ITIF | INFORMATION TECHNOLOGY & INNOVATION FOUNDATION

How to Build Back Better the Transatlantic Data Relationship

NIGEL CORY AND ELLYSSE DICK I MARCH 2021

Transatlantic data flows are essential to organizations of all sizes and industries—not just large technology firms. The EU and United States must establish clear, consistent legal mechanisms for data transfers so both sides can thrive in an increasingly digital global economy.

KEY TAKEAWAYS

- Transatlantic digital relations are in crisis. With the EU-U.S. Privacy Shield invalidated and other legal mechanisms for transferring data under scrutiny, there is a serious risk of a de facto data localization policy hurting both sides.
- Cross-border data flows are critical for firms across the whole economy—from manufacturing and transport to financial and Internet services. Millions of jobs and a large share of transatlantic trade thus depend on strong digital ties.
- Restrictions on data flows disproportionately affect SMEs, which often rely on digital tools to reach new customers and grow their businesses and are less likely than large firms to have the resources to navigate complex legal requirements.
- Beyond trade and commerce, government agencies also depend on cross-border data flows for purposes ranging from regulatory oversight to investigating crimes, protecting national security, and more.
- Policymakers should rebuild a robust framework for transatlantic data flows with a successor to the Privacy Shield, new GDPR-compliant transfer mechanisms, and improved law enforcement cooperation to access electronic evidence.
- Fully harmonizing policies is unrealistic, but the EU and United States should be pragmatic and forge a broad cooperative agenda based on shared values as a strategic counterweight to authoritarian digital powers like China and Russia.
- A pragmatic U.S.-EU digital alliance would be mutually beneficial in influencing global data-sharing frameworks, AI regulation, electronic IDs, standards setting, investment screening, and export controls for data and digital technologies.

CONTENTS

INTRODUCTION

Cross-border data transfers—involving both personal and nonpersonal data—enable firms of all sectors and sizes to engage in transatlantic commerce. Government agencies also need firms to be able to transfer data across borders as part of financial oversight, drug approval, law enforcement, counterterrorism, and other responsibilities. The European Union's (EU) General Data Protection Regulation (GDPR) was supposed to bring a more predictable and harmonized approach to data protection within the EU and provide a range of tools for firms to transfer EU personal data overseas. Instead, successive court challenges have made it harder and more complex—and without political intervention, the situation will devolve into an irrevocably severed transatlantic digital relationship. EU and U.S. policymakers need to step in and avoid taking a narrow and legalistic approach to the challenges facing transatlantic data flows and instead build back better in terms of creating a new and efficient transatlantic data framework.

Transatlantic digital policy cooperation has faced a decade of turmoil—but it has never been as dire as now. For the second time, the EU's top court (in the *Schrems II* case) invalidated the framework that manages transatlantic transfers of EU personal data (the EU-U.S. Privacy Shield), after finding that U.S. laws do not sufficiently protect data about EU citizens stored in the United States.[1] The challenge for policymakers is to reconcile the EU's data protection laws with U.S. surveillance policies and practices. Unfortunately, the current stalemate makes transatlantic data transfers increasingly difficult, if not impossible, and imperils other major transatlantic interests around commercial access to data for trade and innovation and government cooperation on law enforcement, national security, and regulatory issues.

It is impossible to fully localize any digital process, good, or service without some level of impact or disruption. The underlying data storage infrastructure does not necessarily rely on the ability to exchange data across borders, but the services built on it certainly do.

Potential legal challenges and restrictive policy proposals by the European Data Protection Board (EDPB) and others are raising concerns about whether firms will still be able to use standard contractual clauses (SCCs), which are the last broadly accessible legal tool for U.S. and EU firms to transfer EU personal data.[2] Indicative of where this is heading, the EDPB has already issued guidance that "strongly encourages" EU institutions considering new contracts with service providers "to avoid processing activities that involve transfers of personal data to the United States."[3] Another major (and restrictive) policy reaction is making firms (no matter how big or small) responsible for assessing each storage destination's surveillance and government access laws—and that the hypothetical potential for any data disclosure is reason enough to not transfer EU personal data. This is an unrealistic legal and practical threshold for firms to meet given it fails to account for the actual potential of government access and the difficulty in understanding different and constantly changing legal frameworks around the world.

Transatlantic data flows may be suddenly severed through another legal challenge or reduced over time as new restrictive requirements are defined and enforced against firms by the EDPB and individual EU member state data protection authorities. Within this challenge of rebuilding the transatlantic digital relationship, it is important to reinforce the central point that data transfers, data-driven innovation, and data protection are not mutually exclusive. Firms cannot undermine local data privacy, protection, and other related laws by transferring data to another country

because they are held accountable for how they manage data, meaning local legal requirements travel with the data, regardless of where it is stored and processed.[4] This contrasts with the European focus on the geography of data storage. Making international transfers of EU personal data increasingly difficult, costly, and legally uncertain leaves local data storage and processing as the only viable option, which is the end goal for many privacy advocates and policymakers in Europe. As it stands, the EU's approach to data privacy is creating the world's largest de facto data localization framework. The EU's only peer is China's broad and growing explicit data localization regime, with laws that make local data storage and processing the norm and transfers the exception. At some point, the pressure on U.S. policymakers to reciprocate with equally restrictive rules preventing EU firms such as Volkswagen, Phillips, Siemens, and Sanofi from transferring data from their U.S. operations to their EU headquarters will become significant enough to spur retaliatory action.

It is infeasible for firms to build out local human resources, management, research and development (R&D), regulatory compliance, and information technology (IT) and customer support services in each and every market that has local data storage requirements. Such requirements undermine the ability of all firms—especially globally engaged ones—to leverage the distributed power of the Internet and centralized IT systems to manage local, regional, and global business operations and compliance activities. It is impossible to fully localize any digital process, good, or service without some level of impact or disruption. While it may be technically possible for a company—particularly a large one—to fully localize data storage, there would be major disruptions and changes to the type and quality of services, as well as limits on the use of technologies such as artificial intelligence (AI) wherein algorithms improve with larger datasets. The underlying data storage infrastructure does not necessarily rely on the ability to exchange data across borders, but the services built on it certainly do.

Transatlantic data flows have enormous economic implications. Two-way EU-U.S. digital trade grew from an estimated $166 billion in 2005 to $292 billion in 2015. The sectoral case studies in this report show what is at stake. Despite the popular misconception that data flows only benefit search engines and social networks, severing transatlantic data flows would have wide-reaching impacts across the global economy. Yet, some EU policymakers think that restricting or cutting off data flows and digital trade with the United States is a good thing as it aligns with their "digital sovereignty" goals, believing that if it hurts leading U.S. tech firms, then it must be good—without realizing or appreciating the broader and much larger costs. This stance ignores the fact that doing so would also hurt the hundreds of European firms that used Privacy Shield and SCCs to manage data transfers between their headquarters and offices and operations in the United States.[5] Unfortunately, this protectionist impulse is also evident in Europe's ongoing effort to define its own digital economy framework, such as the European Commission's data strategy and its Data Governance Act.[6]

But the impact is not only trade and innovation-related—governments on both sides of the Atlantic depend on firms being able to transfer data as part of day-to-day regulatory requirements, whether for financial oversight of the banking, financial, and payments sectors (for financial stability, counter-terrorism financing, or anti-money-laundering purposes) or the review of clinical trials by respective public health agencies. This is obviously in addition to law enforcement and national security cooperation.

This report starts by outlining the history of the transatlantic digital relationship to show how both the EU and Unites States have continuously recognized the value in working together to address issues as they arise. However, this report also makes the case that this relationship should not be based on troubleshooting, but ideally, on a broader digital agenda, given both sides share many values and interests. It then analyzes estimates of the economic value of transatlantic digital trade, before providing a series of sectoral case studies to show how firms in a diverse range of sectors—from automotive and other advanced manufacturers to life sciences to consumer Internet services to financial and banking services—use transatlantic data flows.

Finally, this report provides recommendations to build a better, stronger, and broader transatlantic digital relationship:

1. Policymakers should negotiate a new Privacy Shield. Long term, the two sides could work toward legislation and a treaty agreement that would codify some of their commitments. In an ideal world, the United States and Europe would work together with like-minded countries to develop a "Geneva Convention for Data," which would create consensus on issues around government access to data.
2. The EU should redouble efforts to build new data transfer mechanisms under GDPR. This would be in addition to the more immediate need to make existing legal tools (SCCs and binding corporate rules) clear, reasonable, and accessible.
3. The United States and EU should conclude negotiations to improve transatlantic access to electronic evidence for law enforcement investigations.
4. The EU and United States should build a broader agenda for pragmatic cooperation on data and digital policy issues—one based on "digital realpolitik." Such cooperation would be economically beneficial to both sides given their extensive economic connections. Furthermore, while there are points of conflict, overall, their shared values stand in stark contrast to those of authoritarian digital powers such as China and Russia. Such an agenda could work on how to develop data sharing frameworks; develop and apply the appropriate regulation of AI, such as via algorithmic accountability; develop interoperable electronic identity systems; build pre-standardization cooperation for new and emerging technologies; develop a coordinated strategy to counter China's efforts to unduly influence international standards setting for AI and digital policies; and cooperate and coordinate investment screening and export controls that increasingly deal with data and digital technologies.

THE EU AND UNITED STATES NEED TO REPAIR AND REINFORCE THE DIGITAL TRANSATLANTIC RELATIONSHIP

Despite constant pressure over the last decade—and as reactions to the Snowden revelations continue to reverberate—both the EU and United States have kept the transatlantic data and digital relationship going. Despite the challenges, there is largely bipartisan support in the United States for EU-U.S. digital engagement.

There was substantial continuity across the Obama and Trump administrations, which is likely to continue in the Biden administration. In 2014, President Obama issued presidential policy directive number 28 on "Signals Intelligence Activities," which included safeguards for non-U.S. persons in signals intelligence.[7] Privacy Shield was signed under President Obama, and was also

supported by the Trump administration. The U.S. Federal Trade Commission enforced Privacy Shield throughout both administrations. Meanwhile, the U.S. Congress continues to debate a comprehensive U.S. data privacy bill that would no doubt improve the overall context for engagement with the EU. However, data privacy legislation would not address the fundamental disagreement over U.S. government surveillance that is at the heart of *Schrems II*.

Without political intervention, it is likely that transatlantic data transfers will eventually be cut off.

Given this, rebuilding a strong transatlantic relationship will require action on both sides. Most of the focus has been on the United States, which has already made changes to account for EU concerns and signaled its willingness to consider further changes. Yet, ongoing conflict over EU policy remains. The United States should take into consideration European concerns as it updates its laws and policies around government access to data and data protection. However, the EU should also consider policy and legal reforms to GDPR and other digital policies as part of constructive efforts to build both short- and long-term tools to address both new and ongoing issues regarding international data governance. EU member states also need to be consistent in addressing data privacy and surveillance issues. National security is not a European Commission or EU competency, so doing so will require EU member engagement. If the EU continues to take a largely hands-off approach about the need to address all related issue—not just privacy, but trade and national security—it will lead to ruin as it leaves privacy advocates, the EDPB, and the courts in the driver's seat of a critically important part of the transatlantic relationship.[8] Without political intervention, it is likely that transatlantic data transfers will eventually be cut off.

The stakes involved in building a successful transatlantic digital relationship are already high, but they grow even higher, given the many global debates about data and digital technologies. If the EU and United States want to truly work together on these issues—as the European Commission frequently calls for—they both need to show that they can address their own issues in a way that presents a model for other countries. Absent such an outcome, calls for transatlantic cooperation on global issues would be seen as meaningless.

THE ROLE AND VALUE OF DATA FLOWS AND DIGITAL TRADE IN THE TRANSATLANTIC RELATIONSHIP

Digital trade—including both digital and digitally enabled services—is an increasingly important component of the global economy. As the sectoral case studies show, cross-border transfers of data underpin virtually all business processes in international trade and investment.[9]

Estimating the value of transatlantic data flows and digital trade is challenging.[10] For example, approximating value by the aggregate volume of data transfers has significant limitations.[11] The value of data depends on its content.[12] Data is also highly context specific. An individual person's data may be valuable to that person, but only hold broader value when aggregated with data from many other individuals and other sources of data. The value of data is temporal in that it may only become valuable when used as part of future analysis. Furthermore, some data flows may be non-monetized—representing intra-company transfers that are commercially valuable, but not captured in a formal transaction. Similarly, gross domestic product (GDP) and other economic statistics do not measure the value of consumer surplus, such as when consumers access digital goods and services at no financial cost.[13] While estimating the value of the specific underlying data and its

transfer is difficult, it is clear that continuous data aggregation and analysis by firms creates enormous value, in what the Organization for Economic Cooperation and Development (OECD) calls the "global data value cycle."[14]

While precise, comprehensive, and consistent measurement of the value of data and digital trade in and between the United States and EU is not yet possible, there are a range of estimates that support what we know anecdotally—that data and digital trade represent an important and fast-growing part of the global economy.[15] In August 2020, the U.S. Department of Commerce's report "New Digital Economy Estimates" calculated that the digital economy accounted for 9 percent of U.S. GDP in 2018, which ranked it just below the manufacturing sector (which accounted for 11.3 percent) and just above finance and insurance (7.6 percent).[16] From 2006 to 2018, the U.S. digital economy's real value added grew at an annual rate of 6.8 percent. It supported 8.8 million jobs, which represented 5.7 percent of U.S. total employment.[17] In Europe, the value added from the information and communication technology (ICT) sector in 2017 was equivalent to at least 3.9 percent of GDP, 2.5 percent of total employment, and 18.6 and 20.6 percent of the total R&D personnel and researchers in the EU, respectively.[18] Employment in the EU's ICT services sector grew by 22.7 percent between 2012 and 2017.[19] And as of 2020, one of the fastest-growing aspects of the global digital economy, the "app economy," accounts for over 2 million jobs in the U.S. and EU alike.[20]

Data and digital trade represent an important and fast-growing part of the global economy.

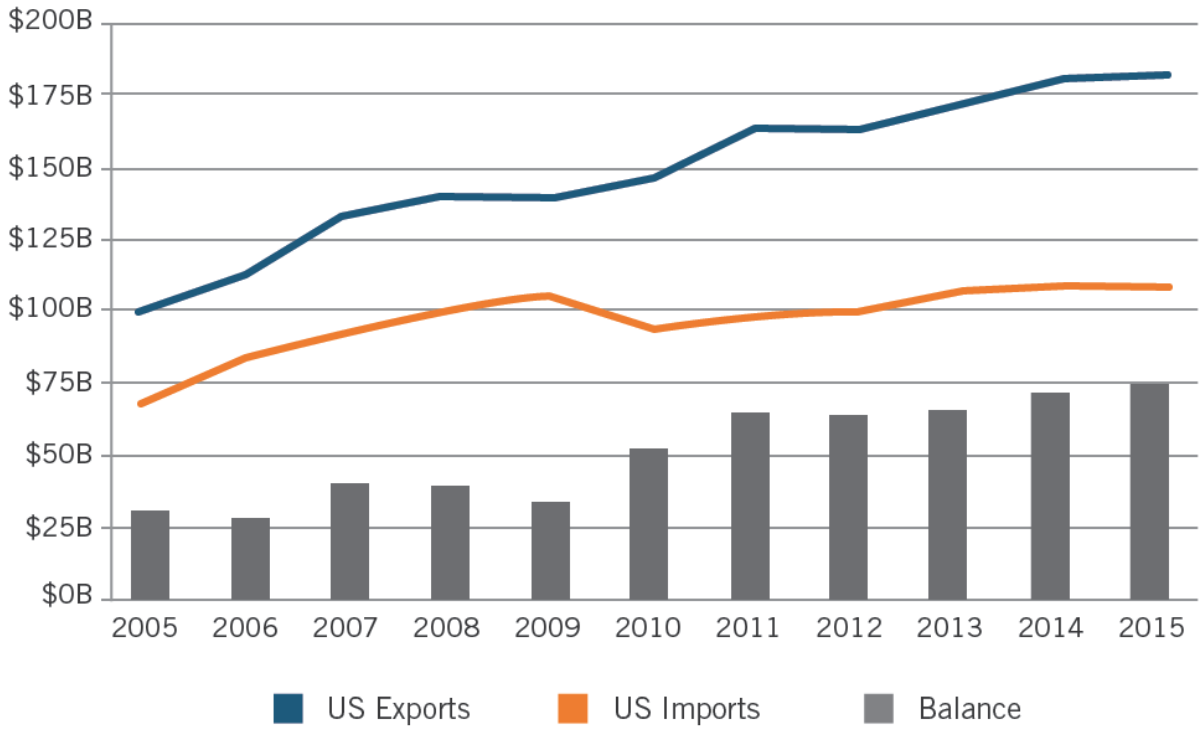
Traditional trade statistics capture some of the EU-U.S. digital trade relationship, but not all.[21] The United States is both the largest (non-EU) market for Europe's digitally enabled services and its largest supplier.[22] Indicative of this, about half of all data flows in both the United States and Europe are transatlantic transfers.[23] In 2018, digitally enabled services accounted for the majority of U.S. services exports (55 percent), nearly half of U.S. services imports (48 percent), and a full 69 percent of U.S. global surplus in services.[24] The U.S. also accounted for 32 percent of exports and 39 percent of imports of digitally enabled services from and to the EU.[25]

The U.S. Department of Commerce's ICT and potential-ICT based digital trade data provides the broadest, and most recent, estimate of transatlantic digital trade, which in total, was worth $295 billion in 2018. It captures both ICT services that are used to facilitate information processing and communication (e.g., computer and telecommunication services) and potentially ICT-enabled services that can predominantly be delivered remotely over ICT networks, such as financial, insurance, intellectual property, professional and management services, and R&D services, among others.[26] The data estimates that, in 2018, ICT and potential-ICT based digital trade between the United States and Europe was $188 billion in exports to, and $107 billion in imports from, the EU, respectively (see figure 1).

Figure 1: U.S. exports and imports of ICT and potential ICT-based digital trade with the EU (2018)[27]

Updating the U.S. Department of Commerce's "digitally deliverable services" (DDS) estimate—which comprises a more narrow set of services than those included in the estimates above—is more readily comparable across countries (using trade in value added (TiVA) and Eurostat databases), but does not have data for recent years (most recent data is for 2015). Analysis of DDS trade captures a mix of transactions that are entirely digital, somewhat digital, or entirely non-digital.[28] It also shows that transatlantic trade is large and growing. U.S. DDS exports to the EU rose from $98 billion to $183 billion between 2005 and 2015, while EU DDS exports to the United States rose from $67 billion to $108 billion (see figure 2).

Figure 2: U.S. exports and imports of digitally delivered services with the EU (2005-1015)[29]



The EU's DDS exports vary considerably by member state, which highlights the economic differences between member states and their use of data, services, and ICTs.[30] According to TiVA data, Germany has seen consistently rising DDS exports, growing from $36 billion in 2010 to $65 billion in 2018 (see figure 4). France has also seen its DDS exports grow, from $27 billion in 2011 to $41 billion in 2018 (see figure 5). By contrast, Italy's exports have barely grown (see figure 6), increasing only from $6.1 billion to $8.6 billion between 2010 and 2018. The Netherlands' DDS exports declined, falling from $41 billion in 2010 to $26 billion to 2018. Despite that country's low overall DDS exports, however, DDS services remain important to the Netherlands, exhibiting a high degree of DDS export intensity (DDS exports as a percentage of total service exports).

