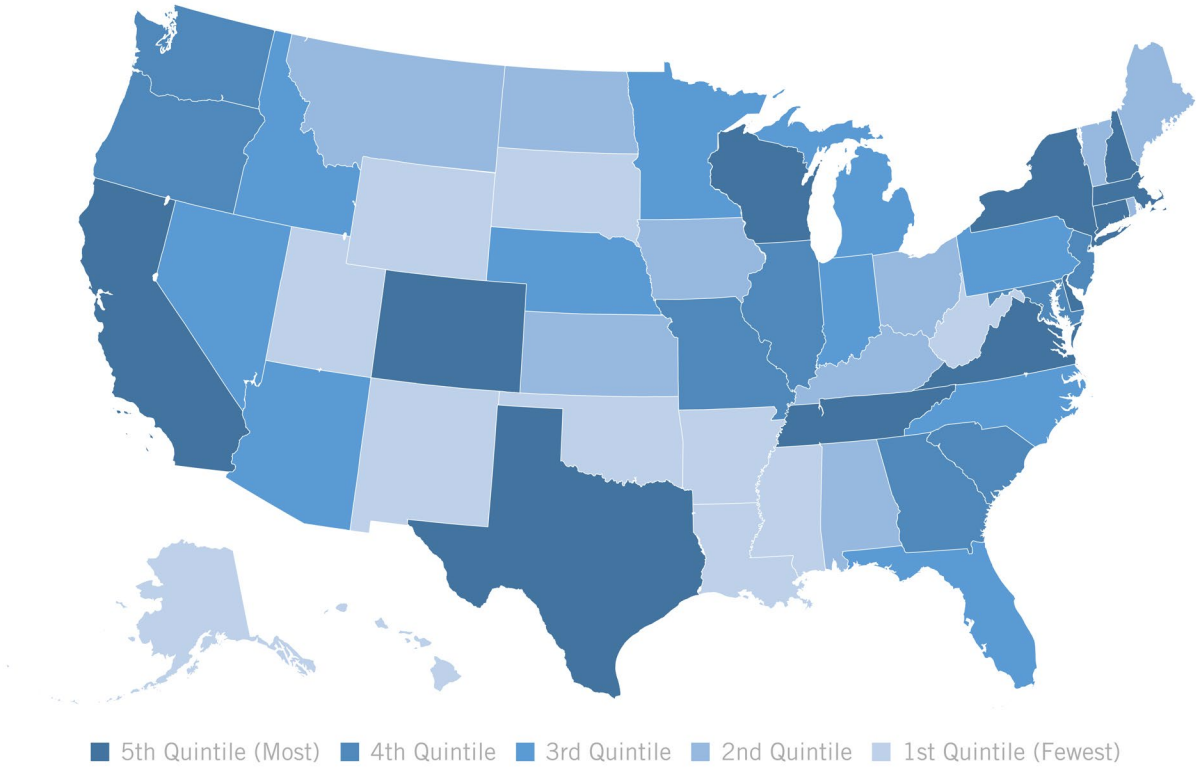
Table 1: Active Privacy Shield firms by U.S. state (October 2020)

Rank	State	Firms	Rank	State	Firms	Rank	State	Firms
1	California	1,357	11	Colorado	135	21	Minnesota	66
2	New York	587	12	Virginia	133	22	Arizona	53
3	Massachusetts	335	13	North Carolina	109	23	Indiana	50
4	Texas	295	14	Maryland	87	24	District of Columbia	49
5	Florida	220	15	Michigan	86	25	Wisconsin	47
6	Illinois	198	16	Ohio	82	26	Missouri	46
7	New Jersey	162	17	Utah	80	27	Nevada	32
8	Pennsylvania	162	18	Connecticut	71	28	Tennessee	31
9	Washington	148	19	Delaware	69	29	New Hampshire	30
10	Georgia	137	20	Oregon	67	30	Idaho	20

On a per-capita basis, Privacy Shield was important to U.S. states that aren't typically thought of as being home to international data-driven firms, such as Colorado, Connecticut, Delaware, New Hampshire, Virginia, Texas, Tennessee, and Wisconsin.