Parsing out DDS exports by industry shows further variation between the United States and the EU. In the United States, "other" DDS exports, represented by services (e.g., the legal, scientific, and architectural fields), has dominated in recent years (see figure 3). Royalties and licensing, as well as financial services, are also both significant drivers of DDS exports. IT services dominate in Germany (growing from $11.6 billion in 2012 to $22 billion in year 2018), while "other" remains at a close second, indicating a heavy IT focus in Germany relative to other EU countries (see figure 4). In France, licensing and "other" services take the lead, followed by IT and financial services (see figure 5). IT services also dominate in Italy, with that sector outweighing licensing and "other" related DDS exports (see figure 6). The EU will continue to remain a key region for many DDS sectors going forward, rivaled by the United States, Japan, and increasingly, China.

Figure 3: U.S. exports of digitally delivered services globally, by product group (2010-2018)[31]

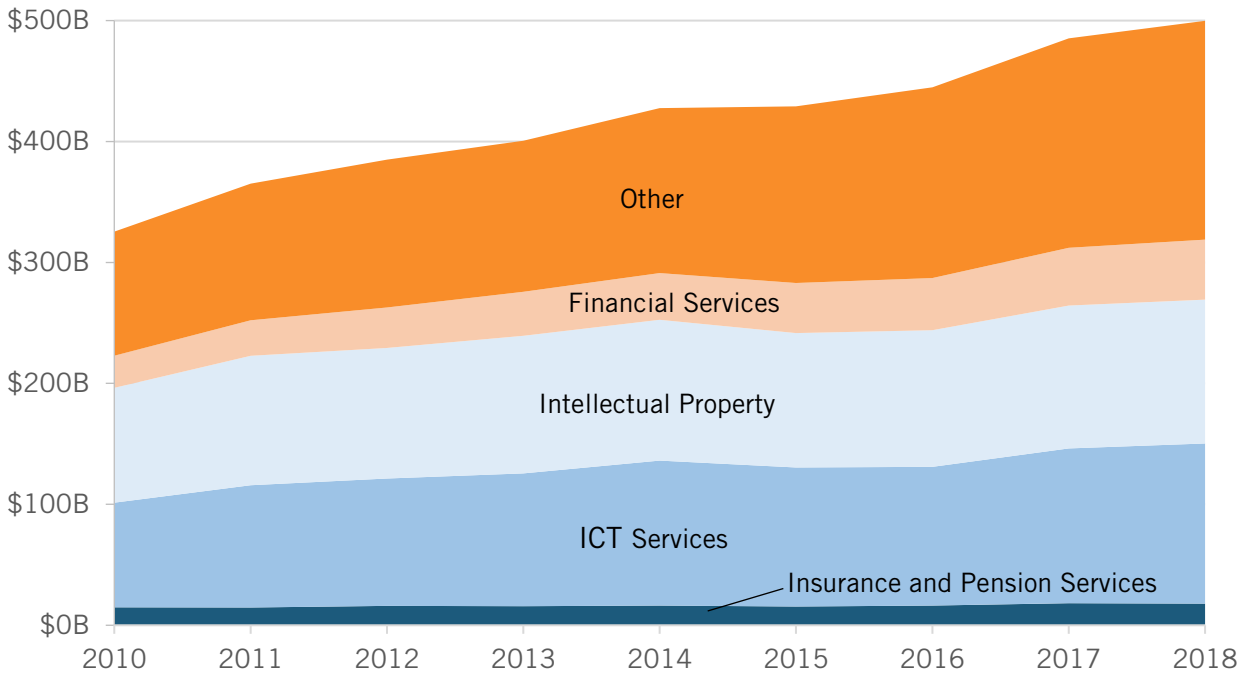


Figure 4: Germany's exports of digitally delivered services outside the EU, by product group (2010-2018)[32]

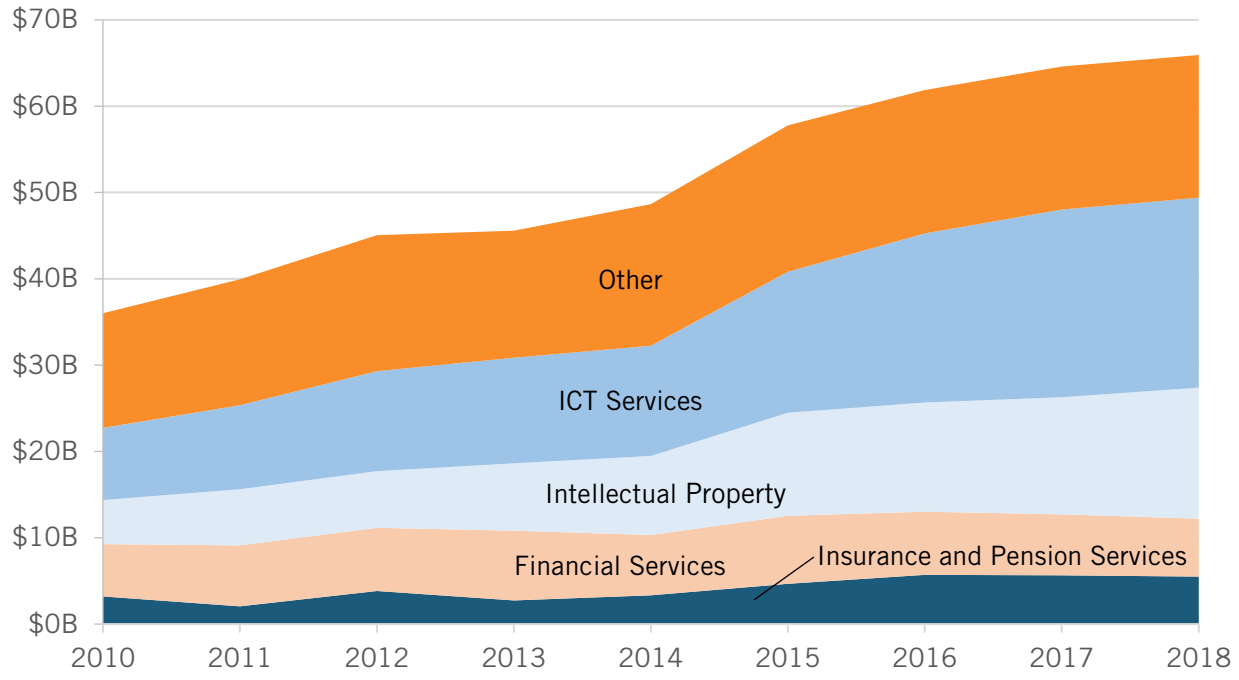


Figure 5: France's exports of digitally delivered services outside the EU, by product group (2011-2018)[33]

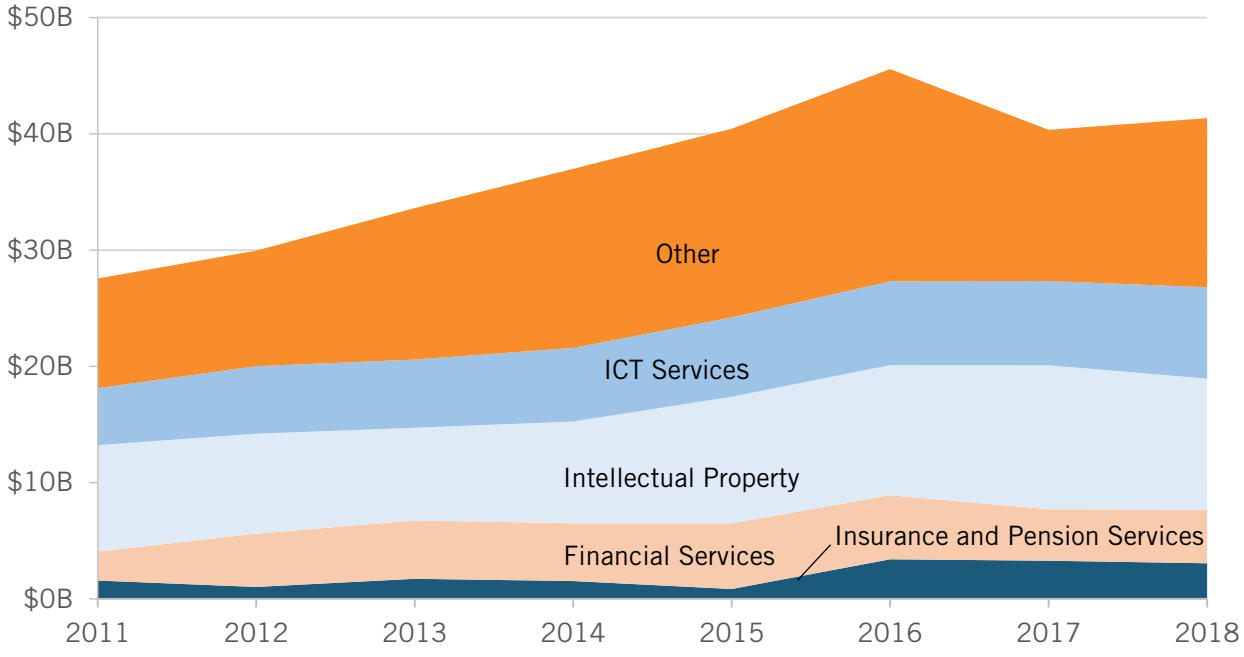
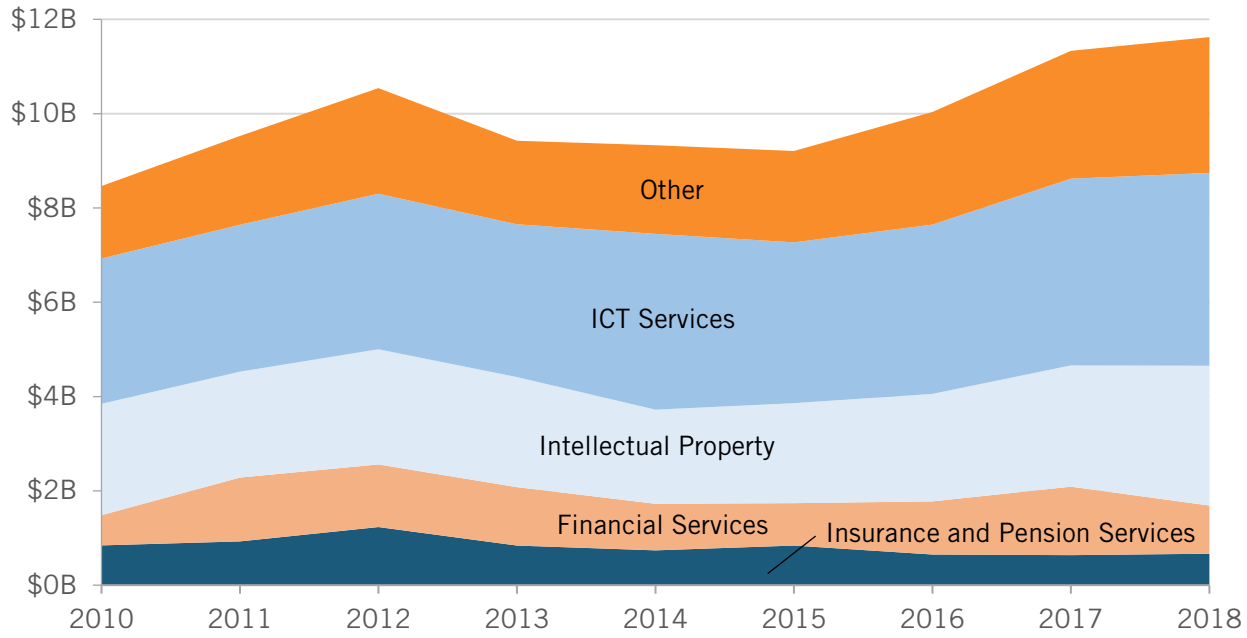


Figure 6: Italy's exports of digitally delivered services outside the EU, by product group (2010-2018)[34]

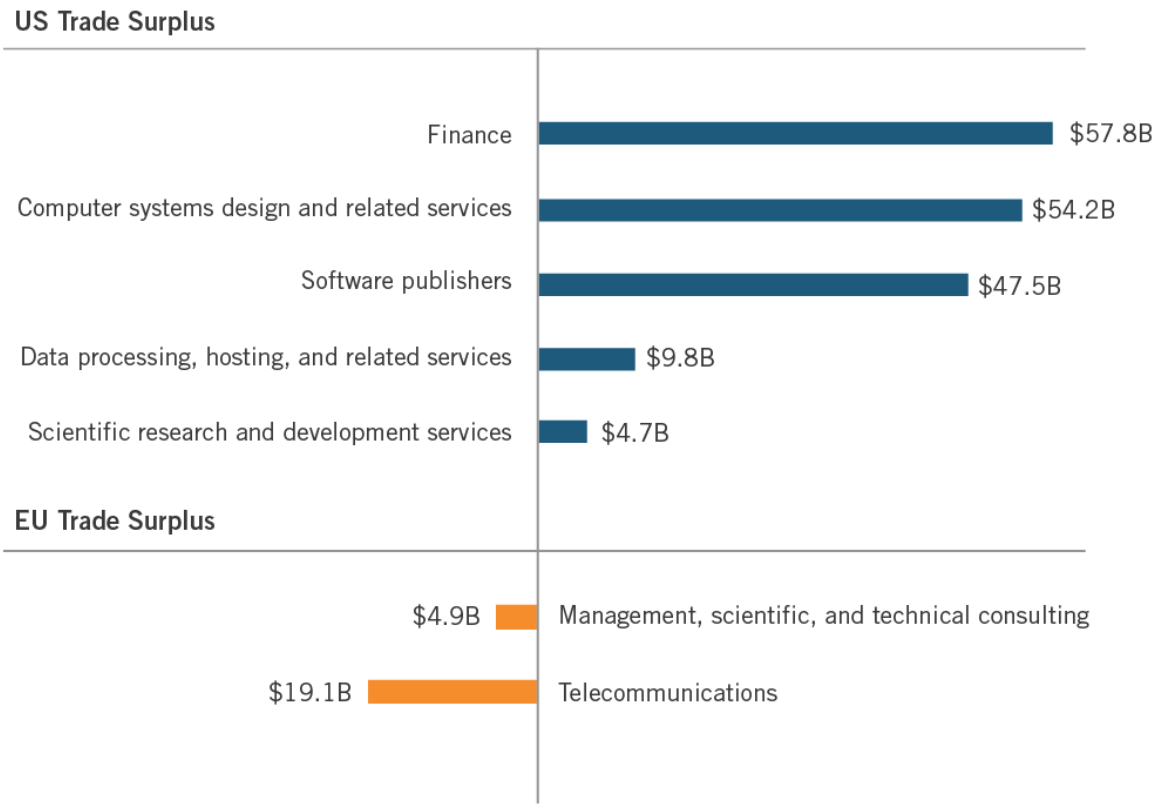


A comprehensive assessment of transatlantic digital trade needs to take into account valuable (but non-monetized) intra-firm data transfers that represent services supplied via affiliates located in both Europe and the United States.[35] As in 2018, about two-thirds of the services provided internationally both by and to the United States were through affiliates.[36] Many (if not all) multinational companies in the United States and EU rely on cross-border data transfers to support their international business operations. Again, there are measurement issues as differences in coverage and classification make it difficult to compare trade in services with services supplied through affiliates.[37] However, they are still useful in showing that the data displayed in figure 5 and figure 6 are conservative estimates of the full value of digital and digitally enabled services in the transatlantic economic relationship.[38]

A comprehensive assessment of transatlantic digital trade needs to take into account valuable (but non-monetized) intra-firm data transfers that represent services supplied via affiliates located in both Europe and the United States.

The U.S. Department of Commerce estimated that 53 percent of the $839 billion in services provided in Europe by U.S. affiliates in 2017 was digitally enabled. That year, U.S. affiliates in Europe supplied $444 billion in digitally enabled services, whereas European affiliates in the United States supplied only $269 billion in digitally enabled services.[39] The United States enjoys continued trade surpluses with the EU in many key digitally enabled services delivered via affiliates. For example, in 2018, U.S. software firms exported over $51 billion worth of services to the EU, whereas the United States only imported around $3.6 billion worth of software services from the EU. However, the EU did have advantages in areas such as management consulting, where it enjoyed a $4.9 billion surplus vis-à-vis the United States (see figure 7).

Figure 7: U.S.-EU trade surpluses in key digitally enabled services by affiliates (2018)[40]



WHAT'S AT STAKE: THE VALUABLE ROLE OF TRANSATLANTIC DATA FLOWS ACROSS SECTORS

Transatlantic data flows and digital trade matter to a broad range of sectors, and are a critical complement to the use of traditional trade statistics in understanding the role and value of data transfers.[41]

Industrial, Transport, and Automotive Sectors: Of Machines and Data

IT is transforming global manufacturing by digitizing virtually every step in how products are designed, fabricated, transported, serviced, and used—a phenomenon called "smart manufacturing" in the United States and "Industry 4.0" in Europe.[42] Indicative of this, as of 2017, digital services provided an estimated 25 percent of manufacturing inputs.[43] The increasingly global nature of manufacturing design, production, and customer and after-sales support processes mean that modern manufacturing firms increasingly rely on cross-border data flows. This section outlines how automotive and industrial firms rely on data and data flows, including a detailed analysis of the automotive sector and case studies on Scania and Volkswagen.

The global race for innovation advantage in modern manufacturing comes down, in no small part, to how firms and their broader production network are able to integrate data from all relevant stakeholders—wherever they are around the world. As part of this race, the United States and Europe have much to share and benefit from in terms of integrating digital manufacturing

operations and associated services. German President Angela Merkel has directly engaged in promoting Industry 4.0, noting, "We have reached a critical moment, a point where the digital agenda is fusing with industrial production." She's also identified the failure to lead in smart manufacturing as a threat to Germany's industrial prowess, "We have to execute quickly, otherwise those who are already leading in digital will snatch the industrial production from us."[44] Europe regards smart manufacturing as a core component of the European strategy on "smart specialization," which aims to strengthen the comparative advantage of the EU in terms of ICT skills, R&D capability, industrial output, and infrastructure. In other words, in Europe, smart manufacturing is being pursued at a regional level to make European regional-manufacturing clusters more globally competitive.[45]

Smart manufacturing provides manufacturers with a comprehensive view of what's occurring at every single point in the production system, along with the insights to make real-time adjustments in order to optimize production. A "plugged in" manufacturer can receive real-time information from suppliers to adapt to supply chain disruptions or use data analytics from across the supply chain to adjust to meet shifting demand.[46] As Robert Hardt, president and CEO of Siemens Canada, explained, smart manufacturing entails nothing less than "the availability of all relevant information in real time, through interconnection of all instances of value creation, and the capacity to derive from this data an optimal value creation flow at any point in time."[47] Cloud services and data flows level the playing field between small and large firms as it makes it easier for the smaller companies to access best-in-class, enterprise-level software and IT solutions.[48]

Manufacturing, transport, and industrial firms need a legal framework to transfer personal and nonpersonal data just as much as any other sector of the economy. Indicative of this, in October 2020, European trade associations from the road, air, maritime, rail, manufacturing, and logistics sectors outlined how they increasingly rely on the exchange of large amounts of personal and nonpersonal data between multiple actors, and explained why the EU needs to create a clear framework for the governance of these business-to-business data transfers.[49] Building on this, on November 26, 2020, a joint report and survey of nearly 300 firms (mainly EU firms (75 percent) headquartered across 25 countries, from all major industries, and a mix of company sizes) by Business Europe, DIGITAL EUROPE, the European Round Table for Industry, and European Automobile Manufacturers Association found that nearly 85 percent use SCCs. Manufacturing firms represented the second-largest users of SCCs (22 percent), behind firms in the ICT sector.[50]

The role of data flows within the global development of smart manufacturing is best demonstrated by cloud computing; additive manufacturing; sensor technologies and networked machine-to-machine (M2M) devices; data analytics and generative design; new business models involving data-dependent after-sales service; the use of AI for predictive and preventative maintenance and repair; and data-driven global research collaboration.

Cloud computing is transforming virtually every part of modern manufacturing. Even by 2015, a majority of manufacturing firms used cloud applications.[51] Expansive cloud-based networks store and process the massive amount of data necessary to manage modern manufacturing operations.[52] Whether it's how manufacturing enterprises operate, how they integrate into supply chains, or how products are designed, fabricated, and used by customers, cloud computing is helping manufacturers innovate, reduce costs, and increase their competitiveness. Cloud computing allows

manufacturers to use new production systems, from 3D printing and high-performance computing (HPC) to the Internet of Things (IoT) and industrial robots. This "Industrial IoT" increasingly relies on cloud computing and data transfers, as there are a number of individuals, objects, and other sensors connected to a growing network of smart devices and sensors.[53] Cloud computing alongside other foundational technologies such as advanced sensors, HPC, and computer-aided design, engineering, and manufacturing (CAD/CAE/CAM) software represents an essential component of the smart manufacturing revolution.[54] One study estimates that manufacturers allocate an average of 8.1 percent of their R&D budgets to developing these types of digital tools.[55]

Business-to-business and M2M cross-border data flows are powering much of the digital transformation sweeping industrial sectors around the world. These business-to-business data transfers don't get nearly as much attention as consumer Internet services, but they're increasingly critical to the global economy. In contrast to the popular perception about the major role played by personal data, individual consumers, and smartphones, Cisco estimated that out of the approximately 18.4 billion networked devices in use in 2018, nearly one-quarter (24 percent) served business customers. Cisco's Annual Internet Report (2018–2023) outlines how a growing number of M2M applications, such as smart meters, transportation, and package and asset tracking are now major drivers in the growth of Internet-connected devices—and that by 2023, M2M connections will account for about half of the world's total devices and connections. M2M connections will be the fastest-growing device and connections category (faster than smartphone use), growing nearly 2.4-fold during the forecast period (19 percent compound annual growth rate (CAGR)) to 14.7 billion connections by 2023.[56]

Business-to-business data transfers don't get nearly as much attention as consumer Internet services, but they're increasingly critical to the global economy.

Additive manufacturing is becoming more common for product prototyping and some mass production. For example, Ford uses 3D printing to make prototypes of auto parts, including cylinder heads, brake rotors, shift knobs, and vents.[57] In 2014, GE Aviation announced plans to begin mass production of its LEAP 3D-printed jet-engine fuel nozzles.[58] Similarly, Boeing has replaced machining with 3D printing for over 20,000 units of 300 distinct parts.[59] Firms are also using additive manufacturing to personalize products. Both Nike and Under Armour are exploring how additive manufacturing can revolutionize how they manufacture footwear, ultimately allowing the shoemakers to customize a sneaker to each athlete's foot.[60] 3D printing allows Nike to produce a shoe with just a few parts instead of dozens, resulting in up to 80 percent less waste.[61] Siemens uses additive manufacturing to create in-the-ear hearing aids that are individually adapted to the wearer's auditory canal.[62] The prosthetics industry has been revolutionized by 3D-printed limbs tailored to patients' specific structural needs and design desires.[63]

Data analytics, machine learning, and AI improve operations across industrial firms—not just on the factory floor. For example, data-driven insights can enable more innovative and efficient product design processes.[64] "Generative design," a process by which a computer algorithm tests thousands (or even millions) of design possibilities based on parameters entered by designers or engineers, accelerates innovation by rapidly generating possibilities that humans alone may not have discovered.[65] Human-machine interaction can also improve production processes, as workers

collaborating with automated machines allows for more dynamic and adaptive processes.[66] In each of these approaches, data flows are necessary to enable cross-border, multi-team collaboration.

Data flows also allow for critical after-sales service and manufacturers to create new services-based business models. For example, maintenance crews can receive diagnostics from an airplane while it's still in-flight, and vehicle manufacturers can remotely monitor their products and alert drivers when repairs are needed.[67] It's becoming more common for manufacturing firms to eschew selling individual products in favor of selling products as integrated services. For example, GE's medical devices division no longer sells individual radiological equipment (e.g., MRI or X-ray machines) to hospitals; rather, it sells radiological services, taking over management of a hospital's entire suite of radiological assets and installing devices with remote-monitoring capabilities that allow GE to both monitor whether they are operating and functioning properly and diagnose and detect maintenance issues.[68] Similarly, Kaeser Kompressoren, a German-based manufacturer of compressed air systems and services, launched an "air-as-a-service" business model in which customers no longer purchase Kaeser compressors but rather lease the compressors and pay only for the compressed air itself. It means customers can scale consumption up or down as the needs of their manufacturing operations change, without needing to purchase new equipment.[69]

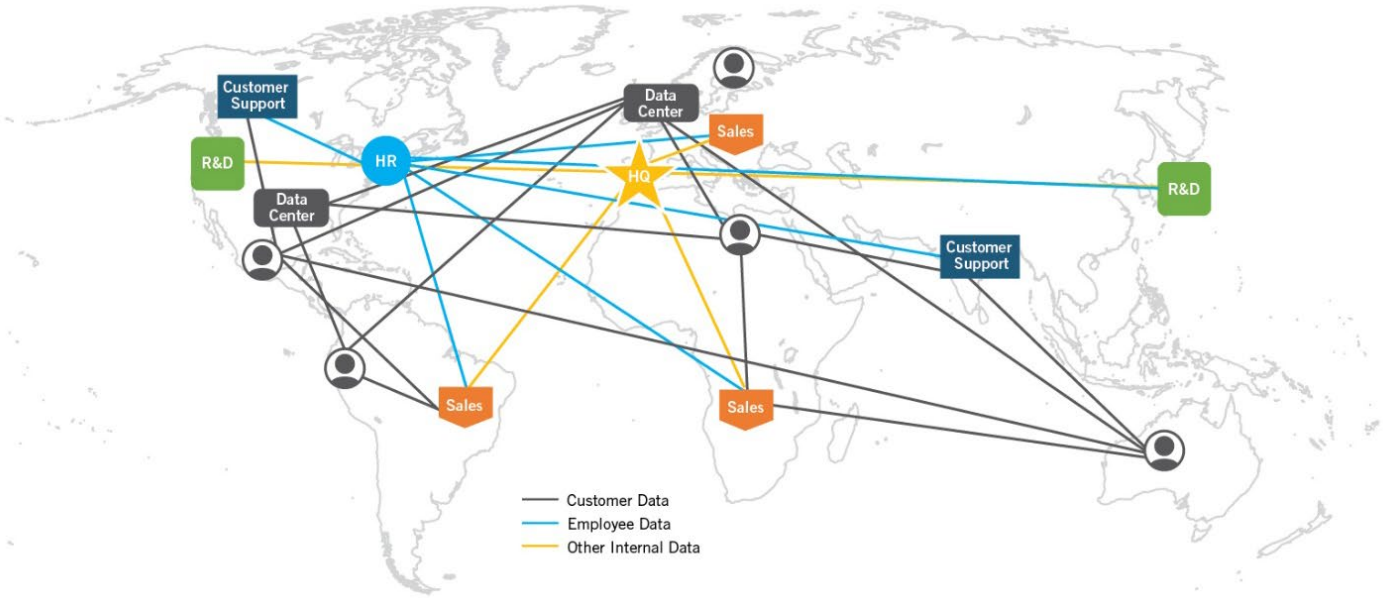
One of smart manufacturing's biggest benefits is in predictive and preventative maintenance and repair, which allows firms to shift from a maintenance model of "repair and replace" to "predict and prevent."[70] The McKinsey Global Institute has estimated that the use of predictive maintenance techniques reduces factory equipment maintenance costs by up to 40 percent, while reducing equipment downtime by up to 50 percent, and capital-equipment investment costs (to replace defective equipment) by 5 percent.[71] For example, Intel uses predictive modeling to anticipate failures, prioritize inspections, and cut monitoring costs at its chip-manufacturing plants.[72] Manufacturers are also integrating predictive-maintenance data into their enterprise resource planning systems to improve workflow scheduling, thus optimizing repair schedules and minimizing machine downtime. Taleris, which supports airline and cargo-carrier operations, uses this technology to predict aircraft-maintenance faults and thus minimize flight delays. Likewise, Germany's ThyssenKrupp AG and Kaeser Kompressoren use tens of thousands of networked equipment sensors to identify and predict maintenance issues, which reduces unscheduled downtime and helps avoid unnecessary repair trips.[73]

The Automotive and Transport Sectors Rely on Data Flows to Support Drivers, Connected Vehicles, and Related Services

Digital technologies and data flows are particularly critical to the automotive and transport sector. As Swedish commercial vehicle manufacturer Scania's Hakan Schildt told the *Financial Times* in 2018, "[T]ransport is becoming a data business."[74] As connected devices, data-driven insights, and advancements in AI accelerate innovation in this sector, the ability to exchange data is crucial to improving the quality and safety of vehicles and transportation systems.[75] Cisco's Annual Internet Report (2018–2023) predicts that connected car applications, which include fleet management, in-vehicle entertainment systems, emergency calling, Internet, vehicle diagnostics, and navigation, will be the fastest-growing category of M2M application, with a 30 percent CAGR.[76] The next generation of trade and innovation between the closely integrated EU-U.S. automotive and transport sectors will be put at risk if the rules and regulations around data are not carefully designed so as to allow the reasonable and responsible collection, processing, and transferring of personal and nonpersonal data associated with connected vehicles.

Automotive and transport manufacturers receive, exchange, and process increasing amounts of both personal and nonpersonal data from individuals and vehicles around the world, including data about the vehicles themselves (e.g., vehicle identification, configurations, maintenance information, and network information such as IP address or Bluetooth name); data about drivers and other users (e.g., driving behavior, geolocation, user-provided information, and contractual data); and data from outside the vehicle (e.g., temperature, weather conditions for automatic lights or wipers, and images and videos from outside the vehicle).[77] For instance, modern vehicles collect map and personal data for real-time analysis and use. Automated and autonomous vehicles rely on AI that uses cameras and sensors to analyze the vehicles' environment, including detecting road signs and other road users, and then shares that data with the cloud to ensure the information is accurate and the cars operate as safely as possible. Similarly, sensors monitor drivers' attention and detect drowsiness. Figure 8 is indicative of the data transfers that an EU-headquartered, globally engaged, manufacturing or transport firm would be engaged with in having R&D, human resources, engineering, sales, and customer support centers around the world.

Figure 8: The data transfers for a (generic) EU-headquartered manufacturing/transport firm with global operations



This data is not only critical to vehicle and driver performance, but also to future innovation, as firms increasingly rely on data to design and deliver better products and services. This will become more important to automotive competitiveness as autonomous vehicles, connected vehicles, and smart cities become more common.[78] Automotive and transport firms will increasingly depend on data transfers to build large and diverse training datasets for product development. For example, to maximize product performance in countries around the world, firms need to ensure their training data captures the variations in environments, traffic conditions, and other variables that reflect the "real world" context in which their products operate.

Smart manufacturing is transforming the automotive industry (see the case studies on Scania and Volkswagen). For example, BMW has set a goal of knowing the real-time status of all major production equipment at each of its component suppliers. Accordingly, upstream tier 1 and tier 2

suppliers such as Austrian brake-pad manufacturer Miba AG have IoT-enabled their production equipment to track and communicate production machines' operational status to its original equipment manufacturer customers.[79] Similarly, Ford has placed sensors on virtually every piece of production equipment at its River Rouge facility outside Detroit.[80] Connected devices and smart manufacturing also dramatically improve automotive companies' ability to manage their supply chains. For example, Toyota reduces the time and cost of recalls by knowing exactly which machine produces each component of each vehicle, thereby enabling the company to track and isolate defective parts (or the defective equipment that produces them) much more rapidly. Smart manufacturing, data connectivity, and connected vehicles also allow products to convey information about how they are consumed and serviced, which firms can feed back into the design process to improve future versions of those products.[81] For instance, heavy-equipment manufacturer John Deere previously manufactured multiple versions of engines with different horsepower levels for its tractors, harvesters, and gins. Today, it manufactures just a single, standard engine and uses software to alter the horsepower level for different applications.[82]

Smart manufacturing is also changing after-sales service. For example, in 2013, Tesla sent an over-the-air software update to all Model S vehicles after batteries fires in two of its vehicles were found to have been caused by a manufacturing flaw that caused the chassis on some of its vehicles to sit too close to the ground.[83]

Case Study: Scania

Scania—a leading Swedish manufacturer of commercial vehicles—is, as one *Financial Times* article put it, "increasingly hindered as much by international obstructions to its data as roadblocks on its lorries."[84] Indicative of the importance of global data transfers, Scania uses a single, global telematics (the field that encompasses telecommunications, vehicular technologies, electrical engineering, and computer science) service platform.[85] Scania has manufacturing centers in Europe and Latin America and is responsible for managing fleets of trucks around the world.[86] Much like with other automotive companies, as a Scania truck is driven through the EU, a small box sends diagnostic data—speed, fuel use, engine performance, even driving technique—to the company's headquarters in Sweden. As of 2017, Scania had more than 280,000 vehicles connected to its Scania One and Scania Digital Services software. The company had 91 percent of its vehicles connected in Europe; globally, it had 60 percent connected.[87] Indicative of the growing role of software and data, Scania is developing an open, brand-neutral platform (the RIO platform) and operating system for software that will host its telematics services as well as software from third parties, thus making it easier for its partners and other transport manufacturers to adopt and use.[88] Scania has likewise increasingly transitioned to a services-based business model focused on fleet management services including logistics, repair, and others. In fact, Scania now generates one-sixth of its revenues through new services enabled by the data-connected devices built into its vehicles.[89]

Hakan Schildt has stated that "the world is moving towards an autonomous, electrified transport system, and that needs data … transport is becoming a data business," and that "the free flow of data is part of free trade."[90] Data transfers and analytics improve Scania's product development process by allowing the company to gain insight into the on-the-ground performance of its vehicles and identify areas for potential improvements.[91] Allowing Scania and vehicle owners to coordinate and control entire fleets of connected and autonomous vehicles leads to improved environmental outcomes, especially reduced CO_2 emissions.[92] For example, collecting and sharing personal and

nonpersonal data allows Scania to "coach" drivers to help them improve, such as with braking points and coasting.[93]

Case Study: Volkswagen

Volkswagen—Europe's biggest automotive manufacturer—is going digital, including through the extensive use of Amazon cloud computing services.[94] As one VW executive put it, "[G]oing forward, our Volkswagens will increasingly become digital devices on wheels."[95]

VW is using data, software, and associated services to differentiate itself from the competition. In 2020, some 1.5 million VW vehicles with no online access could connect with the Internet thanks to the "Volkswagen Connect" (a retrofit solution). In the future, VW will connect every one of the estimated five million vehicles it plans to manufacture each year.[96] VW has over 80 IT specialists, data scientists, programmers, and others at its "Data: Lab Munich" incorporating AI and other digital tools throughout its business, including in production, sales forecasts, predictive maintenance, and autonomous driving.[97] VW is also using AI and other digital technologies to become a "smart enterprise."[98] For example, the Volkswagen Group is the world's first automotive company to intensively test the use of quantum computers, such as to predict vehicle traffic patterns in Barcelona to help taxi and transport firms.[99] Florian Neukart, principal scientist at Volkswagen's CODE Lab in San Francisco, stated, "What makes the now-developed solution so special is the possibility to scale it to any city."[100] However, VW and other firms that seek to use quantum computing would obviously depend on data transfers to deploy this technology, given it would be prohibitively expensive to deploy it to every market.

Volkswagen—Europe's biggest automotive manufacturer—is going digital, including through the extensive use of Amazon cloud computing services.

VW's digital operations are embedded within its transatlantic operations. In 2020, VW announced that its factories in Chattanooga (Tennessee, the United States) and Puebla and Silao (Mexico) would be the first Volkswagen factories outside Europe to connect with VW's global "Industrial Cloud" initiative—which uses Amazon Web Services (AWS). VW's 18 factories in Europe were already networked with its Industrial Cloud, which is designed to gather and analyze data from all connected VW facilities on a real-time basis to help increase efficiency and productivity. It also allows central, standardized access to software applications, much like an app store on a smartphone. VW's Industrial Cloud links not only all of VW's global factories, but also (in a second step) its suppliers in order to simplify the exchange of data across systems and plants.[101] Volkswagen and AWS plan to open the Industrial Cloud to other firms, thus making it a marketplace for industrial applications.[102]

A Connected or Fragmented Transatlantic Manufacturing Network?

Automotive and transport firms are increasingly dependent on the ability to transfer personal and nonpersonal data around the world. As Scania put it, "[V]ehicles would not function effectively without transferring data, and neither would repairs."[103] The automotive and transport sectors are affected just as much as other data-driven sectors by a globally fragmented Internet. Like other sectors, it would be overly expensive and complicated, if not impossible, for these firms to set up duplicative IT and the growing range of support services in each and every market in which their

vehicles are used. Doing so would add unnecessary costs and simply lead automotive and transport firms to cut off critical services to restrictive markets.[104]

Automotive and transport firms are clearly capable of developing sophisticated legal compliance frameworks to use and protect data as per local laws, especially given they already operate in a heavily regulated industry with a host of vehicle safety and performance standards.[105] For example, Volvo, VW, BMW, and many other major car manufacturers use standard contractual clauses to transfer European personal data overseas. The invalidated EU-U.S. Privacy Shield was used by 37 firms in the automotive sector (and 28 firms in the aerospace and defense sector).[106] Firms want a clear, predictable, and reasonable legal framework that allows them to protect data according to local privacy laws, while still using it to design and deliver innovative new products and services. As a position paper from the European Automobile Manufacturers Association (EAMA) cautions, "It is important to stress the use of global data and the implementation of clear guidelines and processes for sharing data between countries … otherwise, the value of the data will be lost."[107] While the 2018 *Roadmap for EU-USA S&T Cooperation* notes that "there is a clear interest in continuing collaborating in areas where interoperability is necessary to ensure smooth and secure transatlantic/global data flows," including "automated driving and road automation in general, air quality and low-emission freight transport systems, [and] multi-modal inter-urban transport," such cooperation is at the mercy of the broader transatlantic conflict over data privacy and surveillance.[108]

Automotive and transport firms are increasingly dependent on the ability to transfer personal and nonpersonal data around the world.

Beyond *Schrems II*'s impact on Privacy Shield and SCCs, the EDPB's generally restrictive approach to regulating the personal data relating to connected vehicles highlights the many and varied challenges to automotive firms that operate on both sides of the Atlantic. The EDPB views most data collected via connected vehicles to be personal, and that data controllers (i.e., the car manufacturers) should, whenever possible, not transfer personal data outside the vehicle (never mind outside the EU). The EDPB thinks that this local processing of personal data keeps drivers in control of their data, as well as their vehicle.[109] While the EDPB makes brief references to the possibility of joint controllership of vehicle data, it has given no firm guidance around the extent to which joint controllership might apply to common use cases in the connected car context, such as data sharing between vehicle manufacturers, data aggregators, and other third parties (e.g., insurance firms).[110] In response, EAMA cautions the EDPB to develop and apply nuanced sector-specific privacy rules for connected vehicles, as the draft guidelines it has issued have been overly broad, ill-fitting, and restrictive.[111]

Data restrictions in other countries offer a glimpse of the potential consequences for automotive and manufacturing firms should the United States and EU fail to build a legal framework to allow firms to transfer personal and nonpersonal data across the Atlantic. India requires gateways and application servers that support the Internet of Things to be located inside the country.[112] China has data localization for both personal and mapping data (as well as restrictions on whom can collect and use this mapping data). This includes the high-definition maps that are critical to the operation of automotive vehicles.[113] Indicative of the duplicative and unnecessary impact on

automotive manufacturers, Tesla (which has a large factory in China) has moved its user data from the United States to China to comply with local data storage requirements.[114]

Turkey requires all new cars to provide e-call services, carry local eSIM cards, and store all relevant data in Turkey. Turkey's restrictive rules are broad in that they apply to all M2M communications.[115] Vehicle manufacturers and associated service providers need to transfer and share this type of data, such as with insurance companies to determine coverage; geographic location data with tow-truck operators for emergency help; and performance data to help firms develop better safety systems.[116] In Turkey, major automotive producers have mostly chosen to shut down e-call services for cars already in the marketplace and have stopped exporting new cars. So it's hardly a win for automotive safety, never mind trade.