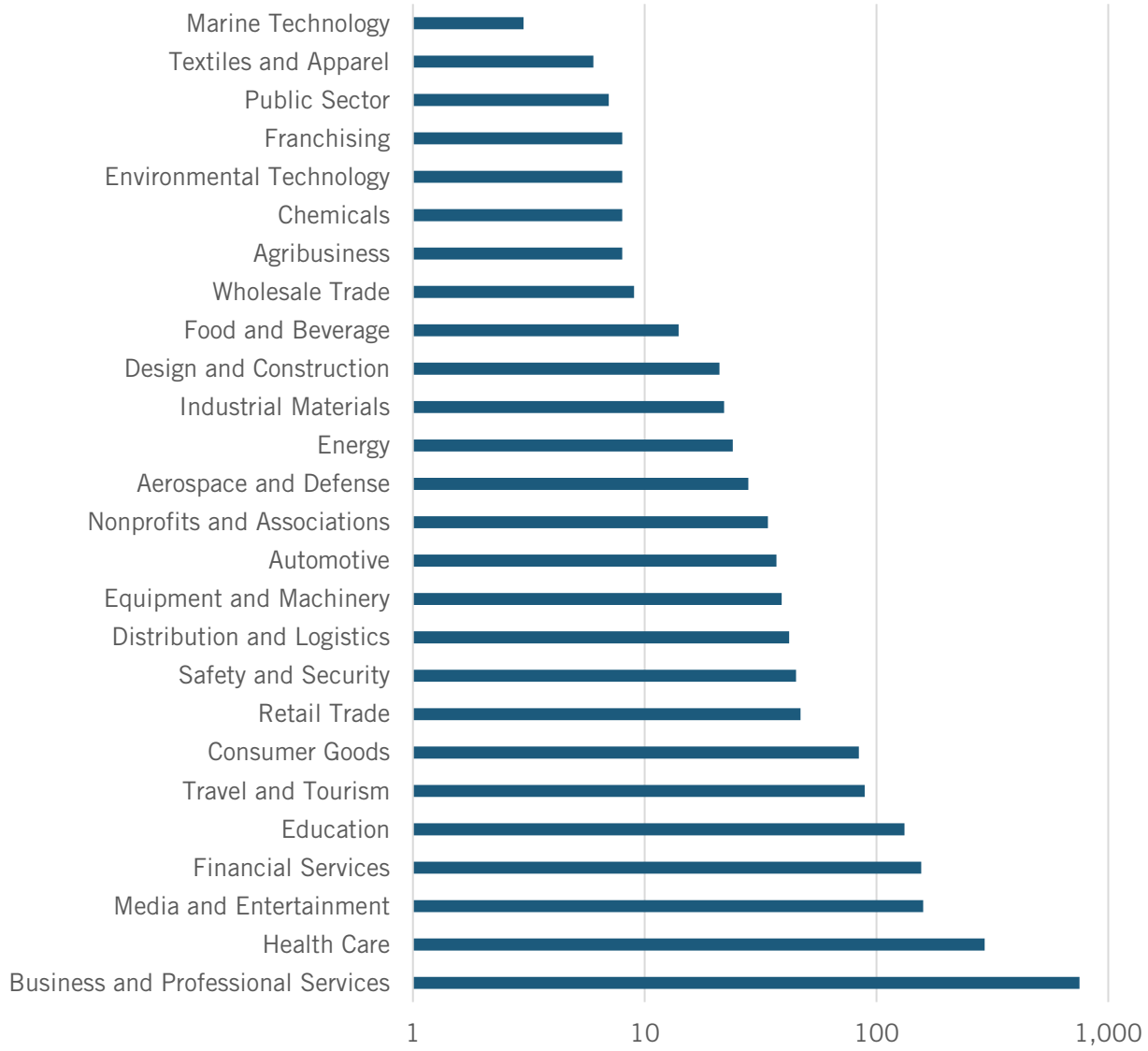
Privacy Shield's relative importance to a range of states (and the District of Columbia) becomes clearer when the data is normalized by population to show how many firms per million used it.[25] In contrast to the general perception that it's solely about California and New York, Privacy Shield was actually more important to several U.S. states (see figure 3). It's especially important to U.S. states that aren't typically thought of as being home to international data-driven firms, such as Virginia (195 firms per million), the District of Colombia (63), Delaware (63), Texas (39), and Tennessee (31). Similarly, when divided into population normalized quintiles, Colorado, Connecticut, New Hampshire, Tennessee, and Wisconsin are all in the top quintile, with Georgia, Illinois, Maryland, New Jersey, and South Carolina part of the fourth quintile.

Figure 3: Privacy Shield firm participation by U.S. state, normalized by population (firms per person)



Privacy Shield was important to the many data-driven firms that underpin trade and innovation in both the United States and Europe. Unsurprisingly, the information and communication technologies industry (2,597 firms) was the largest user of Privacy Shield, followed by business and professional service industries (751).[26] Indicative of how digitalization is increasingly critical to all sectors of the economy, there were many Privacy Shield users from a range of industries, such as health care, media and entertainment, financial services, education, consumer goods, and retail trade (see figure 4, which excludes the ICT industry to better show the diversity of industries that used Privacy Shield).