Financial, Payment, and Insurance Services: Key Enablers of Global Digital Trade

Banking, finance, and insurance services depend on data flows to engage and support trade. Consumers and firms want these services to seamlessly manage the considerable challenges of managing cross-border transactions, while maintaining a high level of security and privacy.[117] This is a challenge, as these services are already among the most heavily regulated in the global economy. For example, as part of a Committee on Payments and Market Infrastructures (a global standards-setting forum for central banks and others) survey, payment service providers cited anti-money-laundering, know-your-customer, risk-mitigation, and consumer-protection requirements as the most significant costs and challenges to their business, especially for cross-border payments.[118] Adding new data-related restrictions further complicates efforts to address these domestic regulations that act as a bottleneck to the use of these services in global trade. This section analyzes the role of data in global financial, payment, and insurance services.

Data and digital technologies have transformed the financial, banking, and insurance sectors. Internet banking is increasingly the norm for consumers and businesses around the world. The many leading U.S. and European providers need to be able to seamlessly transfer tremendous amounts of data for their own operations (e.g., human resources and IT development) and between subsidies (to complete transactions), but also as part of both exchanging information with third parties and the day-to-day business of checking and processing payments, fund investments, and other transactions.

New data-driven services are at the heart of the fierce competition that is underway between incumbent firms and fintech start-ups.[119] The basis for competition in these sectors increasingly revolves around their ability to develop and deploy new payment services, AI, and other innovations, whether as part of improved cybersecurity, digital identity, digital assistants (e.g., natural language processing robo-advisors), or blockchain services. Indicative of this, in 2017, JP Morgan had 4,000–5,000 software developers working on applications.[120] Traditional banks are fighting back against new fintech entrants by providing end-to-end services across the banking and payments sector, including through partnerships with new entrants.[121] Meanwhile, new fintech entrants are providing new means of payments, often as part of a broader set of digital services.[122] At the big end, this is perhaps best demonstrated by Chinese insurance firm Ping An's technological prowess and its use of a vast platform of services to become a "fintech super-app."[123]

Cloud computing allows all payment, banking, and insurance firms to handle high-volume, complex computations at sometimes irregular intervals, while maintaining stringent cybersecurity

protections and allowing access to data for compliance purposes (e.g., for anti-money-laundering and counter-terrorism financing). Given the sensitivity of the data and processes involved, some of these firms have been reluctant to move away from in-house data storage. Yet, more and more firms are shifting to public cloud services that are increasingly able to provide the strict cybersecurity services and compliance processes these firms need.[124] Given the sensitivity of the data being managed and the strict regulatory oversight in place, if these firms can use public cloud services on a global scale, so should pretty much any firm.

Insurance, reinsurance, financial, and payment firms rely on data and data flows in similar, but sometimes different, ways.

Unnecessarily restrictive data-related rules make it costlier and more complex, if not impossible, for financial, payment, and insurance firms to transfer and use data as part of seamless, standardized, and centralized service offerings.

Insurance firms rely on data to provide products to individuals and firms around the world. Personal insurance products are increasingly being sold and policies managed online and on mobile phones. The basic customer interface depends on data flows, in terms of accessing their policies, especially if they move or are part of an international business operation. The underwriting process that is central to insurers depends on data transfers and analytics, which are necessary to understanding their clients, assessing risk, and pricing and tailoring packages of insurance products for clients.[125] For example, real-time data analytics allow insurance firms to predict and react to events such as severe weather and natural disasters, in addition to how likely someone's car is to be stolen in a given month or whether a person is likely to face a health issue. Also, when clients voluntarily provide more data on their behavior through telematics—such as sensors in vehicles to assess how they drive—it allows insurers to better understand their clients and encourage less-risky behavior. Greater access and use of data and data analytics can also dramatically reduce administrative costs for insurance and reinsurance firms, which is important as claims settlement, acquisition, and administration are expensive, taking up about 33 cents out of every dollar a policyholder pays to an insurer. For instance, when claims are made, improved data analytics and access to large pools of data aid insurers in identifying genuine versus fraudulent claims.[126]

Both insurance firms and reinsurance firms—which take on portions of risk portfolios of other insurers—need to be able transfer data in order to build large datasets and provide better and cheaper products. Indicative of this, as Kai-Uwe Schanz and Fabian Sommerrock of The Geneva Association noted, "In the digital age, traditional information asymmetries in insurance are likely to disappear, with both insurers and policyholders benefitting from much improved information at much lower cost."[127] For example, while major insurance firms underwrite processes in each client's home country, for regional and global products and customers, this happens at a higher level that thereby makes it necessary to transfer personal and other data. Likewise, reinsurance relies on transfers of personal and other data, as the client taking on the reinsurance needs to assess the underlying data in order to assess the associated risk. Furthermore, reinsurance contracts often involve a firm in one of only a few global hubs, namely Switzerland, Bermuda, Singapore, New York, or Munich, even if the two parties are outside of these countries (e.g., between an Argentinian insurance company and a reinsurance client in Uruguay). Personal data

therefore needs to be able to flow between these hubs and the multiple parties involved in a transaction.

Data is also central to the role payment services play in global trade. A growing number of individuals and firms that travel and engage in worldwide trade have come to expect payment providers to do likewise. Indicative of this, payment networks clear and settle transaction information, not funds. Ensuring that consumers and firms in every market can access new, low-cost, and innovative electronic payment options is critical to supporting domestic commerce and global trade. There is a clear trend in the payment services space toward new partnerships and digital technologies, so companies can provide a more personalized, secure, and seamless suite of services embedded in mobile apps, e-commerce marketplaces, emails, and elsewhere. In this way, payment services represent a critical part of the suite of online services that together make it much easier and cheaper for firms of all sizes to access customers around the world. These services increasingly go beyond payments and money transfers to include financial dashboards, credit score management, customized loan/insurance plans, and investment services.

Unnecessarily restrictive data-related rules make it costlier and more complex, if not impossible, for financial, payment, and insurance firms to transfer and use data as part of seamless, standardized, and centralized service offerings. Payment and financial are among the most commonly targeted types of data in the world, alongside personal data. Restrictions on the movement of data undermine firms' ability to aggregate and analyze data from the broadest range of sources.[128] They also have a significant impact on trade, effectively prohibiting foreign firms from bringing to bear their globally distributed data analytics platforms—such as for fraud and money-laundering prevention, cybersecurity, and other data-driven services—which is a key part of their competitive offering.

Having all relevant regulatory compliance and service support expertise in every market isn't viable.

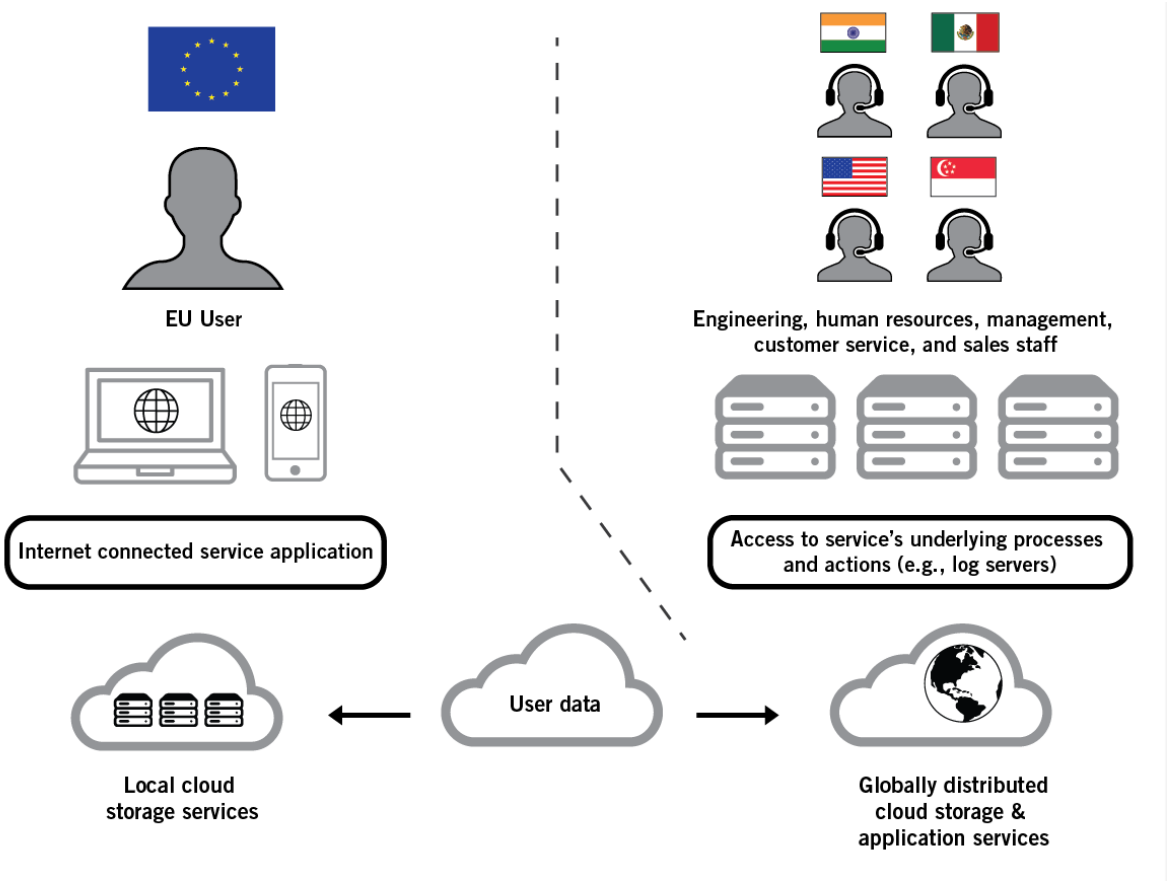
Fraud, for instance, is not limited by national boundaries. Preventing payment firms from working with global datasets undermines their ability to use data analytics to combat it.[129] Data analytics use behavioral, temporal, and spatial techniques to assess a consumer's behavior and whether a transaction is out of the normal or not. When a transaction is initiated, hundreds of pieces of information (e.g., about the customer, merchant, place, and time, all compared against years' worth of prior transactions) are gathered and sent for analysis by the payment processer's predictive model to determine if it is likely a genuine or fraudulent transaction. For payment firms, this process happens tens of thousands of times daily, ultimately involving billions of pieces of data.[130] These data-driven systems are powerful and fast enough to detect fraud in real time by using models based on historical data (and deep learning). Similarly, big data analytics are used to detect money laundering disguised as legitimate payments.

Ultimately, forcing payment service firms to use an artificially altered (i.e., only local) database for analysis would render them unable to provide the most accurate prediction for customers as it relates to fraud and other activities.[131] In the case of data localization, this would mean firms would only be able to identify local patterns of fraud, and thus would be blind to wider fraud patterns and threats, which would have the unintended and undesirable consequence of benefiting

criminals. Consumers, financial institutions, and regulators all stand to lose if firms are not able to use data from around the world to prevent this type of unwanted activity.

Data localization's impact is much broader. U.S. and European financial, payment, and insurance firms must transfer data as part of their global IT network and data engineering, regulatory compliance, and customer support teams and operations they have in their home country. Having all relevant regulatory compliance and service support expertise in each and every market isn't viable. Obviously, many firms set up country and regional support teams, such as to ensure compliance with GDPR or U.S. financial regulators, but they all report to, and benefit from, seamless engagement with central support teams based in their home country. For example, if an EU customer identifies an issue with a firm's service, the firm may well need an engineer or customer service representative based in the United States, India, or elsewhere to access the issue, user data, and local IT systems in order to resolve it (see figure 9).

Figure 9: Cross-border implications for EU users and U.S. firms that rely on data flows and cloud-based services



It is unreasonable to expect that firms would not only set up local data center infrastructure but also duplicative full-service engineering and customer support operations in each market, so the right person to fix an issue is based locally (and personal data doesn't need to be transferred as part of a fix). Given the cost and operational efficiencies, and in order to provide more secure services and responsive regulatory services, banks and payment and insurance firms (like most global firms) want IT operations to be centralized. Upskilling staff, licensing technology tools and utilities, and providing adequate support and maintenance become significantly more complex and

expensive (or even prohibitive) in a decentralized system wherein firms must unnecessarily expand and add duplicative services to their IT network.

This does not mean these firms don't set up substantial operations outside their home markets—they obviously do. But these firms are often driven by commercial and other considerations as they set up locations as part of strategic corporate plans. For example, many U.S. financial firms have regional compliance and tech support teams in Dublin, Ireland, as part of their European headquarters. But these are not simply compliance services: Mastercard's and Citi's Dublin centers, for instance, were each set up for global R&D and service. Mastercard's tech hub will grow to over 2,000 employees in the next few years and serve customers across Europe and the rest of the world.[132] It will also need to integrate with the company's other global technology centers in Vancouver, New York, St. Louis, Pune-Vadodara (India), and Sydney.[133] Similarly, Citi's service center provides support services to customers across Europe and the world—and includes the company's first Innovation Lab, which is dedicated to R&D in the financial services industry.[134]

Given their critical supporting role in global trade and economic activity, financial, insurance, and payment firms need to have a clear legal framework to transfer data for both commercial and regulatory purposes. Even before *Schrems II*, this was challenging. For example, U.S. financial firms faced regulatory issues in Europe related to their need to provide data to the U.S. Office of Foreign Assets Control and requirements for them to do screening for terrorism-related transactions.[135] Many banks and insurance and payment firms rely on SCCs to transfer data around the world—not just between the EU and the United States—as they are the most flexible legal tool to manage a diverse range of tasks. Previously, as in other sectors, Privacy Shield was a complementary legal tool used in the financial services sector. As at October 2020, 156 financial service firms relied on Privacy Shield as their primary mechanism for EU-U.S. data transfers.[136] For financial, insurance, and payment firms, adjusting to the uncertainty and changes in the EU's data protection regime with GDPR and *Schrems II* will be challenging, even with their extensive, existing legal compliance capabilities.

Cutting off financial, insurance, and payment data transfers between the EU and United States (and between the EU and the rest of the world) would mean fewer, more expensive, and less-than-best-in-class services, as the many firms and sectors that rely on these services to engage in transatlantic and global trade would inevitably be affected. Longer term, it would affect competition and innovation in these sectors, as it would disproportionality disadvantage new small and medium-sized fintech firms that otherwise could use access transatlantic markets in order to scale and compete with incumbents. EU and U.S. policymakers need to avoid making the regulatory-compliance situation any worse in these sectors and ensure that all these firms have a reasonable data transfer framework to manage varying local legal requirements (whether privacy or financial-oversight related), without unnecessarily inhibiting their role in global trade and innovation.

Data Flows Support the Growth of Small and Medium-Sized Enterprises

Restrictions on transatlantic data flows would disproportionately affect start-ups and small and medium-sized enterprises (SMEs), regardless of whether they are trade-orientated, given it would affect their ability to use the most useful and competitive services (in Europe or the United States) and easily and seamlessly find and serve customers on both sides of the Atlantic.[137] In this way, restrictive data rules undermine one the central benefits of the Internet—reducing, or removing,

the impact geography has on small firms' ability to engage in cross-border trade and use the best-in-class services (e.g., those in the United States). Ultimately, the direct and indirect impacts of restrictions on data transfers will affect the broader start-up and SME ecosystem by affecting firms' ability to scale.

Restrictions on transatlantic data flows would disproportionately affect start-ups and small and medium-sized enterprises, regardless of whether they are trade-orientated.

Ironically, given European policymakers' focus on large tech firms, the slide to ever greater restrictions on data transfers would make the European digital market inaccessible to all but the largest firms. Data privacy laws and international data transfer rules need to be easy to apply so SMEs and start-ups can build to a reasonable legal requirement from the start. This would allow them to focus on growing their ideas and businesses through trade and the best digital tools available, rather than on ever-changing and costly administrative compliance. In particular, start-ups are often early users of new digital technologies and therefore do not have to deal with the legacy IT systems of older firms. For example, many start-ups have been able to outcompete their more established rivals by virtue of being "born digital," meaning they have been better able to leverage productivity gains of newer technologies. Limitations on data flows would restrict EU start-ups from leveraging new U.S.-based technologies, especially from other start-ups and smaller firms that have not established a European presence. This would put EU start-ups, as well as other EU SMEs, at a disadvantage to their foreign competitors.

The survival and success of SMEs and tech start-ups increasingly depend on seamless and affordable access to data and digital tools. For example, surveys show that 74 percent of SMEs in the United States and 55 percent of EU start-ups and scale-up firms use cloud services.[138] Should cloud services providers and similar enterprise services take on higher compliance costs or halt data exchanges outside the EU, start-ups may face increased costs or less-optimal alternatives. SMEs greatly benefit from a range of digital tools that allow them to operate seamlessly in both their home and international markets: to develop, for example, an online presence, such as via online directory listings, websites, and mobile apps; social media for customer engagement, sales, and marketing; data analytics to gain customer insights or inform business decisions; customer acquisition via e-commerce marketplace platforms; and internal productivity tools, such as cloud-based software, video conferencing, and corporate social networks.[139] The COVID-19 pandemic has accelerated the broader digital transformation of SMEs, with more and more turning to online solutions to connect with customers and sell their products.[140] Start-ups and SMEs do not look at countries of origin when choosing their IT, software, and Internet services. Whether it comes to cloud services, marketing and advertising, customer relations, or some other service, data flows allow these firms to select the services that best align with their needs.

Small firms' ability to go global with only limited IT spending and little complexity will be undermined if major markets such as that of the EU require them to build out or pay for duplicative local services and infrastructure in each market. Access to inexpensive cloud and other ICT services has also been a key leveler in the playing field between SMEs and start-ups versus larger firms. As Allied for Startups (a worldwide network of 45 advocacy organization) has stated, every additional layer of regulatory complexity and cost makes it harder for EU start-ups to emerge from or enter into a new market, and effectively ring-fences bigger firms from greater

competition.[141] Previously, a lot of firm and venture capital had to be invested in expensive IT. Inexpensive global cloud services are now the norm. Yet, growing data restrictions could reverse that. It is simply not feasible for each and every service provider with a few customers in a given market to build out local infrastructure and operations, which means many will simply not serve certain markets (given the growing threat of fines). Data-transfer restrictions would force firms to choose local service providers that may not be the most competitive, cost-effective, or comprehensive in providing international services.

This would be a sad result, as the United States and Europe are developing a more connected and dynamic tech start-up scene involving venture capital, people, and ideas.[142] Start-ups in both the United States and EU have thus far been able to rely on data flows to grow and expand on both sides of the Atlantic. The United States is an important market for fledgling European start-ups, as it is home to four of the top ten start-up ecosystems in the world.[143] However, European start-ups, bolstered by cross-border opportunities, are catching up. Europe produced about 36 percent of start-ups worldwide between 2009 and 2019, and hubs such as Stockholm, Paris, Amsterdam, and Berlin are emerging.[144]

Small firms' ability to go global with only limited IT spending and little complexity will be undermined if major markets such as that of the EU require them to build out or pay for duplicative local services and infrastructure in each market.

Greater transatlantic engagement between start-up ecosystems would benefit everyone. A recent National Bureau of Economic Research study into cross-border venture capital, technology spillovers, and start-ups in the United States from 1976 to 2015 demonstrates the depth of the connections and the benefits. Of the 524 firms that had non-U.S. corporate investors, 11.5 percent of their investors were from Germany and 6.9 percent were from France. Both countries were in the top six home countries of foreign firms that invested in U.S. start-ups.[145] In addition, by studying subsequent patenting and citations in specific technology classes, the study finds that a country learns about a technology class from investing in a U.S. start-up that specializes in that class of technology.[146]

While the United States offers a single large market for European start-ups, small companies must overcome barriers to entry in 28 different countries to reach a similar market size without leaving the EU.[147] Despite ongoing efforts to build a more integrated EU "Digital Single Market," scaling across Europe is still not easy. In one study, 55 percent of SMEs in the EU, including 57 percent of start-ups and 60 percent of scale-ups, listed regulatory obstacles or administrative burden as one of the three biggest problems for their enterprise. By comparison, only 30 percent of SMEs in the United States indicated it as among their greatest concerns.[148] The ability to scale globally is critical to start-ups on both sides of the Atlantic. While about half of U.S. unicorns (start-ups with a $1 billion or more valuation) established a global presence in order to reach unicorn stage, the same is true for 70 percent of their European counterparts.[149]

The regulatory back and forth surrounding EU-U.S. data flows leave SMEs and start-ups in a constant state of legal uncertainty, even if new rules are not immediately enforced on them.[150] For those seeking to gain a foothold outside of the EU, or for globalizing U.S. start-ups seeking to enter the European market, transfer mechanisms are critical, such as EU-U.S. Privacy Shield, which was

a clear and accessible legal framework firms of all sizes and sectors could use.[151] Without Privacy Shield, SMEs and start-ups are turning to SCCs. But with the *Schrems II* ruling putting greater responsibility on data exporters and importers to determine whether SCCs are sufficient, this solution is at best inelegant and costly—and at worst, infeasible.[152]

Even for the smallest businesses, legal fees for developing SCCs can easily reach thousands of dollars.[153] The rush to align with new compliance standards also swells demand for—and with it, the cost of—legal services and other necessary external expertise, which further disadvantages firms with fewer resources. Indicative of the cost, a study by the New Economics Foundation and UCL European Institute estimates that the impact of a no-adequacy decision for the United Kingdom (and a shift to SCCs) would cost $4,120 each for micro businesses, $13,730 for small business, and nearly $27,000 for medium-sized business.[154] Given that the shift to SCCs is just one part of the impact, the total cost is likely to be higher given the impact on IT networks, staffing, and other operations.[155] These costs will price many small firms out of digital trade. [156]

Start-ups have long called for policymakers to give greater recognition to the impact data transfer rules have on them, arguing that they need to be accessible to firms of all sizes, and that they need more dedicated support to comply with new rules and regulations. U.S. and EU policymakers need to ensure their understanding of who relies on data transfers reflects reality—as it is not just large tech firms, but a diverse range of firms, including many SMEs and start-ups. In an open letter to European leadership, representatives from 14 European start-up advocacy organizations argued, "EU institutions have a responsibility to address a fundamental question: Do they stand behind a mechanism whereby data transfers to the US and elsewhere is [*sic*] possible and feasible for SMEs and startups?"[157]

SMEs and start-ups will become collateral damage if policymakers view the issue through the lens that data flows only matter to large tech firms. This fear is valid: In a 2018 Allied for Startups survey, 81 percent of respondents agreed that "the principle of designing policy and/or legislation in order to target specific companies (i.e., global giants) could lead to poor outcomes that inadvertently hurt or hinder tech start-ups."[158] As Atomico's "State of European Tech 2019" outlines, while the tech sector has grown in Europe, EU policymakers focus more on U.S. big tech than on helping and championing existing European tech successes.[159] Start-ups and SMEs need policymakers to rectify this past lack of attention and keep them in mind as they work on next steps and new data transfer mechanisms.

Consumer Internet Services: Connected, Personalized, and Valuable? Or Disconnected, Generic, and Less Valuable?

Transatlantic data flows deliver the responsive, innovative, and valuable experience individuals expect from Internet services. Every time a user opens a web page or email, plays a video, listens to a podcast, buys a product online, saves an online file, or conducts any number of other Internet-based activities, a complex data exchange takes place in the background. Companies shape user experiences within these services, such as delivering personalized search results, recommending content, and integrating advertisements in a way that complements rather than disrupts the overall user experience. Even consumers that never leave their home country benefit from international data flows, given the benefits from data aggregation and analysis, as well as simply being able to connect, communicate, and learn about people, businesses, and related content and services. These processes continue to shape the Internet users recognize today. Yet, most users and

policymakers do not understand the complexity involved in the services and IT networks required to provide a quick, seamless, and low- or no-cost service to consumer. Enacting barriers to data flows would impact all of these services. This section details the many ways in which consumer Internet services rely on data flows and the potential impacts if transfers of personal data were stopped.

Consumer Internet services (such as search, email, and social networks) are built upon open, global systems where data and information can flow freely. Firms can provide these services while abiding by non-localization-based local data privacy laws, which can differ country to country. Firms cannot escape local laws by simply transferring data overseas—as legal responsibility moves with the data, regardless of where it is stored. Ongoing cases against U.S. tech firms in Europe and elsewhere are indicative of this. And while local laws, such as GDPR, affect how certain consumer services function, they would have nowhere near the impact if Europe completely prevented the transfer of personal data to the United States.

Even consumers that never leave their home country benefit from international data flows, given the benefits from data aggregation and analysis, as well as simply being able to connect, communicate, and learn about people, businesses, and related content and services.

Given the centrality of personal data exchanges to common consumer Internet services, it is hardly surprising that IT firms are among the most-prominent users of legal mechanisms to ensure data transfers from the EU are compliant with GDPR. In a joint survey of European firms by Business Europe, DIGITALEUROPE, the European Round Table for Industry, and European Automobile Manufacturers Association, ICT companies represented 37 percent of those relying on SCCs to transfer data outside the EU.[160] While this includes many leading tech firms, there's a much bigger and broader ecosystem of firms that work as subcontractors for different tasks relating to tech firms' data processing, such as for troubleshooting or technical support services. Many of these firms were likely users of Privacy Shield. As of October 2020, about half of all firms certified under Privacy Shield (2,597) were in the ICT industry.[161]

Transfers of personal data are central to the online advertising that has powered the Internet's rapid growth.[162] Targeted advertising reduces search and transaction costs for many Internet services.[163] Advertisers bid for visibility in the fractions of a second before web content loads. Ads allow many services and content creators to monetize their work. In return, users see content, goods, and services they are most likely to be interested in. The sharing and use of information about a user, such as their browsing history or other user-specific data, allow firms to provide more-relevant ads—a benefit to both consumers who get more utility from these ads and advertisers that are willing to pay more to reach their target audience. Just as loyalty schemes operated by brick-and-mortar retail and service providers enable them to build up customer profiles, so too does personal data for Internet consumer services.

Restricting personal data transfers would likely lead to fewer and less-relevant (and thus valuable) ad services. Some opposition to advertising is driven by misconceptions about how targeted advertising works.[164] However, losing the ability to use global IT services to provide targeted and personalized advertising could cause a regression back to the old Internet, with more (and worse) types of ads (such as pop-ups and click-through ads). Users would see ads that are irrelevant. Local businesses would find it harder to find customers. It could lead to more subscription-based

services instead of free services, given the impact of less-effective ads. It would likely lead to a decrease in competition and digital economic engagement that would likely lead to higher ad costs, as their effectiveness would decrease as they would not be as useful for both advertisers and users. Many firms had to make major adjustments (e.g., requiring consent for marketing) following GDPR's introduction, but a broader block on the transfer of personal data would make the issue much harder to work around.[165]

Personal data transfers also allow Internet services to identify and authenticate individual users when they are logged in to their unique account and provide them with seamless access to multiple applications and the information, goods, and services they want. Many Internet services use a single sign-on (SSO) so users can use just one (instead of several) set of login credentials for multiple applications, whether it be a person's Facebook account, their GAIA (Google Accounts and ID Administration) ID, or their Microsoft Office SSO.[166] These could also be external, in that a user could use their Facebook, Twitter, or Google login to authenticate a user for a third-party service.

Beyond simply recognizing a returning user, SSOs are the gateway for the valuable and useful personalized services that drive people to use Internet-based services. They allow firms to provide a single, personalized experience across services, whether it is email, search, photos, maps, videos, news, chat, or other connected services—as well as embedded services such as search and sharing functions for photos and other content. Data flows provide users with seamless access to these personalized services from anywhere, anytime, and on any computer or device.

Many European policymakers do not understand the impact restrictions on data flows would have on their local Internet experience. As noted, while it may be technically possible for a large firm to achieve local data storage, there would still be major disruptions and changes to the types and quality of Internet services, especially between those used in and outside of Europe. The true complication of data localization in Europe is the impact on data analytics and other data-driven services. Email account login notifications and credit and bank alerts about potentially fraudulent transactions or activity would be inhibited as users would live in separately engineered IT worlds. It would mean that global providers would have to engineer ways into and around Europe, as many common (and common-sense) features rely on transfers of personal data. Data localization would make these far more complicated, degraded, or impossible.

Ultimately, severe restrictions on the transfer of personal data would lead to users in Europe having a markedly different Internet experience than that of global users. Many firms would be forced to provide less-personalized and less-valuable services more akin to generic "signed out" services (in that many users would not have to sign in to use many Internet services). These firms would still be able to service ads to users, but they would not be personalized (and thus would be less valuable to both users and organizations that use targeted advertising in Europe). Customers have grown to expect these personalized services, as have businesses (especially retailers) gotten used to providing them.[167]

Furthermore, restrictions on personal data transfers mean that related services become biased by users within that region. Search results for users in a restricted European data region would become biased by users within that region as the search service would not be able to aggregate that data with data from users outside the region in providing the most relevant and accurate results. For example, with videos, a company's algorithm is likely to look at what a user has already viewed, so it'll find content and ads that it thinks would appeal to the user. Many services such as

these do not look specifically at the person when providing personalized services, but at what other similar users have viewed, much like Netflix's recommendation algorithm.[168] So a search in a country/region with personal data localization would show results that are shaped by a smaller group of users (who may be very different from the individual user). The search service wouldn't be able draw on data from people that are actually more like the user, meaning their Internet experience would be degraded. In essence, it would move the result from an individualized to an aggregated country/regional experience.

Social media networks would also be disaggregated based on the ability of firms to transfer the personal data that connects friends and families (such as on Facebook), professional contacts and work and business opportunities (LinkedIn), and businesses with potential customers. It would be incredibly difficult—if not impossible—for online social networks to operate in a fully localized Internet ecosystem, as Facebook has already noted to European policymakers.[169] Policymakers need to realize that targeting social networking sites such as Facebook would have broad economic effects.

Segregated personal data regimes would not break the technical infrastructure that makes up the Internet, but it would go a long way toward breaking the way the Internet works at the application layer and in defining and differentiating the Internet experience of users in each realm.

Social networking sites are increasingly seen as a business and trade tool, and an essential part of marketing and advertising strategies, whether it is TikTok, Facebook, Instagram, or LinkedIn. Much like the impact on advertising, limitations on social networks inevitably affect firms that use them to find and serve customers in other markets.[170] Advertising through social media is much cheaper than other forms of traditional advertising—hence, in 2017, nearly half of all EU enterprises used social media for advertising purposes.[171] E-commerce and brick-and-mortar retailers account for a large portion of advertising revenues for social networking sites, so any reduction in the value of advertisements is most likely to affect this sector.[172] Similarly, from a small package trade perspective, it would mean that customers would be less likely to see goods or services on e-commerce platforms from other countries (that may actually be closer to what those customers actually want).

Overall, allowing firms to transfer and process personal data results in a better online experiences for both users and businesses. Segregated personal data regimes—whether between the United States and Europe, the United States and China, or Europe and China—would not break the technical infrastructure that makes up the Internet, but would go a long way toward both breaking the way the Internet works at the application layer and defining and differentiating the Internet experience of users in each realm. Such a scenario—which is where the global Internet is heading—lends itself to policymakers using personal data restrictions as a tool for digital protectionism, as it allows them to pick and choose their favored (local) Internet service provider, with each data realm having its own local social network and search and email provider, for example. This is fundamentally different from the current situation wherein personal data, advertising, and digital technologies such as cloud computing have allowed many Internet services to provide a nearly ubiquitous, easily accessible, and valuable service to people around the world—often for free.

Maximizing the Benefits of Transatlantic Health Data Transfers

From screening chemical compounds to optimizing clinical trials to improving post-market surveillance of drugs, the increased use of data and better analytical tools, such as AI, hold the potential to transform health care and drug development, leading to new treatments, improved patient outcomes, and lower costs.[173] Given what it reveals about an individual, health information is among the most sensitive of data categories. At the same time, its potential to improve and save lives also makes it one of the most valuable. While policymakers need to be certain that health data is carefully protected, they also need to ensure that legal frameworks allow for the reasonable, responsible, and ethical sharing of data—including transatlantic sharing—given the enormous potential social and economic benefits of new and improved health services.[174] Unfortunately, there's a real risk that GDPR will impede transatlantic health research.

Data and digital technologies are transforming the life sciences sector. For example, Johnson & Johnson uses a real-time, cloud-based system to connect and share data between internal and external units and manufacturers in order to monitor and better control production processes, while abiding by relevant security, data privacy, and compliance requirements.[175] The mainstreaming of genome sequencing is set to increase the number of patients who undergo the procedure, the number of research opportunities, and the range of health care professionals who will require access to genetic and health data.[176] The emergence of learning health systems is blurring the traditional boundary between clinical research and care, as data is collected routinely in the process of care, with the explicit aim improving health care outcomes.[177]

While policymakers need to be certain that health data is carefully protected, they also need to ensure that legal frameworks allow for the reasonable, responsible, and ethical sharing of data.

COVID-19 has accelerated the life sciences sector's digital transformation. Most pertinently, COVID-19 researchers have needed digital tools and data flows in order to run the biggest experiment of their lives, in record time.[178] For example, firms have had to set up digital monitoring operations at production facilities to maintain compliance with safety and quality control requirements. Pfizer rolled out a virtual reality-based capability that enables the remote diagnosis and repair of equipment; and in distribution, it developed dashboards to track and manage supply chains.[179] Firms have also revised operations to reduce the amount of in-person contact necessary for clinical trials, such as by using wearables to communicate with patients and monitor their condition. The effort to fight COVID-19 has brought traditional health and life sciences firms together with tech firms to figure out ways to improve health care.[180]

This section details the critical role data flows play in driving transatlantic life sciences research, including a case study on diabetes and Alzheimer's research, how regulatory agencies on both sides of the Atlantic depend on data transfers to research and regulate new health products in their respective jurisdictions, and how GDPR already makes it difficult for firms to transfer health data. This analysis confirms that, after *Schrems II*, these processes are only going to get more difficult, costly, and complicated.

Data Transfers Drive Transatlantic Life Sciences Research

Health research is increasingly an international endeavor that depends on the aggregation and sharing of personal data. Life sciences research is global, so data should be able to move among

democratic, rule-of-law nations. There is a real risk of overly restrictive data privacy rules in Europe (as well as elsewhere) impeding the critical role data transfers play in supporting the use of AI and other digital technologies to come up with health breakthroughs that hold potentially enormous societal and economic benefits.

Health data transfers make health research better for many reasons. Research into rare and extremely rare diseases (from those that occur in 1 in every 10,000 to as rare as 1 in every 1 million people) best highlights the need to allow data flows and aggregation—as otherwise it's significantly harder to identify and collect enough data in each and every country, given how many of them have only small patient populations.[181] American and European researchers need to be able to pool data from across the Atlantic and around the world to improve their ability to properly conduct clinical trials. Along the same lines, aggregating data across borders also allows the robust examination of the penetrance (the proportion of people with a particular genetic change) of disease and the study of heterogeneous diseases, such as cancer.[182]

Health data transfers, aggregation, and analysis create new, more diverse, and valuable datasets with enduring research value. The aggregation and availability of personal data allows new scientific questions to be asked of existing data, whether in regard to discovery, hypothesis generation, or external validation of predictive models. In this way, repurposing existing data for novel research purposes means that the resources required to collect personal data are greatly reduced. Larger databases would allow researchers to better assess risks of bias, while new digital technologies and data transfers would lead to both larger and more diverse datasets, as firms increasingly use non-clinical sources of data, such as from wearable technologies, as part of their research. This is indicative of how the future of clinical trials will involve using more diverse and complex data from stakeholders other than the pharmaceutical industry itself.

In this way, the ability to transfer and share health data maximizes the potential for individual researchers and life sciences firms—regardless of location—to advance scientific knowledge.[183] The Global Alliance for Genomics and Health has stated that the availability of large cohorts (10 million-plus people) representing individuals from different populations throughout the world would be transformative for human research.[184] The Matchmaker Exchange Project (involving a global set of partners) aims to facilitate the matching of cases with similar genomic profiles.[185] As of 2017, it had produced nearly 30 matches involving patients in different countries.[186] Similarly, the Cascadia Data Discovery Initiative (which involves Microsoft, the Fred Hutchinson Cancer Research Center, and a range of other research partners in Canada and the United States) aims to create a more integrated and productive health data ecosystem that focuses on enabling collaboration and data sharing.[187] Recognizing the difficulties in aggregating data to support AI—especially internationally—the initiative aims to build a framework for cross-institutional data governance and create a shared data ecosystem across partners.[188]

Seamless health data transfers are critical to maximizing the power of the digital technologies that are driving health care innovation, especially cloud computing and AI. Cloud services provide researchers with the computing power needed to search vast libraries of molecules for potential cures. Experts anticipate genomics will play an increasingly important role in cancer diagnoses, and leading scientists expect to see 83 million genome sequences for cancer worldwide by 2025, which is generating huge volumes of data that will be impossible to analyze efficiently without cloud computing.[189] For example, as part of the COVID Moonshot initiative, UCB (a Belgian drug

company) shifted from internal to cloud-based services (in this case, Microsoft), which increased its data-analytics capacities sixfold. UCB's CEO estimates that this increased power shortened a six-month screening process—that involved data in both the United States and Europe—into three days.[190] Similarly, Takeda Pharmaceuticals used cloud services (in this case, AWS) to create a data sharing and clinical trials acceleration program that took only five days, when it'd normally take around three months.[191]

The U.S. Food and Drug Administration's clinical trials database shows how critical EU-U.S. cooperation is for life sciences innovation.