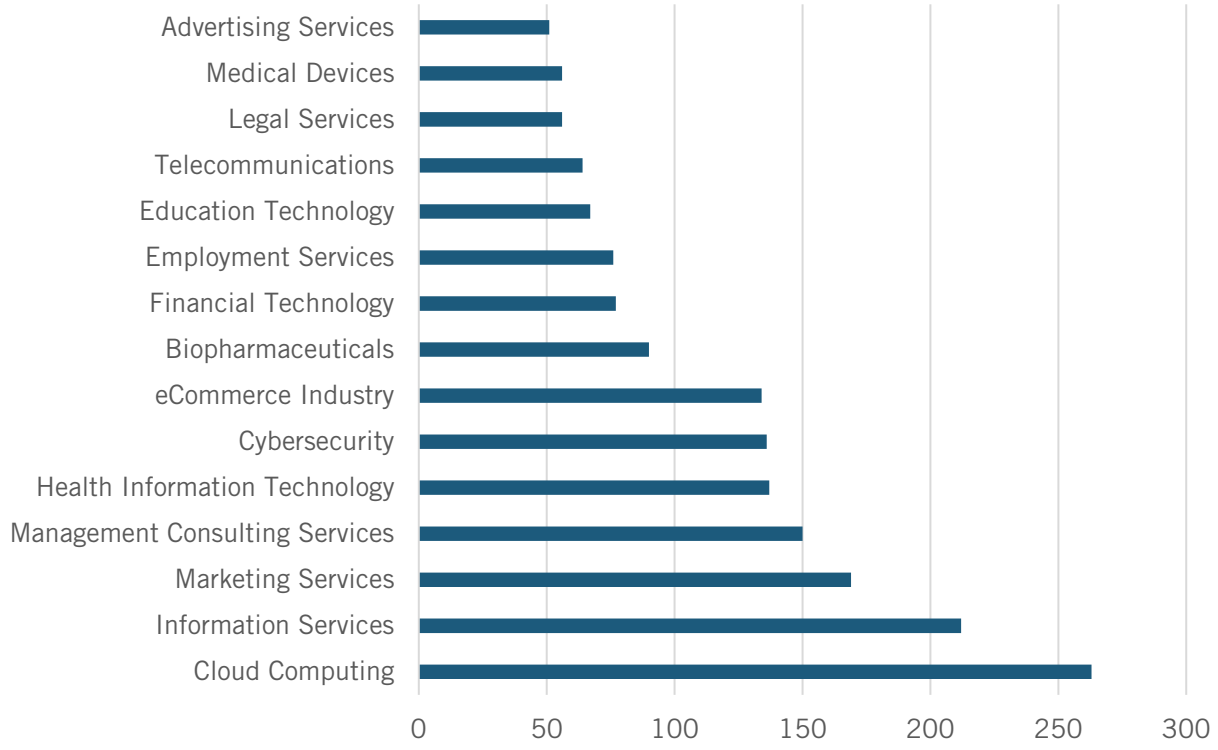
Figure 4: Active Privacy Shield participants by industry



Data flows are the lifeblood of many firms and industries directly engaged in transatlantic trade, but the use of Privacy Shield across support service industries shows its broad indirect impact on trade. It's not surprising that many firm providing business services (751), financial services (156), travel and tourism services (89), and distribution and logistics services(42) used it.

Breaking Privacy Shield use down by sector shows how widely used it was across support services, such as cybersecurity, employment services, freight forwarding, passenger transport, aviation, translation and interpretation services, insurance services, event management, education and training, intelligent transportation systems, accounting services, corporate training, due diligence investigative services, and legal services (see figure 5).

Figure 5: Key sectors using Privacy Shield (number of firms, excluding the software and IT services sectors)



Privacy Shield also highlighted the role data plays in the mining, manufacturing, and agricultural sectors, such as automotive parts (22), metals manufacturers (13), oil and gas (7), building products (5), machinery and tools (5), road vehicles (5), materials handling machinery (4), 3D printing (3), and agricultural equipment and machinery (2).

Similarly, health services, medical devices, and life science research are among the largest and clearest beneficiaries of being able to transfer and use data for trade and innovation. Data increasingly drives drug development and better health outcomes.[27] Privacy Shield's use is indicative of the health sector's growing digitalization, with 137 firms in the health information technology sector, 90 firms in biopharmaceuticals, 56 in medical devices, and 36 in health care services. Never mind that many supporting research and scientific firms would indirectly support these sectors, with 38 firms in the scientific and technical services sector and 8 firms in the scientific laboratory equipment sector using Privacy Shield.