Whether for drug discovery or clinical trials, AI is critical to helping researchers by making the process of analyzing the sheer amount of data that can be generated from computer simulations faster and more precise. Compared with traditional methods, AI can shorten the time it takes to synthesize and screen new drugs by 40 to 50 percent, thereby reducing costs in those parts of the research process by as much as $26 billion annually. In the clinical research phase, AI can cut costs by $28 billion per year, and reduce the phase's length by half or more.[192] For example, Merck improved one of its vaccines by conducting 15 billion calculations to determine which environmental and process factors influenced the quality of the final product.[193] Takeda Pharmaceuticals plans to pair every employee with an "AI assistant" to help advance drug discovery.[194]

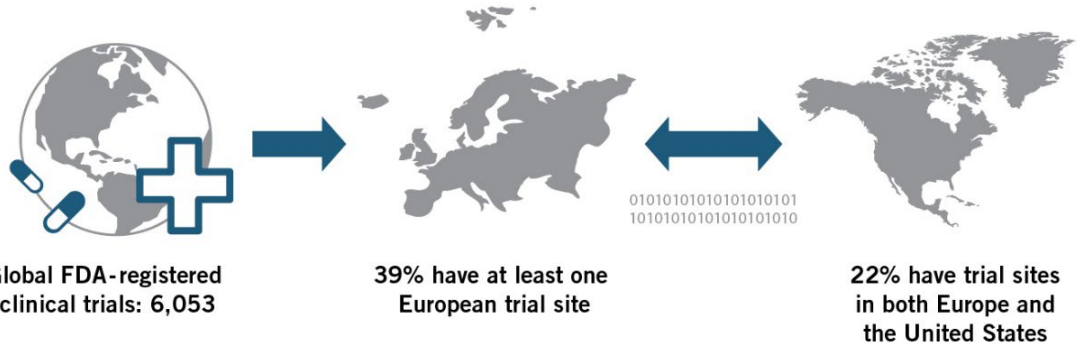
Data privacy frameworks play a critical role in not only supporting, but also preventing, international health research—GDPR already makes transatlantic health research increasingly uncertain and difficult. There's clearly a need for reforms and greater legal clarity and certainty. Indicative of this, the global Pan-Cancer Analysis of Whole Genomes consortium has called for an international code of conduct for genomic data sharing, noting the difficulty it faced in developing a single cloud of data accessible to researchers worldwide due to "European regulators having concerns about genomics data from Europeans being held in the United States."[195]

Transatlantic data transfers are critical to the clinical trials involved in modern drug discovery. As far back as 2010, 80 percent of applications for drugs and biologics contained data from clinical studies conducted outside the United States.[196] Although data from clinical trials is often anonymized, demographic details about each participant still need to be included. Clinical trials are often conducted by third-party vendors with country-specific expertise and relationships with hospitals and the research facilities necessary to conduct high-quality trials. Multi-country clinical trials are preferable, as they typically include a more diverse set of participants. Global clinical trials are especially crucial to rare disease research, as the patient population of a single country will likely not have enough potential participants for a valid clinical trial.[197]

The U.S. Food and Drug Administration's (FDA) clinical trials database shows how critical EU-U.S. cooperation is for life sciences innovation—in February 2021, there were 1,303 active, industry-funded clinical trials in both the United States and the European Economic Area (EEA). Of these, 39 percent had a clinical trial in at least one European country, while 22 percent had clinical trials on both sides of the Atlantic (see figure 10).[198] COVID-related clinical trials make this clear: Of the 97 COVID-19-related clinical trials registered with the FDA, 12 involve the EEA, 6 of which involve both EU and U.S. trial sites. This includes such treatments as canakinumab (for patents with

COVID-19-induced pneumonia) and ruxolitinib (for patients battling the cytokine storm associated with COVID-19). It also includes the full spectrum of health conditions, with a number of transatlantic studies targeting many types of cancer, arthritis, asthma, HIV infections, lupus, epilepsy, and more.

Figure 10: Health data transfers are critical to the many FDA-registered clinical trials in both the United States and European Economic Area (EU plus Iceland, Liechtenstein, and Norway)[199]



Case Study: Restrictions on Data Transfers Affect Research on Diabetes and Alzheimer's

GDPR has become an impediment to transatlantic life sciences research for the U.S. National Institutes of Health (NIH) and on diabetes and Alzheimer's. Since 1993, the NIH and Finland's own National Institute for Health and Welfare have been engaged in a joint research project studying type 2 diabetes in Finnish people. Finnish and U.S. researchers used data from 32,000 DNA samples to discover more than 200 places in the genome where variants increase the risk of illness. However, in May 2018, when GDPR came into force, the Finnish institute stopped all data sharing on the project because NIH could not provide guarantees that would satisfy the institute's interpretations of the law's requirements. NIH cannot use SCCs because of their requirement that institutions either agree to European audits of their data systems or submit to the jurisdiction of its courts—which NIH, as a U.S. government agency, cannot accept. NIH and its Finnish partner are working to find a solution, based around how best to define the transfers as necessary for the public interest.[200]

Similarly, GDPR has undermined data sharing for the International Genomics of Alzheimer's Project—the largest ever Alzheimer's gene study.[201] Researchers from the United States and Europe gathered DNA sequences from more than 90,000 people to find genetic variants associated with Alzheimer's disease. But since GDPR, some EU nations have restricted data sharing, so the consortium now runs separate analyses on each side of the Atlantic. As co-founder neuroscientist Sudha Seshadri of the University of Texas Health Science Center in San Antonio noted, this limits analysis, particularly when searching for rare variants that require big datasets.[202]

GDPR Makes It Hard, If Not Impossible, for Health Data Transfers to U.S. and International Public Health Agencies

Firms and institutions need to be able to transfer health data as part of the regulatory approval process for new drugs and health products. Whenever a firm applies to the FDA to investigate a new drug, it must still comply with all relevant FDA regulations even if the clinical study is conducted outside the United States.[203] Data from clinical trials must be shared with the FDA

during the approval process. Adverse events during clinical trials or after a medicine has made it to market also must be reported to regulatory bodies. Quality control and testing data during the manufacturing process also need to be shared with the FDA.

Even before *Schrems II*, GDPR made health data sharing between public bodies difficult to impossible. For example, after GDPR was enacted, the Statens Serum Institute in Copenhagen (which houses the Danish National Biobank) suspended data transfers to important partners, including the NIH and the World Health Organization's International Agency for Research on Cancer (based in Lyon, France).

As mentioned, SCCs are not viable when the recipient entity is an arm of the U.S. government, such as the NIH or public universities, because the U.S. government cannot agree to certain terms in SCCs, including dispute resolution in European courts.[204] Similarly, U.S. state entities (including state universities and public hospitals) often cannot agree to certain terms due to restrictions in state and local laws. Given the large amount of research that is funded by the NIH or that involves U.S. public universities or academic medical centers, the inability to rely on SCCs has proved a major obstacle to transatlantic health research. [205]

GDPR also restricts data transfers to international organizations involved in health research and services. For example, the large scale and broad membership of many genomics projects mean these "data controllers" count as an international organization under GDPR.[206] Organizations such as the European Molecular Biology Laboratory (which is headquartered in Heidelberg, Germany) has legal standing as an intergovernmental organization, given it is a subject of, and governed by, international law. Transfers of personal data to international organizations may be even more difficult than to non-adequate third countries, given how difficult it is to assess the "adequacy" of an international organization (e.g., How does an international institute provide available judicial remedies?)[207] The EDPB is conscious of this challenge in approving more flexible alternative "redress mechanisms" where SCCs are impossible, such as arbitration.[208] But again, this advice is hardly clear and comprehensive, proving wholly inadequate as it relates to the many and varied issues GDPR raises for international health research.

Transatlantic Health Data Sharing Benefits Everyone: But It Is Getting Harder, More Costly, and More Complicated

Restrictions on the transatlantic transfer of data for health research would ultimately detract from the potential to use that data for the greatest public good. Data localization and data sovereignty would hurt everyone on both sides of the Atlantic, given it would inevitably lead to less health-related innovation and poorer health outcomes.

As previously highlighted, GDPR already adversely affects global health research.[209] The European Court of Justice's (ECJ) decision in *Schrems II* is likely to make it even worse.[210] Furthermore, in April 2020, as part of COVID-19 related guidance, the EDPB formally recognized COVID-19 as an important public interest and said that addressing it may involve private firms and public bodies transferring data to third countries. But, as to be expected, this is a very narrow and technical view that does not lend itself to a broader, supportive framework that is needed for health data transfers and research.[211]

The invalidation of the EU-U.S. Privacy Shield will affect hundreds of firms in the health and life sciences sectors. It was an important complementary legal mechanism for many firms, especially

SMEs and third-party vendors. As at October 2020, 293 firms—around 6 percent of all firms—in the health care IT industry were certified under Privacy Shield.[212] Broken down by sector, this involves 137 health IT firms, 90 biopharmaceutical firms, 56 medical device firms, and 36 health care service firms.[213]

Meanwhile, SCCs for health data—even before *Schrems II*—are complicated and costly. For example, a University College of London (UCL) European Institute and New Economics Foundation study into the issue (in the context of U.K.-EU data flows) finds that the cost of drafting and negotiating SCCs for medical research is vastly more expensive than for other sectors, costing $68,000 to $136,000 for a data sharing agreement between a U.K. university and a U.S. organization receiving data and tissue samples.[214] Potential EDPB post-*Schrems II* changes to SCC would likely only make them even more complicated and costly.

GDPR's impact on transatlantic health research is made worse as individual EU member states are also pursuing restrictive health data policies, which makes legal compliance for life sciences and health firms that much harder and more complex. France's recent efforts to create its own local health data hub are indicative of the broader fragmentation (and digital protectionism) within the EU.[215] Creating its own health data hub was one of France's major initiatives under its AI strategy.[216] In October 2020, the country's highest court rejected efforts by the government and others to force data to be transferred from Microsoft to a local provider due to concerns over U.S. government surveillance. The judges noted that the case was purely hypothetical, that the data was pseudonymized before it was added to the hub, and that in light of the COVID-19 pandemic, there was an important public interest in allowing the continuous processing of health data as enabled by the health data hub.[217]

These existing and new barriers to transatlantic health data transfers and research highlight the critical need for broader political engagement and policy reforms by European policymakers. Patients, life sciences researchers, manufacturers, and IT and health service providers need a clear, predictable, and practical data protection and sharing framework. Instead, what they largely have now is a restrictive, complex, and uncertain set of compliance requirements that impede their ability to innovate and provide more and better health products and services. Health data is obviously incredibly sensitive and deserving of detailed privacy and data protections. But data protection, transfers, and innovation are not mutually exclusive. It is a matter of policymakers developing clear and predictable frameworks for the collection, use, and sharing of personal health data to provide a much better balance between privacy and innovation interests.

POLICY RECOMMENDATIONS

The key question is where do the United States and Europe go from here? The sectoral case studies show the broad and significant role data flows play in transatlantic commerce. The following recommendations provide ideas for how the two sides could build a better, stronger, and broader transatlantic digital relationship.

Negotiate a New Privacy Shield

The EU and United States should initiate both short- and long-term initiatives to build a durable and comprehensive data protection framework that manages the interests of individuals, firms, and governments.

EU policymakers should not pursue the issue through the singular lens of privacy or put their hopes on the United States enacting GDPR-like data privacy to solve the issue. Any pursuit of data privacy harmonization—which assumes that if only the United States and the rest of the world enacted GDPR, everything would be fine—is unrealistic. To their credit, leading EU officials involved in past EU-U.S. privacy negotiations have generally avoided this approach. But many other European officials are more aligned with privacy fundamentalists (or those that use the issue of privacy as a disguise for protectionism). The United States may well (and should) enact a comprehensive data privacy bill, but it is unlikely any such law would address the underlying issues regarding surveillance and government access to data. A comprehensive data privacy bill would likely improve the context for transatlantic cooperation on digital issues, but cooperation would still need to be based on pragmatism and the need to build mechanisms for sharing between different regimes. Policymakers on both sides would be well served to remain firmly rooted in this realization and the need to balance multiple interests and different data privacy and national security systems.

Any pursuit of data privacy harmonization— which assumes that if only the United States and the rest of the world enacted GDPR everything would be fine—is unrealistic.

Ultimately, the EU and United States need to negotiate a new Privacy Shield. Given the legal uncertainty regarding many transfers (with Privacy Shield's invalidation and the EDPB's overly strict guidance about transferring data to third countries such as the United states), ideally, the EU would provide a short-term bridging mechanism. As this report shows, many firms and sectors have relied on the ability to transfer personal data for critical economic and social purposes during COVID-19. As the Biden administration takes its time to "get going," legal uncertainty only continues to grow, while court cases, EDPB guidance, and data protection authority (DPA) decisions make transfers extremely difficult or even impossible. Even if such a new bridging mechanism were time limited, it would be extremely useful in providing breathing room for the administration to start addressing both the Privacy Shield and broader EU-U.S. digital issues.

Thankfully, the EU and the United States have pledged to work together in good faith to come up with a successor to Privacy Shield.[218] Exactly what that successor agreement should look like—in light of the Court of Justice of the European Union's concerns—is hard to say. For example, the ombudsperson established by Privacy Shield to hear complaints about unnecessary access to data could be given greater independence, just as the United States has independent agencies across its government. Any new agreement will be the product of negotiations, and inevitably will need to balance the various interests involved, including national security.

Long term, the EU and United States could work toward legislation and a treaty agreement that would codify some of their commitments, especially around government access to data and restrictions around data localization. For example, legislation could address concerns that informal guidance or even agency policies are not "established in law," and therefore would not be as effective as a statute or other binding legal instrument.[219]

In an ideal world, after building a new transatlantic data privacy framework, the United States and Europe would work together with like-minded countries to develop a "Geneva Convention for Data" to establish international rules for transparency, settle questions of jurisdiction, engender

cooperation for better coordination of international law enforcement requests, and limit unnecessary government access to data on citizens of other countries.[220] This would also help countries follow similar rules and procedures for cross-border law enforcement requests and actions. And it would address the issues of localization and barriers to data flows, with parties agreeing not to enact data localization (as this would undermine the central point of the agreement).

EU Should Redouble Efforts to Build New Data Transfer Mechanisms Under GDPR

Firms are evaluating alternative transfer mechanisms to Privacy Shield and SCCs, but these mechanisms are few, hardly comprehensive, and not readily accessible and applicable for many firms.[221] The only truly comprehensive alternative for firms is to shift their data transfer activities to countries with adequacy decisions, which are those whose legal regimes are deemed by the European Commission to provide for an "adequate" level of personal data protection. However, the countries with adequacy decisions is only a small and disparate group of 12 nations (mainly former colonies). Binding corporate rules (BCRs) are among the few alternatives some (large) firms already use to transfer EU personal data overseas, but they are only for intra-firm data transfers. While the ECJ decision in *Schrems II* upheld SCCs as a valid transfer mechanism, it also added new compliance requirements and exposed individual SCC-based transfer agreements to further legal challenges. Likewise, BCRs may also face further legal challenges. EDPB guidance is likely to make SCCs harder and more complex, if not impossible, to use to transfer EU personal data to the United States.[222]

The EU and its member states need to reconcile privacy with their other interests instead of letting concerns about the former (largely driven by civil society advocates who privilege privacy concerns over almost everything else) outweigh the latter (as every country inevitably does in balancing human rights and economic, health, security, and other rights and interests). From an economic and trade standpoint, the EU recognizes that digitization has transformed the global economy, and the transfer of data, including personal data, across borders is part of the daily operations of European companies of all sizes, across all sectors. It also recognizes that these commercial exchanges rely on personal data flows, and protecting and exchanging personal data are not mutually exclusive.[223] It knows that greater compatibility between different data protection systems facilitates international flows of personal data as part of global trade (and as part of cooperation between governments, such as on law enforcement and surveillance).[224] Yet, as this report shows, GDPR does not provide a broad, varied, and accessible tool kit for firms to transfer personal data out of the region.[225] The European Commission and EU member states need to ensure that Europe's approach to privacy better reflects these broader aspirations and interests.

Obviously, the EU's priority should be to negotiate a new Privacy Shield agreement and make SCCs and BCRs clear, predictable, and accessible. However, in line with making GDPR truly accessible and adaptable, the EU should also ramp up efforts to enact codes of conduct and certification schemes to provide a broader, flexible set of legal tools for firms from different sectors to manage data reasonably and responsibly under GDPR.[226] U.S. firms should have the opportunity to participate in these discussions. Certifications are a voluntary mechanism for organizations to validate their compliance with GDPR, while codes of conduct are created by stakeholders in specific sectors (both public and private) to resolve data protection challenges, with assurance from DPAs that the respective codes, and the monitoring thereof, are appropriate and compliant with GDPR.[227] Both tools allow firms to demonstrate compliance with GDPR. Indicative of the lack

of progress toward developing alternative transfer mechanisms, the cloud sector (including European, U.S., and other firms) developed and submitted a code of conduct to the EDPB years ago, which still has not yet been approved.[228]

The EU should ramp up efforts to enact codes of conduct and certification schemes to provide a broader, flexible set of legal tools for firms from different sectors to manage data reasonably and responsibly under GDPR.

There have been some discussions on potential codes of conduct for the market research, health research, and clinical research services sectors, but they do not appear anywhere close to final.[229] In light of the life sciences case study of this report, one idea for specific attention is for EU and U.S. stakeholders to work together to develop a certification for genomic data sharing. Concerns about the ethical, technical, and administrative processes for genomic data could be addressed via the development and use of new international standards. Such a certification could form part of a broader effort to develop a code of conduct for genomic data sharing. Together, these two legal mechanisms would provide legal certainty for all stakeholders, while still allowing them to use data for innovation.[230]

Improve Transatlantic Law Enforcement Cooperation and Data Requests

The United States and EU should conclude negotiations to improve transatlantic access to electronic evidence for law enforcement investigations. Just as both sides ultimately benefit from the sharing of intelligence information that *Schrems I* and *II* affect, both benefit from the better exchange of data for law enforcement purposes. Negotiations started in September 2019. An agreement would complement and build upon the existing EU-U.S. Umbrella Agreement, the EU-U.S. Passenger Name Records Agreement, and the Terrorist Finance Tracking Programme. These agreements are indicative of the fact that the United States and EU have one of the most sophisticated law enforcement relationships, one that provides a solid foundation of trust and goodwill to address other data-related issues.[231] However, this cooperation and these agreements cannot be taken for granted as they come under review following *Schrems II*.[232]

Electronic evidence is needed in around 85 percent of criminal investigations; and in two-thirds of EU investigations, there is a need to obtain evidence from online service providers based in other jurisdictions.[233] Given it is home to many leading Internet service providers, the United States receives a growing number of requests from Europe and the rest of the world. For example, requests to the principal online service providers increased 84 percent from 2013 to 2018.[234]

The United States and EU should conclude negotiations to improve transatlantic access to electronic evidence for law enforcement investigations.

The problem is the current legal framework for managing law enforcement's cross-border requests for data is out of date and far too slow. A new agreement would improve law enforcement investigations while accounting for privacy and other concerns. It would provide Internet service providers with a clear legal framework to manage requests, and remove a motivation that some policymakers elsewhere around the world have used to try to justify data localization (in terms of facing issues with working through existing legal frameworks to access data stored overseas).

Thankfully, both the United States and Europe recognize that they need to update their respective legal frameworks, which is indicative of their ability to look past ongoing conflicts regarding transatlantic data governance. In 2018, the U.S. Clarifying Overseas Use of Data (CLOUD) Act came into force to do this. The United States can negotiate CLOUD Act agreements with other countries to create updated frameworks to manage law enforcement requests for data. So far, it has concluded an agreement with the United Kingdom and launched negotiations with Australia and the European Union. Meanwhile, the EU's e-Evidence initiative includes the mandate to negotiate new agreements with the United States.[235] Whether an agreement is concluded under the CLOUD Act or some other legal mechanism, it's important that both sides address this issue as part of building a broader, constructive transatlantic relationship.[236]

Build a Transatlantic Agenda Based on "Digital Realpolitik"

The EU and United States should build an agenda for pragmatic and practical cooperation on data and digital policy issues—one based on "digital realpolitik" and not some one-sided push for a harmonized approach that will never come. The European Commission's recent call for a new EU-U.S. Trade and Technology Council, including on data flows, cybersecurity, digital governance, and a transatlantic AI agreement, is welcome.[237] It reflects the fact that the United States and EU's long-standing science and technology cooperation needs a digital upgrade.[238] However, any such agenda needs to be based on a mutually beneficial, constructive, and pragmatic agenda.

Too often in the past, such calls from Europe were based on the expectation that the United States would simply do what the EU does. This is not the basis for genuine collaboration on bilateral, regional, or global issues of mutual concern. The EU's drive for harmonization to its approach to data privacy and digital regulation is a roadblock to building global consensus around these issues, as few countries would ever align their approaches precisely with Europe's, and instead would adapt privacy (and other digital policy) issues to their own system. However, countries can work together to develop shared principles (based on shared values), with an overarching goal of building broadly similar and interoperable approaches to digital regulations.[239]

Transatlantic cooperation based on genuine shared values and "digital realpolitik" is needed now more than ever. Europe and the United States have 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. However, it will require both sides to either back down, resolve, or relegate bilateral irritants in order to focus on shared strategic concerns around data and technology and find new, emerging issues to work together on to develop a coordinated response (before it becomes another potential point of conflict).

Europe and the United States have 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 the EU and the United States want emerging global norms to reflect their many shared values, they need to work together. Otherwise, fragmentation and protectionism will continue to undermine any chance of these countries working together to create an open, rules-based, and innovation-friendly global digital economy.

The EU and United States could work on a range of data and digital policy issues, such as:

- How to develop mutually beneficial—and accessible—data sharing frameworks, including for both public and private data. These frameworks could address various types of data, including sensitive commercial data and sensitive government data, that may have high value but be difficult to share under existing rules. In addition, this framework could address interoperable mechanisms for allowing individuals to donate their data for public benefit to both commercial and non-commercial entities. The EU and United States could also work to establish common data pools and shared guidance on best practices for responsible and ethical data collection, analysis, and sharing (as in the idea for genetic data sharing).[240] Both sides could explore how to use data trusts and other data sharing models to improve the quality (and quantity) of datasets. This type of cooperation is important because advances in AI, especially machine learning, needs access to good data, not just more data.[241]

- How to develop and apply the appropriate regulation of AI, such as via algorithmic accountability, which is the principle that an algorithmic system should employ a variety of controls to ensure the operator (i.e., the party responsible for deploying the algorithm) can verify it acts in accordance with its intentions, as well as identify and rectify harmful outcomes.[242] Consistent with the OECD Principles on AI, the two sides could discuss the development and adoption of AI and how they could ensure their respective emerging regulatory approaches are interoperable. In particular, this could address algorithmic accountability in key sectors such as health care, banking, finance, and military applications, where the increased use of algorithms and automation may require new types of oversight. Similarly, joint efforts to provide feedback to industry on the responsible use of AI in areas directly affecting individuals, such as employment, would ensure that the companies developing and using the technology have an opportunity to receive the important ideas and perspectives from both EU and U.S. stakeholders.

- How to develop interoperable electronic identity systems that allow for greater interaction, security, and privacy online. As both the EU and the United States continue to explore new electronic ID systems, in parallel with private sector initiatives to improve identification and authentication technologies, it would be helpful to consider how joint efforts could help establish a global, multilayered, interoperable system of electronic identification for individuals, businesses, and devices. With a shared goal of increasing trust in the digital economy, improving electronic identification is an important opportunity.

- Building pre-standardization cooperation for new and emerging technologies.[243] Both the United States and Europe recognize the critical role standards play in modern trade. As the conflict over data privacy shows, identifying how to make existing standards and regulatory systems compatible between different regimes is a legitimate, albeit complicated, process. However, both sides could work together on pre-standardization cooperation on new and emerging technologies so their respective firms have the advantage of basing their technology on the same foundational, technical elements (in terms of terminology, measurement methodology, and other technical processes) as another leading tech-driven trading partner. All of this could be done well before standards are finalized and part of regulatory systems that are much harder to change once enacted. Such transatlantic and

global pre-standardization cooperation has proven useful for advanced material testing, nanotechnology and nanomaterials, and health-related measurement.[244]

- Cooperating on standardization and conformity assessment issues related to data and digital technologies. As part of broader efforts to counter China's attempts to unduly influence international standards, the United States and Europe need to ensure their respective approaches are aligned and compatible.[245] Given the debate over standards is a global one, it would be ideal if their respective approaches relied on global, industry-driven, voluntary consensus standards to demonstrate conformity with new and emerging regulatory requirements. Moreover, it will be important that emerging technologies are not banned based on country of origin but rather only on specific and objective threats.

- Developing a coordinated strategy to counter China's efforts to unduly influence international standards setting for AI and digital policies in ways that are either discriminatory (from a trade perspective) or based on social and political values that are at odds with democratic values and human rights. Standards are a key tool in the global race for innovation and trade advantage in new and emerging technologies, whether it's 5G, AI, data privacy, facial recognition, advanced manufacturing, digital finance, or other sectors.[246]

- Cooperating and coordinating investment screening and export controls, as they increasingly relate to data and digital technologies.[247] Changes to export control and foreign investment screening laws in the United States, the European Union, and elsewhere over the last few years have increasingly addressed concerns about data and digital technologies. The United States, the EU, and individual EU member states should work together to share experiences and best practices to ensure that their respective approaches are broadly aligned.

CONCLUSION

This latest data transfer crisis will likely prove decisive in determining whether the transatlantic digital relationship will survive and thrive or be further undermined and diminished. Whether the United States and Europe can work together to rebuild the transatlantic relationship holds much broader implications. Severing transatlantic digital engagement and cooperation would accelerate the fragmenting of the global digital economy, as it would reflect a fundamental fracture between two key players, which would only help China. Forward-looking policymakers on both sides of the Atlantic need to recognize this and redouble efforts to build a better, stronger, and broader transatlantic digital relationship.

Acknowledgments

This report was made possible in part by generous support from Facebook. The authors wish to thank Daniel Castro and Kevin Gawora for their contributions. 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.

Ellysse Dick (@Ellysse_D) is a policy analyst 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 an independent, nonprofit, nonpartisan research and educational institute focusing on the intersection of technological innovation and public policy. Recognized by its peers in the think tank community as the global center of excellence for science and technology policy, 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. Nigel Cory, Daniel Castro, and Ellysse Dick, "'Schrems II': What Invalidating the EU-U.S. Privacy Shield Means for Transatlantic Trade and Innovation" (ITIF, December 3, 2020), https://itif.org/publications/2020/12/03/schrems-ii-what-invalidating-eu-us-privacy-shield-means-transatlantic.
2. Nigel Cory et al., "The Role and Value of Standard Contractual Clauses in EU-U.S. Digital Trade" (ITIF, December 17, 2020), https://itif.org/publications/2020/12/17/role-and-value-standard-contractual-clauses-eu-us-digital-trade.
3. European Data protection Supervisor, "Strategy for EU Institutions to Comply with 'Schrems II' Ruling," edps.europa.eu, October 29, 2020, https://edps.europa.eu/press-publications/press-news/press-releases/2020/strategy-eu-institutions-comply-schrems-ii-ruling_en; Nigel Cory et al., "The Role and Value of Standard Contractual Clauses in EU-U.S. Digital Trade" (ITIF, December 17, 2020), https://itif.org/publications/2020/12/17/role-and-value-standard-contractual-clauses-eu-us-digital-trade.
4. Reflecting the central principle of accountability that is at the heart of most countries' data privacy frameworks (including GDPR). Nigel Cory, Robert D. Atkinson, and Daniel Castro, "Principles and Policies for "Data Free Flow With Trust" (ITIF, May 27, 2019), https://itif.org/publications/2019/05/27/principles-and-policies-data-free-flow-trust.
5. For example, many firms that used Privacy Shield are headquartered or have offices in the EU. 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). 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/.
6. For example, the European Commission's data strategy has many worthy goals, such as making it easier to share commercial data in nine different sectors; however, the strategy asserts that the EU needs cloud providers to be owned and operated in Europe, implying that U.S. cloud providers are neither secure nor trustworthy, despite the fact that they remain best equipped to support EU digital development. Yet, the United States is not calling for 5G equipment sovereignty despite the fact most of the equipment U.S. carriers will buy is from Ericsson and Nokia, two European companies. Similarly, the European Commission's Data Governance Act has many good ideas, but they are overshadowed by restrictions on processing certain types of data outside the EU. European Commission, "A European Strategy for Data," ec.europa.eu, November 25, 2020, https://ec.europa.eu/digital-single-market/en/european-strategy-data; European Commission, "Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: A European Strategy for Data," COM(2020) 66, February 19, 2020, https://ec.europa.eu/info/sites/info/files/communication-european-strategy-data-19feb2020_en.pdf; Eline Chivot, "Why the European Commission Should Revise its Data Governance Act," Center for Data Innovation, November 5, 2020, https://datainnovation.org/2020/11/why-the-european-commission-should-revise-its-data-governance-act; Eline Chivot, "EU Data Strategy Has Worthwhile Goal, but Misses the Mark," Center for Data Innovation, August 13, 2020, https://datainnovation.org/2020/08/eu-data-strategy-has-worthwhile-goal-but-misses-the-mark.
7. "Presidential Policy Directive – Signals Intelligence Activities," PPD-28, January 17, 2014, https://obamawhitehouse.archives.gov/the-press-office/2014/01/17/presidential-policy-directive-signals-intelligence-activities.
8. See suggestions in: Peter Swire, Testimony to U.S. Senate Commerce Committee Hearing on "The Invalidation of the EU-U.S. Privacy Shield and the Future of Transatlantic Data Flows," December 9,

2020, https://www.commerce.senate.gov/services/files/6E06A2A6-A9D9-4EFA-8390-0A288B7C1DCA.

9. U.S. Department of Commerce (2016). Measuring the Value of Cross-Border Data Flows. September 2016; OECD (2018a), "Trade and cross-border data flows," Preliminary Draft, TAD/TC, OECD Publishing, Paris; Nigel Cory, Robert D. Atkinson, and Daniel Castro, "Principles and Policies for "Data Free Flow With Trust"; Swedish National Board of Trade (2015), "No Transfer, No Production: A Report on Cross-border Data Transfers, Global Value Chains, and the Production of Goods," https://www.ospi.es/export/sites/ospi/documents/documentos/Measuring_the_Economic_Value_of_Data.pdf; https://www.oecd.org/trade/topics/digital-trade/.
10. See Economics and Statistics Administration and the National Telecommunications and Information Administration, "Measuring the Value of Cross-Border Data Flows," U.S. Department of Commerce, September 2016, https://www.ntia.doc.gov/files/ntia/publications/measuring_cross_border_data_flows.pdf; Nigel Cory, "Surveying the Damage: Why We Must Accurately Measure Cross-Border Data Flows and Digital Trade Barriers" (ITIF, January 2020), https://itif.org/sites/default/files/2020-surveying-the-damage.pdf.
11. As in: McKinsey Global Institute (2016a), "Digital Globalization: The New Era of Global Flows," McKinsey & Company, February 2016.
12. As the U.S. Department of Commerce states: "Streaming a video might be of relatively little monetary value but use several gigabytes of data, while a financial transaction could be worth millions of dollars but use little data." "Measuring the Value of Cross-Border Data Flows," op cit.
13. One study found that, when accounting for advertising revenues, Facebook alone generated a median consumer surplus of about $500 per person in both the United States and Europe. See Erik Brynjolfsson and Avinash Collis, "How Should We Measure the Digital Economy?" *Harvard Business Review*, November–December 2019, https://hbr.org/2019/11/how-should-we-measure-the-digital-economy.
14 OECD, "Measuring the Economic Value of Data and Cross-Border Data Flows: A Business Perspective," OECD Digital Economy Papers No. 297, August 2020, https://www.ospi.es/export/sites/ospi/documents/documentos/Measuring_the_Economic_Value_of_Data.pdf.
15. OECD and the U.S. Bureau of Economic Analysis (BEA) lead the way in developing new and better ways to measure the value of data and digital trade. See OECD, "Measuring the Economic Value of Data and Cross-Border Data Flows: A Business Perspective."
16. BEA constructed the estimates within a supply-use framework following the same methodology developed for the initial estimates published in the March 2018 report. For that report, BEA first developed a conceptual definition of the digital economy. BEA's information and communications technology (ICT) sector served as a starting point for the definition of the digital 5 economy. While not all ICT goods and services are fully in scope, the ICT sector and the digital economy largely overlap. The estimates presented in this report include BEA's ICT sector as well as additional goods and services determined to be in scope for the digital economy. To create digital economy estimates, BEA identified specific goods and services categories within BEA's supply-use framework relevant to measuring the digital economy. In previous estimates, only items considered to be primarily digital were included. The estimates presented in this report include items on a partial basis for the first time, meaning that only the in-scope portion of an item's value is included in the estimates. The partial inclusion of additional retail and wholesale e-commerce items expands the coverage of the BEA digital economy estimates. This latest set of estimates incorporates guidance on terminology and digital economy structure from OECD. See Jessica Nicholson, "New Digital Economy Estimates," Bureau of Economic Analysis, August 2020, https://www.bea.gov/system/files/2020-08/New-Digital-Economy-Estimates-August-2020.pdf.
17. Nicholson, "New Digital Economy Estimates."

18. "ICT Sector—Value Added, Employment and R&D," Eurostat, February 2020, https://ec.europa.eu/eurostat/statistics-explained/index.php?title=ICT_sector_-_value_added,_employment_and_R%26D#The_size_of_the_ICT_sector_as_measured_by_value_added; European Commission, "The 2018 PREDICT Key Facts Report," EU Science Hub, 2018, https://ec.europa.eu/jrc/en/predict/ict-sector-analysis-2018/2018-key-facts-report.
19. Nicholson, "New Digital Economy Estimates"; "ICT Sector—Value Added, Employment and R&D."
20. Daniel S. Hamilton and Joseph P. Quinlan, "The Transatlantic Economy 2020: Annual Survey of Jobs, Trade and Investment Between the United States and Europe," Foreign Policy Institute, Johns Hopkins University SAIS, 2020, https://www.uschamber.com/sites/default/files/te2020_report_final.pdf.
21. IMF/OECD, "How to move forward on measuring digital trade," Thirty-Second Meeting of the IMF Committee on Balance of Payments Statistics, Thimphu, Bhutan October 29–November 1, 2019, https://www.imf.org/external/pubs/ft/bop/2019/pdf/19-07.pdf.
22. Hamilton and Quinlan, "The Transatlantic Economy 2020."
23. Ibid.
24. Trade data is for 2018. Affiliate data is for 2017, the latest available year. Source: U.S. Bureau of Economic Analysis. Jessica R. Nicholson, "New BEA Estimates of International Trade in Digitally Enabled Services," Bureau of Economic Analysis, May 24, 2016, http://www.esa.doc.gov/economic-briefings/new-bea-estimates-international-trade-digitally-enabled-services.
25. Hamilton and Quinlan, "The Transatlantic Economy 2020."
26. Potential ally ICT-enabled services exports are those that "can predominantly be delivered remotely over ICT networks, a subset of which are actually delivered via that method." The Department of Commerce can precisely measure these ICT services, as they are defined as a group of service types rather than by the mode of delivery. BEA collects much of its data on international trade in services directly from businesses through surveys. While the data indicates the value and type of service provided, there is no information on whether the service was delivered digitally or in person. As BEA does not have a direct measure of services that are digitally traded within each service category, it is difficult to precisely estimate how much this percentage has increased over time. However, BEA is working with the EU and others to develop a better estimate as to mode of supply. BEA has some figures for 2019, but it omitted/suppressed the figure for U.S. imports from Europe for that year in order to avoid the disclosure of data of individual companies. See Bureau of Economic Analysis, "International Data: International Transactions, International Services, and International Investment Position Tables," apps.bea.gov, accessed March 4, 2021, https://apps.bea.gov/iTable/iTable.cfm?reqid=62&step=9&isuri=1&6210=4; Grimm, Alexis. "Trends in U.S. Trade in Information and Communications Technology (ICT) Services and ICT-Enabled Services," Bureau of Economic Analysis, https://apps.bea.gov/scb/pdf/2016/05%20May/0516_trends_%20in_us_trade_in_ict_serivces2.pdf; Jessica R. Nicholson, "Digital Trade in North America," U.S. Department of Commerce Economics and Statistic Administration, January 5, 2018, https://www.commerce.gov/sites/default/files/media/files/2018/digital-trade-in-north-america.pdf; Michael A. Mann, "Measuring Trade in Services by Mode of Supply," BEA Working Paper Series WP2019-7, U.S. Bureau of Economic Analysis, August 2019, https://www.bea.gov/system/files/papers/WP2019-7_2.pdf.
27. U.S. Bureau of Economic Analysis, U.S. Trade in Services – Table 3.3 U.S. Trade in ICT and Potentially-ICT Enabled Services, by Country or Affiliation, https://apps.bea.gov/iTable/iTable.cfm?reqid=62&step=9&isuri=1&6210=4.
28. Our analysis mostly follows Department of Commerce methodology and that of UNCTAD in defining seven categories in the International Monetary Fund balance of payments accounts as ICT-enabled: communications services; insurance; financial services; computer and information services; royalties and license fees; other business services; and personal, cultural, and recreational services. BEA uses

the term "digitally deliverable" rather than "digitally enabled" to describe these categories, as there is no data available that indicates whether these services were actually delivered digitally or by some other means. Hence, the term "digitally deliverable" is intended to convey that these services maybe delivered digitally. See Jessica R. Nicholson and Ryan Noonan, "Digital Economy and Cross-Border Trade: The Value of Digitally-Deliverable Services," U.S. Department of Commerce Economics and Statistics Administration, January 27, 2014, https://www.commerce.gov/sites/default/files/migrated/reports/digitaleconomyandcross-bordertrade.pdf.

29. This graph uses TiVA data, which comes from OECD. See "Trade in Value Added (TiVA): Principal Indicators," OECD.Stat, https://stats.oecd.org/Index.aspx?datasetcode=TIVA_2018_C1.
30. DDS bilateral trade data comes from Eurostat. See "International Trade in Services (Since 2010)," Eurostat, last updated March 3, 2021, https://appsso.eurostat.ec.europa.eu/nui/show.do?dataset=bop_its6_det&lang=en.
31. U.S. Bureau of Economic Analysis, U.S. Trade in Services – Table 3.1 U.S. Trade in ICT and Potentially-ICT Enabled Services, by Type of Service, https://apps.bea.gov/iTable/iTable.cfm?reqid=62&step=9&isuri=1&6210=4.
32. Ibid.
33. Ibid.
34. Ibid.
35. "Measuring the Value of Cross-Border Data Flows."
36. Shari A. Allen et al., "U.S. International Services: Trade in Services in 2019 and Services Supplied Through Affiliates in 2018," *Survey of Current Business,* October 2020, https://apps.bea.gov/scb/2020/10-october/1020-international-services.htm.
37. "Definition of International Services," U.S. Bureau of Economic Analysis, last modified October 21, 2020, https://www.bea.gov/international/international-services-definition.
38. BEA states that despite the difficulties in comparing statistics on U.S. trade in services with statistics on services supplied through affiliates, the large difference in value between the two indicates that the services supplies through affiliates is the larger channel of delivery of services in international markets. See "Definition of International Services."
39. "Seismic Shift: The Transatlantic Digital Economy," in Hamilton and Quinlan, *The Transatlantic Economy 2020*.
40. U.S. Bureau of Economic Analysis, International Transactions, International Services, and International Investment Position Tables (Table 4.1., "U.S. International Transactions in Primary Income," March 23, 2021, and Table 5.1., "U.S. International Transactions in Secondary Income," March 23, 2021; accessed April 1, 2021), https://apps.bea.gov/iTable/iTable.cfm?reqid=62&step=6&isuri=1&tablelist=56&product=1 and https://apps.bea.gov/iTable/iTable.cfm?reqid=62&step=6&isuri=1&tablelist=62&product=1.
41. See OECD, "Measuring the Economic Value of Data and Cross-Border Data Flows: A Business Perspective."
42. Stephen Ezell, "A Policymaker's Guide to Smart Manufacturing" (ITIF, November 30, 2016), https://itif.org/publications/2016/11/30/policymakers-guide-smart-manufacturing.
43. Sherry M. Stephenson, "The Linkage Between Services and Manufacturing in the U.S. Economy," Washington International Trade Association, May 23, 2017, https://www.wita.org/blogs/the-linkage-between-services-and-manufacturing-in-the-u-s-economy.
44. Matthew Karnitsching, "Why Europe's Largest Economy Resists New Industrial Revolution," Politico EU, July 6, 2016, http://www.politico.eu/article/why-europes-largest-economy-resists-new-industrial-revolution-factories-of-the-future-special-report.