PRIVACY SHIELD'S DEMISE: AN UNCERTAIN, AND POTENTIALLY BROAD, IMPACT ON TRANSATLANTIC TRADE AND INNOVATION

The most immediate result of Privacy Shield's demise is widespread uncertainty about firms' legal obligations in transatlantic data flows. There is probably not a single company today with operations, suppliers, or customers in more than one nation that does not rely on moving data across international borders—whether to gain competitive advantage or as part of normal business operations. The ripple effects of Privacy Shield's demise are spreading through the transatlantic trade and innovation relationship as firms contemplate the implications and redo the cost-benefit analysis. Firms have to recalculate whether the alternatives and the short- and-

long-term legal compliance costs and uncertainty outweigh the commercial benefits of remaining engaged in transatlantic trade and innovation. To make matters worse, the ECJ did not allow any transition or grace period, unlike when the EU Safe Harbor decision was invalidated in 2015. This section details some of the impacts.

Privacy Shield's Demise Impacts All Firms, but It Affects SMEs Disproportionately

The invalidation of Privacy Shield creates a different and more onerous regulatory environment for its many users in Europe, especially SMEs. By invalidating Privacy Shield while upholding SCCs, the ECJ transferred additional accountability to firms, and with it, new costs, risks, and complexity. However, SCCs and BCRs are also facing legal challenges and are far from a perfect fit for a lot of firms. There are no clear, easily accessible, and adaptable alternative data transfer mechanisms for firms to transfer EU personal data to the United States. Any organization engaging in data transfers to the United States—and indeed any non-EU country not covered by an adequacy decision—will need to conduct a comprehensive assessment of the laws and regulations of where they usually transfer and store data and determine what changes they need to make—or whether they simply withdraw from transatlantic trade.

For many large firms, some of the cost of Privacy Shield's demise was pre-paid before the ECJ ruling. SCCs were already a popular way for large firms to meet compliance obligations.[28] Many firms shifted to SCCs after the demise of Safe Harbor, with many others also shifting to them ahead of this latest ECJ ruling. However, the ultimate cost and impact of Privacy Shield's demise is not yet known as the *Schrems II* decision also left SCCs on much less stable ground. For example, data controllers are responsible for determining what constitutes adequate "supplementary measures" (a subsequent ITIF briefing will focus on SCCs). The EDPB's recent recommendations on these supplementary measures provided some clarity, but also considerable complexity, to firms trying to decide what exactly they need to do.[29]

SMEs—the vast majority of Privacy Shield users—on both sides of the Atlantic will be disproportionately impacted as they do not have the resources and expertise to manage complex international legal compliance operations.

Some large firms use BCRs, which perhaps offer more (but far from assured) legal certainty than SCCs, but they're far from a silver bullet for international data transfers. BCRs are simply one tool in the legal toolbox as they're limited in scope in that they only cover intra-firm data transfers, so they are typically used alongside SCCs, which governs data transfers to third parties. Also, BCRs must be approved by a firm's relevant DPA in a long (typically taking two years or more), costly, and uncertain process (given the potential for individual DPAs to assess requirements differently). Thus, BCRs are only feasible for large corporations, and even for them, it's not a straightforward process. Whether its SCCs or BCRs, EU data compliance is expensive and complicated for firms that need to transfer data outside the EU. But ultimately, large firms have the legal, technical, and administrative resources and expertise to adjust—and the economies of scale to absorb or pass these costs on to customers through higher prices.

The remaining options are limited, hardly ideal, and not widely applicable. EU data protection law allows for certain exceptions, or derogations, such as public or economic interests. But

derogations must be determined on an ad hoc basis and are generally insufficient to reach full compliance for international data transfers.

Data localization is the other glaring alternative: firms being forced to transfer EU personal data within the region, which adds its own additional costs and complexities. Ultimately, to mitigate the risks data transfers may present, firms may use a combination of different legal mechanisms. Either way, the web of changing and uncertain compliance activity is likely to complicate EU operations for even the largest firms engaging in transatlantic data flows.

SMEs—the vast majority of Privacy Shield users—on both sides of the Atlantic will be disproportionately impacted as they do not have the resources and expertise to manage complex international legal compliance operations. Cecilia Bonefeld-Dahl, director general of DIGITALEUROPE, was right when she called the decision a "bombshell for small businesses."[30] For the one-third of Privacy Shield firms that had less than $5 million in revenue, it'll no doubt be difficult to justify spending tens or hundreds of thousands on legal advice and changes to operational and IT services.[31] This reinforces the point that when thinking about Privacy Shield, U.S. and EU policymakers should have an SME in mind—not Facebook, Google, or some other large firm that saw this judgment coming and shifted all operations to SCCs and other legal tools.

SMEs that can't transfer data to the United States will be affected in two clear ways. First, making it harder and more expensive for SMEs to transfer and use data will reduce the likelihood, scale, and extent they engage in trade. Reduced economies of scale and scope will affect SME's ability to thrive and, perhaps, survive, especially in the era of COVID-19 wherein digital and digitally enabled goods and services trade is more essential than ever. Second, SME's competitiveness will decrease as it's harder and more expensive for them to engage in transatlantic trade and innovation. Both impacts directly undermine a central benefit of the Internet and digital trade: reducing the impact that geography has on trade and opening up trade to more individuals and firms from around the world.

Impact on Innovation

Privacy Shield's demise will undermine transatlantic innovation as it will be harder and more expensive, if not impossible, for firms—especially SMEs—to gain exposure and benefit from the ideas, research, technologies, and best practices that accompany data transfers and the innovative new goods and services that rely on data. Organizations use data to create better insights, which, in turn, lead to innovation. Businesses use data to enhance research and development, develop new products and services, create new production or delivery processes, improve marketing, and establish new organizational and management approaches.[32] Companies of all types and sizes are sharing in the benefits of data innovation. For example, a 2014 survey found that data analytics are important to 60 percent of U.S. and European businesses with 50 or fewer employees.[33]

For example, barriers to the exchange of personal medical and genomic data could prevent firms from engaging in medical research and large international medical studies. It could prevent the transfer of data as part of cutting-edge diagnostic services, thereby increasing health care costs and time demands on doctors. It could prevent biopharmaceutical firms from conducting and aggregating data from clinical trials spread throughout the United States and Europe in order to get enough of the right candidates to make research progress, especially on rare diseases. By erecting barriers to the exchange of medical information, even anonymous data, countries'

restrictive data transfer policies harm not only their own citizens but people around the world, all of whom benefits from the advancement of medical science.

Health services and biopharmaceutical firms clearly need—and demand—some legal framework given how many used Privacy Shield. For example, in February 2020, leading health researchers called for an international code of conduct for genomic data following the end of their first-of-its-kind international data-driven research project.[34] The project used a purpose-built cloud service that stored 800 terabytes of genomic data on 2,658 cancer genomes across 13 data centers on 3 continents.[35] The collaboration and use of cloud computing were transformational in enabling large-scale genomic analysis. If policymakers want more international collaboration such as this, including around COVID-19, then they need legal frameworks such as Privacy Shield to manage health data transfers.

The use of data analytics does not mean the unrestricted use of personal data. Cross-border data transfers do not allow firms to abdicate their responsibilities to process data according to local data protection laws, such as GDPR.

It's important to highlight that data-driven innovation, such as the use of data analytics, does not mean the unrestricted use of personal data. Cross-border data transfers do not allow firms to abdicate their responsibilities to process data according to local data protection laws. U.S. firms, for example, have to abide by GDPR's requirements wherever they transfer and process data. Over the last two decades, U.S. and EU firms have used progressively stronger mechanisms (in Safe Harbor and Privacy Shield) to engage in transatlantic digital trade and innovation, while also adjusting for the huge changes brought on by technological innovation and regulation, especially GDPR in Europe. Experience shows that both the United States and EU can work together to develop new and better frameworks to ensure firms are held accountable and responsible for how they collect, manage, use, and transfer EU personal data. Such transatlantic innovation is mutually beneficial given it makes them more competitive in the growing global digital economy. Ultimately, failing to repair or replace Privacy Shield will slow transatlantic collaboration and innovation.

CONCLUSION

The major challenge ahead lies in reconciling different government surveillance systems, both between the United States and the EU and between EU member states themselves. This problem is not one the private sector can solve on its own. It is highly unlikely the United States will make changes to its own surveillance laws that would fully align the EU's demands—nor should the EU expect the United States to make such a change. But there may be ways to improve transparency and oversight of respective surveillance processes. This isn't the first time both sides have had to bridge their differences. They've done it before and will hopefully do it again, in some way, shape, or form. As they proceed, policymakers in Europe and the United States should be reminded they share more in common than they may even care to admit—even when it involves contentious issues—and their shared values stand in stark contrast to those of authoritarian digital powers such as China and Russia.

If European nations are willing to accept this information and assistance, they should not then turn around and retaliate against the United States for its policies and practices.

Moreover, Europe should recognize that it has been a significant beneficiary of U.S. surveillance practices. Indeed, the EU is rarely critical of U.S. intelligence capabilities when it is offered for its own needs. For example, the National Security Agency (NSA) has used Section 702 Foreign Intelligence Surveillance Act (FISA) data requests to help prevent terrorist attacks in EU nations or locate and prosecute known extremists operating on European soil, including one with connections to the 2015 Paris attacks.[36] If European nations are willing to accept this information and assistance, they should not then turn around and retaliate against the United States for its policies and practices.

An interoperable privacy mechanism is critical to the transatlantic economic relationship. Privacy Shield, and Safe Harbor before it, made the two different approaches to personal data protections compatible. Although both U.S. and EU authorities have indicated that discussions are underway to explore the potential for a new framework to serve the same purpose as Safe Harbor and Privacy Shield, it seems firms that engage in transatlantic data flows will not have a direct substitute for the foreseeable future.[37] This is unfortunate because complex firm-level compliance requirements are a poor substitute for international agreements that embed shared data protection principles and processes alongside a recognition of the value of free data flows.

Unless EU and U.S. policymakers want to de facto exclude SMEs from the global digital economy, there needs to be a clear, reasonable, and accessible mechanism for them to account for data protection concerns.

Until parameters for adequate safeguards are clarified, this uncertainty will hinder U.S. and EU organizations' cross-border operations and undermine transatlantic trade and innovation. Furthermore, unless EU and U.S. policymakers want to de facto exclude SMEs from the global digital economy, there needs to be a clear, reasonable, and accessible mechanism for them to account for data protection concerns. Establishing a new transatlantic data transfer mechanism should be a top priority for the new Biden administration.

It's important EU and U.S. policymakers realize the enormous economic and innovation stakes involved as they consider next steps. Severing transatlantic digital engagement and cooperation will accelerate the fragmenting of the global digital economy—it'd reflect a fundamental fracture between two key players, which would hurt everyone by multiples of what is at stake between the United States and Europe. Transatlantic data flows are the critical international extension to their related domestic efforts to help their people, firms, and industries use data and digital tools to become more productive and innovative. The role and importance of transatlantic data protection and flows will only grow. Forward-looking policymakers on both sides of the Atlantic need to recognize this reality and its trajectory in ensuring this is supported through a new legal data transfer mechanism.

Acknowledgments

This report was made possible in part by generous support from Facebook. The authors wish to thank Kevin Gawora for his assistance in providing data, research, and graphics. Any errors or omissions are the authors' responsibility alone.

About the Authors

Nigel Cory (@NigelCory) is an associate director covering trade policy at ITIF. He focuses on cross-border data flows, data governance, and intellectual property, and how they each relate to digital trade and the broader digital economy.

Daniel Castro (@CastroTech) is vice president at ITIF and director of its Center for Data Innovation. He writes and speaks on a variety of issues related to information technology and Internet policy, including privacy, security, intellectual property, Internet governance, e-government, and accessibility for people with disabilities.

Ellysse Dick (@Ellysse_D) is a research fellow in tech and cyber policy at ITIF. Her research focuses on AR/VR innovation and policy including privacy, safety, and accountability.

About ITIF

The Information Technology and Innovation Foundation (ITIF) is a nonprofit, nonpartisan research and educational institute focusing on the intersection of technological innovation and public policy. Recognized as the world's leading science and technology think tank, ITIF's mission is to formulate and promote policy solutions that accelerate innovation and boost productivity to spur growth, opportunity, and progress.

For more information, visit us at www.itif.org.

ENDNOTES

1. Daniel Castro and Alan McQuinn, "Cross-Border Data Flows Enable Growth in All Industries" (ITIF, February, 2015), https://itif.org/publications/2015/02/24/cross-border-data-flows-enable-growth-all-industries.
2. *Information on U.S. Privacy Safeguards Relevant to SCCs and Other EU Legal Bases for EU-U.S. Data Transfers after Schrems II*, U.S. Department of Commerce, U.S. Department of Justice, and the Office of the Director of National Intelligence (white paper, September, 2020), https://www.commerce.gov/sites/default/files/2020-09/SCCsWhitePaperFORMATTEDFINAL508COMPLIANT.PDF.
3. *European Data Protection Board - 41st Plenary session: EDPB adopts recommendations on supplementary measures following Schrems II*, European Data Protection Board (EDPB), November 11, 2020, https://edpb.europa.eu/news/news/2020/european-data-protection-board-41st-plenary-session-edpb-adopts-recommendations_en.
4. "Adequacy decisions: How the EU determines if a non-EU country has an adequate level of data protection," European Commission, https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en.
5. European Commission and the United States, "EU Commission and United States agree on new framework for transatlantic data flows: EU-US Privacy Shield," press release, February 2, 2016, https://ec.europa.eu/commission/presscorner/detail/en/IP_16_216.
6. Federal Trade Commission Chairwoman Edith Ramirez, "Statement of FTC Chairwoman Edith Ramirez on the EU-U.S. Privacy Shield Agreement," press release, February 2, 2016, https://www.ftc.gov/news-events/press-releases/2016/02/statement-ftc-chairwoman-edith-ramirez-eu-us-privacy-shield.
7. "Self-Certification Information," Privacy Shield website, https://www.privacyshield.gov/article?id=Self-Certification-Information; U.S. Department of Commerce, "EU-U.S. Privacy Shield Framework Principles," https://www.privacyshield.gov/servlet/servlet.FileDownload?file=015t00000004qAg.
8. "FAQs: General," Privacy Shield website, https://www.privacyshield.gov/article?id=General-FAQs.
9. European Commission, "Third annual review of the functioning of the EU-U.S. Privacy," October 23, 2019, https://ec.europa.eu/info/sites/info/files/report_on_the_third_annual_review_of_the_eu_us_privacy_shield_2019.pdf.
10. See: U.S. Federal Trade Commission, "FTC Finalizes Privacy Shield Settlement with Ortho-Clinical," press release, July 13, 2020, https://www.ftc.gov/news-events/press-releases/2020/07/ftc-finalizes-privacy-shield-settlement-ortho-clinical; U.S. Federal Trade Commission, "FTC Gives Final Approval to Settlement with Background Services Provider over Allegations Related to Privacy Shield," press release, March 23, 2020, https://www.ftc.gov/news-events/press-releases/2020/03/ftc-gives-final-approval-settlement-background-services-provider; U.S. Federal Trade Commission, "FTC Finalizes Settlements with Four Companies Related to Privacy Shield Allegations," press release, January 29, 2020,https://www.ftc.gov/news-events/press-releases/2020/01/ftc-finalizes-settlements-four-companies-related-privacy-shield; U.S. Federal Trade Commission, "FTC Finalizes Settlements with Five Companies Related to Privacy Shield Allegations," press release, January 16, 2020, https://www.ftc.gov/news-events/press-releases/2020/01/ftc-finalizes-settlements-five-companies-related-privacy-shield; U.S. Federal Trade Commission, "FTC Finalizes Settlement with California Tech Company Related to Privacy Shield," press release, January 9, 2020, https://www.ftc.gov/news-events/press-releases/2020/01/ftc-finalizes-settlement-california-tech-company-related-privacy.

11. "ICDR-AAA EU-U.S. Privacy Shield and Swiss-U.S. Privacy Shield Program Independent Recourse Mechanism," International Center for Dispute Resolution and the American Arbitration Association, https://go.adr.org/privacyshield.html.
12. Castro and McQuinn, "Cross-Border Data Flows Enable Growth in All Industries."
13. U.S. Secretary of Commerce Wilbur Ross, "Schrems II Ruling and the Importance of EU-U.S. Data Flows," press release, July 16, 2020, https://www.commerce.gov/news/press-releases/2020/07/us-secretary-commerce-wilbur-ross-statement-schrems-ii-ruling-and.
14. Robert D. Atkinson and Stephen Ezell, "Promoting European Growth, Productivity, and Competitiveness by Taking Advantage of the Next Digital Technology Wave" (ITIF, March 26, 2019), https://itif.org/publications/2019/03/26/new-itif-report-commissioned-incoming-eu-council-presidency-offers-policy.
15. Ibid.
16. The majority of firms stated separating personal and non-personal data was costly or very costly. Consistent across sectors, this finding has broad ramifications for the digital economy. It means that if a firm is unable to separate personal and non-personal data, a restriction on cross-border transfers of personal or personally identifiable data might in effect become a measure affecting all types of data. This contrasts with the view shared by some advocates and policymakers that data privacy measures only affect a very small and specific category of data. Francesca Casalinii and Javier López Gonzálezi, *Trade and Cross-Border Data Flows* (The Organisation for Economic Cooperation and Development, January 23, 2019), https://doi.org/10.1787/b2023a47-en.
17. Drew Medway and Jeremy Greenberg, "New FPF Study: More Than 250 European Companies are Participating in Key EU-US Data Transfer Mechanism" (Future of Privacy Forum, July 14, 2020), https://fpf.org/2020/07/14/new-fpf-study-more-than-250-european-companies-are-participating-in-key-eu-us-data-transfer-mechanism/; Jeremy Greenberg, "New FPF Study Documents More Than 150 European Companies Participating in the EU-US Data Transfer Mechanism" (Future of Privacy Forum, December 20, 2018), https://fpf.org/2018/12/20/new-fpf-study-documents-more-than-150-european-companies-participating-in-the-eu-us-data-transfer-mechanism/.
18. List of active firms using Privacy Shield: https://www.privacyshield.gov/list.
19. Ibid.
20. "IAPP-EY Annual Governance Report 2019," International Association of Privacy Professionals, 2019, https://iapp.org/resources/article/iapp-ey-annual-governance-report-2019/.
21. James Sullivan, "The EU-U.S. and Swiss-U.S. Privacy Shield Frameworks: Why They Matter," U.S. Department of Commerce Tradeology blog post, September 13, 2019, https://blog.trade.gov/2019/09/13/the-eu-u-s-and-swiss-u-s-privacy-shield-frameworks-why-they-matter/.
22. Ibid.
23. Future of Privacy Forum staff performed a web search for each current company by name, checking the location of the company's headquarters on a combination of public databases such as LinkedIn, CrunchBase, Bloomberg, and companies' own websites. A company that listed its headquarters in an EU member state or in Switzerland was counted as a match; companies that merely had a prominent EU office or were founded in an EU member state were not counted. Drew Medway and Jeremy Greenberg, "New FPF Study: More Than 250 European Companies are Participating in Key EU-US Data Transfer Mechanism" (Future of Privacy Forum, July 14, 2020), https://fpf.org/2020/07/14/new-fpf-study-more-than-250-european-companies-are-participating-in-key-eu-us-data-transfer-mechanism/;
24. This is a simple, sample analysis, based on a search of firms with "US," "USA," "international," or "global" in their title.
25. Total number of firms in a state/state population (in millions).

26. Industry is the broadest category, which is subsequently broken down into sector.
27. Joshua New, "The Promise of Data-Driven Drug Development" (Center for Data Innovation, September 18, 2019), https://www.datainnovation.org/2019/09/the-promise-of-data-driven-drug-development/; Nigel Cory and Philip Stevens, "Building a Global Framework for Digital Health Services in the Era of COVID-19" (ITIF, May 26, 2020), https://itif.org/publications/2020/05/26/building-global-framework-digital-health-services-era-covid-19.
28. "IAPP-EY Annual Governance Report 2019," International Association of Privacy Professionals, 2019, https://iapp.org/resources/article/iapp-ey-annual-governance-report-2019/.
29. *European Data Protection Board - 41st Plenary session: EDPB adopts recommendations on supplementary measures following Schrems II*, European Data Protection Board (EDPB), November 11, 2020, https://edpb.europa.eu/news/news/2020/european-data-protection-board-41st-plenary-session-edpb-adopts-recommendations_en.
30. Cecilia Bonefeld-Dahl, "Schrems II ruling puts European recovery at risk," *The Parliament,* September 15, 2020, https://www.theparliamentmagazine.eu/news/article/schrems-ii-ruling-puts-european-recovery-at-risk-22391.
31. James Sullivan, "The EU-U.S. and Swiss-U.S. Privacy Shield Frameworks: Why They Matter," U.S. Department of Commerce Tradeology blog post, September 13, 2019, https://blog.trade.gov/2019/09/13/the-eu-u-s-and-swiss-u-s-privacy-shield-frameworks-why-they-matter/.
32. Christian Reimsbach-Kounatze and Brendan Van Alsenoy, "Exploring Data-Driven Innovation as a New Source of Growth"(Paris: Organization for Economic Co-operation and Development, June 2013), http://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=DSTI/ICCP(2012)9/FINAL&docLanguage=En.
33. Victoria Espinel, "Executive Survey Shows the Benefits of Data Innovation Across the Whole Economy," TechPost, December 10, 2014, http://techpost.bsa.org/2014/12/10/executive-survey-the-shows-the-benefits-of-data-innovation-across-whole-economy/.
34. Mark Phillips et al., "Genomics: data sharing needs an international code of conduct," *Nature,* February 5, 2020, https://www.nature.com/articles/d41586-020-00082-9.
35. P.J. Campbell et al., The ICGC/TCGA Pan-Cancer Analysis of Whole Genomes Consortium, Pan-cancer analysis of whole genomes, *Nature*, 578, 82–93 (2020). https://doi.org/10.1038/s41586-020-1969-6.
36 *Information on U.S. Privacy Safeguards Relevant to SCCs and Other EU Legal Bases for EU-U.S. Data Transfers after Schrems II*, U.S. Department of Commerce, U.S. Department of Justice, and the Office of the Director of National Intelligence (white paper, September, 2020), https://www.commerce.gov/sites/default/files/2020-09/SCCsWhitePaperFORMATTEDFINAL508COMPLIANT.PDF.
37. "Joint Press Statement from European Commissioner for Justice Didier Reynders and U.S. Secretary of Commerce Wilbur Ross," press release, August 10, 2020, https://ec.europa.eu/info/news/joint-press-statement-european-commissioner-justice-didier-reynders-and-us-secretary-commerce-wilbur-ross-7-august-2020-2020-aug-07_en.