45. Ezell, "A Policymaker's Guide to Smart Manufacturing."
46. Accenture Cloud, "Supply Chain Management in the Cloud: How Can Cloud-Based Computing Make Supply Chains More Competitive?" Accenture, 2014, https://www.accenture.com/t20150523T022449__w__/us-en/_acnmedia/Accenture/Conversion-Assets/DotCom/Documents/Global/PDF/Dualpub_1/Accenture-Supply-Chain-Management-in-the-Cloud.pdf.
47. Robert Hardt, "Is It Worth Our While to Invest in Manufacturing?" Siemens Canada, November 17, 2014, https://www.siemens.ca/web/portal/en/NewsEvents/Siemens-Canada-News/Pages/Isitworthourwhiletoinvestinmanufacturing.aspx.
48. Stephen Ezell and Bret Swanson, "How Cloud Computing Enables Modern Manufacturing," (ITIF, June 2017), http://www2.itif.org/2017-cloud-computing-enables-manufacturing.pdf.
49. European Automobile Manufacturers Association, "Transport Sector Calls for an EU Framework on the Governance of B2B Data," press release, October 7, 2020, https://www.acea.be/news/article/transport-sector-calls-for-an-eu-framework-on-the-governance-of-b2b-data; Afroz Mirzaie Shra, "A New Insight into Data Requirements Between Discrete Event Simulation and Industry 4.0: A Simulation-based Case Study in the Automotive Industry Supporting Operational Decisions," Master Thesis, 2018, https://www.diva-portal.org/smash/get/diva2:1289789/FULLTEXT01.pdf.
50. "Schrems II Impact Survey Report," DIGIALEUROPE, BusinessEurope, ERT, and ACEA, 2020, https://www.businesseurope.eu/sites/buseur/files/media/reports_and_studies/2020-11-26_schrems_ii_impact_survey_report.pdf.
51. Jeff Edwards, "IDC Survey: Majority of Manufacturers use Cloud," Enterprise Cloud Solutions Review, April 21, 2015, https://solutionsreview.com/cloud-platforms/idc-survey-majority-of-manufacturers-use-cloud; "Global Digital Trade 1: Market Opportunities and Key Foreign Trade Restrictions," U.S. International Trade Commission, August 2017, 192, https://www.usitc.gov/publications/332/pub4716.pdf.
52. Amber Markim, "8 Ways Cloud Technology is Changing the Game for Supply Chain Management," cerasis, July 23, 2015, https://cerasis.com/cloud-technology-in-supply-chain-management.
53. Ezell and Swanson, "How Cloud Computing Enables Modern Manufacturing."
54. Ibid.
55. Paul Tate, "Are Digital Tools the Future of Manufacturing Innovation?" Manufacturing Leadership (Frost & Sullivan), October 29, 2013, http://www.gilcommunity.com/blog/are-digital-tools-future-manufacturing-innovation.
56. "Cisco Annual Internet Report (2018-2023) White Paper," Cisco.com, March 9, 2020, https://www.cisco.com/c/en/us/solutions/collateral/executive-perspectives/annual-internet-report/white-paper-c11-741490.html; "Cisco Annual Internet Report – Cisco Annual Internet Report Highlights Tool," Cisco.com, accessed March 4, 2021, https://www.cisco.com/c/en/us/solutions/executive-perspectives/annual-internet-report/air-highlights.html.
57. Edy Liongosari et al., "Smart Production: Finding a Way Forward: How Manufacturers Can Make the Most of the Industrial Internet of Things," Accenture, 2015, 11, https://www.accenture.com/t20160119T041002__w__/us-en/_acnmedia/PDF-5/Accenture-804893-Smart-Production-POV-Final.pdf.
58. Michael Molitch-Hou, "GE Announces the Launch of Mass 3D Printing Facility," 3D Printing Industry, July 16, 2014, https://3dprintingindustry.com/news/ge-announces-launch-mass-3d-printing-facility-29909/.
59. Sandra Zistl, "3D Printing: Facts and Forecasts," Siemens, October 1, 2014, http://www.siemens.com/innovation/en/home/pictures-of-the-future/industry-and-automation/Additive-manufacturing-facts-and-forecasts.html.

60. John Brownlee, "What Under Armour's New 3D-Printed Shoe Reveals About the Future of Footwear," Co.Design, March 25, 2016, http://www.fastcodesign.com/3057983/what-under-armours-new-3D-printed-shoe-reveals-about-the-future-of-footwear; John Koten, "A Revolution in the Making," *The Wall Street Journal*, June 10, 2013, http://www.wsj.com/articles/SB10001424127887324063304578522812684722382.
61. John Koten, "A Revolution in the Making."
62. Sandra Zistl, "3D Printing: Facts and Forecasts."
63. Victoria Woollaston, "How Tech Is Revolutionising the Prosthetics Industry: 3D-Printed Limbs and Hands Controlled by Apps Becoming Mainstream," *Daily Mail*, April 8, 2014, http://www.dailymail.co.uk/sciencetech/article-2599863/How-tech-revolutionising-prosthetics-industry-3D-printed-limbs-hands-controlled-apps-mainstream.html#ixzz4KEnQTFnK; Jonathan Schwartz, "The Future of 3D-Printed Prosthetics," *TechCrunch*, June 26, 2016, https://techcrunch.com/2016/06/26/the-future-of-3d-printed-prosthetics/.
64. Ezell and Swanson, "How Cloud Computing Enables Modern Manufacturing."
65. Autodesk, "The Next Wave of Intelligent Design Automation," Harvard Business Review Analytic Services, 2018, https://damassets.autodesk.net/content/dam/autodesk/www/mech-eng-ressource-center/assets/The%20next%20wave%20of%20intelligent%20design%20automation%20-%20white%20paper.pdf.
66 . Robert Atkinson and Stephen Ezell, "The Manufacturing Evolution: How AI Will Transform Manufacturing & the Workforce of the Future" (MAPI Foundation, August 6, 2019), https://static1.squarespace.com/static/58862301f7e0ab813935c244/t/5d48788e7b132300013f15b0/1565030557296/MAPI-ITIF-AI-workforce-report-F.pdf.
67. Ezell and Swanson, "How Cloud Computing Enables Modern Manufacturing."
68. Hearing Before the House Ways and Means Trade Subcommittee on Expanding U.S. Digital Trade and Eliminating Barriers to U.S. Digital Exports, 114th Cong. (2016) (written testimony of Robert D. Atkinson, Founder and President ITIF), http://www2.itif.org/2016-expanding-us-digital-trade.pdf.
69. Kaeser reports that this "air-as-a-service" business model produced a 28.5 percent reduction in compressed air usage for a representative building supplies manufacturer and €30,000 in annual savings for a paint manufacturer. Hewlett Packard Enterprise, "A Heavy Equipment Provider Uses the Industrial IoT to Cut Customers' Downtime by 60%.".
70. James Manyika et al., "The Internet of Things: Mapping the Value Beyond the Hype" (McKinsey Global Institute, June 2015), 68, http://www.mckinsey.com/~/media/McKinsey/Business%20Functions/McKinsey%20Digital/Our%20Insights/The%20Internet%20of%20Things%20The%20value%20of%20digitizing%20the%20physical%20world/Unlocking_the_potential_of_the_Internet_of_Things_Executive_summary.ashx.
71. Ibid.
72. Mark Doms and Daniel Castro, "Data Is the Key to the Factory of the Future" (Washington, D.C: U.S. Department of Commerce, Economics and Statistics Administration, October 2, 2014), http://www.esa.doc.gov/under-secretary-blog/data-key-factory-future.
73. Kaeser Kompressoren uses IoT sensors to capture key environmental and performance data from the over 100,000 compressors actively in use. With equipment continuously transmitting its operational status in real time, Kaeser conducts predictive analytics to determine whether parts might be prone to failure, and so can identify and replace faulty parts during regularly scheduled maintenance instead of after an outage has occurred. Hewlett Packard Enterprise, "A Heavy Equipment Provider Uses the Industrial IoT to Cut Customers' Downtime by 60%," https://www.hpe.com/us/en/customer-case-studies/kaeser-iiot.html. Edy Liongosari et al., "Smart Production: Finding a Way Forward: How Manufacturers Can Make the Most of the Industrial Internet of Things," Accenture, 2015, 11,

https://www.accenture.com/t20160119T041002__w__/us-en/_acnmedia/PDF-5/Accenture-804893-Smart-Production-POV-Final.pdf.

74. https://www.ft.com/content/6f0f41e4-47de-11e8-8ee8-cae73aab7ccb
75. For example: https://www.acea.be/news/article/saving-lives-with-big-data-and-ai-requires-better-infrastructure
76. Alan Beattie, "Data Protectionism: The Growing Menace to Global Business," The Financial Times, May 14, 2018, https://www.ft.com/content/6f0f41e4-47de-11e8-8ee8-cae73aab7ccb.
77. For example: Eric-Mark Huitema, "Saving Lives with Big Data and AI Requires Better Infrastructure," ACEA, February 26, 2020, https://www.acea.be/news/article/saving-lives-with-big-data-and-ai-requires-better-infrastructure.
78. "ACEA Comments: EDP Guidelines 1/2020 on Processing Personal Data in the Context of Connected Vehicles and Mobility Related Applications," ACEA, April 2020, Microsoft Word - ACEA_comments_EDPB_guidelines_1-2020_CLEAN.
79. Ezell, "A Policymaker's Guide to Smart Manufacturing."
80. One benefit for Ford has been that downstream machines can detect if inputs they receive from an upstream machine deviate in even the minutest dimension from specifications, thereby indicating possible problems in upstream machines that can be immediately identified and fixedJames Manyika et al., "The Internet of Things: Mapping the Value Beyond the Hype," 68..
81. Michael E. Porter and James E. Heppelmann, "How Smart, Connected Products Are Transforming Companies," *Harvard Business Review*, October 2015, https://hbr.org/2015/10/how-smart-connected-products-are-transforming-companies.
82. Ibid.
83. Ibid.
84. Beattie, "Data Protectionism: The Growing Menace to Global Business."
85. Transatel, "Transatel and G+D Sign with Scania to Provide Trucks with Machine-to-Machine Connectivity Worldwide," press release, December 3, 2018, https://www.transatel.com/press-releases/transatel-and-gd-sign-with-scania-to-provide-trucks-with-machine-to-machine-connectivity-worldwide.
86. "No Transfer, No Trade: The Importance of Cross-Border Data Transfers for Companies Based in Sweden," National Board of Trade, 2014, https://unctad.org/system/files/non-official-document/dtl_ict4d2016c01_Kommerskollegium_en.pdf.
87. "Rio connectivity," Traton website, accessed December 15, 2021, https://traton.com/en/innovation/connected-driving/rio_connectivity.html.
88. "Rio without the Rio Box: Mixed Fleet Bridge Opens up the Rio Platform to Trucks without Hardware," Rio website, https://rio.cloud/en/press/rio-without-rio-box.
89. OECD, *The Next Production Revolution: Implications for Governments and Business,* (OECD Publishing: Paris, 2017), https://doi.org/10.1787/9789264271036-en.
90. Beattie, "Data Protectionism: The Growing Menace to Global Business."
91. Ibid.
92. "Connectivity," scania.com, accessed March 8, 2021, https://www.scania.com/group/en/home/about-scania/innovation/technology/connectivity.html.
93. "No Transfer, No Trade: The Importance of Cross-Border Data Transfers for Companies Based in Sweden."

94. Mark Brohan, "Volkwagen Builds Marketplace to Push Digital Manufacturing," Digital Commerce 360, July 28, 2020, https://www.digitalcommerce360.com/2020/07/28/volkswagen-builds-a-marketplace-to-push-digital-manufacturing.
95. "Volkwagen Develops the Largest Digital Ecosystem in the Automotive Industry," volkswagenag.com, August 2018, https://www.volkswagenag.com/en/news/stories/2018/08/volkswagen-develops-the-largest-digital-ecosystem-in-the-automot.html.
96. Ibid.
97. "Learning to Learn," volkswagenag.com, November 2018, https://www.volkswagenag.com/en/news/stories/2018/11/learning-to-learn.html.
98. "'Man Against Machine?' No, Because Together They're Unbeatable!" volkswagenag.com, May 2018, https://www.volkswagenag.com/en/news/stories/2018/05/artificial-intelligence-helps-employees.html.
99. "The Beginnings of a Quantum Leap," volkswagenag.com, March 20, 2017, https://www.volkswagenag.com/en/news/stories/2017/03/the-beginnings-of-a-quantum-leap.html.
100. "Intelligent Traffic Control with Quantum Computers," volkswagenag.com, November 218, https://www.volkswagenag.com/en/news/stories/2018/11/intelligent-traffic-control-with-quantum-computers.html.
101. Volkswagen, "Digital Transformation: Volkswagen Factories in the U.S. and Mexico to Link Up with the Industrial Cloud," press release, December 14, 2020, https://media.vw.com/en-us/releases/1446.
102. Initial app developers include ABB Group (a Swedish-Swiss firm), ASCon Systems GmbH, BearingPoint Europe Holdings BV (a Dutch firm), Celonis GmbH, Dürr AG, GROB-WERKE GmbH, NavVis, SYNAOS GmbH, Teradata Corp. (a U.S. firm), WAGO Kontakttechnik GmbH, and MHP. See Brohan, "Volkswagen Builds Marketplace to Push Digital Manufacturing."
103. "No Transfer, No Trade: The Importance of Cross-Border Data Transfers for Companies Based in Sweden."
104. Ibid.
105. Daimler AG, "Using New Opportunities Responsibly: Daimler AG Adopts Principles for Dealing with Artificial Intelligence," press release, September 9, 2019, https://media.daimler.com/marsMediaSite/en/instance/ko.xhtml?oid=44351958&relId=1001&resultInfoTypeId=175#toRelation.
106. Cory et al., "'Schrems II': What Invalidating the EU-U.S. Privacy Shield Means for Transatlantic Trade and Innovation."
107. "ACEA Position Paper: Artificial Intelligence in the Automobile Industry," ACEA, November 2020, https://www.acea.be/uploads/publications/ACEA_Position_Paper-Artificial_Intelligence_in_the_automotive_industry.pdf.
108 "Roadmap for EU-USA S&T Cooperation," European Commission, 2018, https://ec.europa.eu/research/iscp/pdf/policy/us_roadmap_2018.pdf.
109. James Fenelon and Gabriel Voisin, "EDPB Publishes Draft Guidelines on Connected Vehicles," Bird & Bird, February 2020, https://www.twobirds.com/en/news/articles/2020/global/eu-data-regulator-edpb-publishes-draft-guidelines-on-connected-vehicles.
110. Ibid.
111. ACEA, "Personal Data: Connected Vehicles not the Same as Smartphones, Says Auto Industry," press release, May 15, 2020, https://www.acea.be/press-releases/article/personal-data-connected-vehicles-not-the-same-as-smartphones-says-auto-indu; "ACEA Comments: EDP Guidelines 1/2020 on Processing Personal Data in the Context of Connected Vehicles and Mobility Related Applications."
112. "National Telecom M2M Roadmap," Ministry of Communications & Information Technology, May 2015, http://www.dot.gov.in/sites/default/files/u10/National%20Telecom%20M2M%20Roadmap.pdf;

Daniel Castro,"The False Promise of Data Nationalism," (ITIF, December 2013), http://www2.itif.org/2013-false-promise-data-nationalism.pdf.

113. Mark Schaub et al., "China: Mapping the Future – Current Challenges and Forecast Trends in Respect of Mapping for Autonomous Vehicles," King & Wood Mallesons, January 19, 2018, https://www.kwm.com/en/cn/knowledge/insights/china-mapping-the-future-20180119.
114. Xie Jun, "Tesla Shifting Chinese User Data Server Out of US," *Global Times*, June 23, 2020, https://www.globaltimes.cn/content/1192567.shtml.
115. Begüm Yavuzdogan Okumus, "Latest Development on Data Localization Requirements in Turkey," IAPP, February 7, 2020, https://iapp.org/news/a/latest-development-on-data-localization-requirements-in-turkey.
116. See the Tele2 case study here: https://unctad.org/system/files/non-official-document/dtl_ict4d2016c01_Kommerskollegium_en.pdf.
117. Dwayne Gefferie, "The Top 3 Trends that will impact the Payments Industry in 2018," The Startup page on Medium.com, January 2, 2018, https://medium.com/swlh/the-top-3-trends-that-will-impact-the-payments-industry-in-2018-3bed3588f98f.
118. Formerly known as the Committee on Payment and Settlement Systems. Cross-border retail payments. Basel: Bank for International Settlements, February 2018, https://www.bis.org/cpmi/publ/d173.pdf.
119. "No Transfer, No Trade: The Importance of Cross-Border Data Transfers for Companies Based in Sweden."
120. Kim S. Nash, "J.P. Morgan Set to Run First Apps in Public Cloud," *The Wall Street Journal*, March 30, 2017, https://blogs.wsj.com/cio/2017/03/30/j-p-morgan-set-to-run-first-apps-in-public-cloud.
121. "Top 10 Trends in Payments in 2018" (Industry paper by Capgemin), https://www.capgemini.com/wp-content/uploads/2017/12/payments-trends_2018.pdf.
122. Alan McQuinn, Weining Guo, and Daniel Castro, "Policy Principles for Fintech" (The (ITIF, October 18, 2016), https://itif.org/publications/2016/10/18/policy-principles-fintech.
123. "How Ping An, An Insurer, Became a Fintech Super-App," *The Economist*, December 3, 2020, https://www.economist.com/finance-and-economics/2020/12/03/how-ping-an-an-insurer-became-a-fintech-super-app.
124. Steven Norton, "Big Banks Starting to Embrace Public Cloud, Deutsche Bank Says," *The Wall Street Journal*, June 9, 2016, https://blogs.wsj.com/cio/2016/06/09/big-banks-starting-to-embrace-public-cloud-deutsche-bank-says/; Nash, "J.P. Morgan Set to Run First Apps in Public Cloud."
125. Testimony of Stephen Simchak before the U.S. International Trade Commission Hearing on "Global Digital Trade I: Market Opportunities and Key Foreign Trade Restrictions," U.S. International Trade Commissio, April 4, 2017, https://www.usitc.gov/press_room/documents/testimony/332_561_013.pdf.
126. Ibid.
127. The Geneva Association, "Harnessing Technology to Narrow the Insurance Protection Gap," December 2016, 7.
128. Based on a conversation with an industry representative.
129. Ibid.
130. Ibid.
131. Ibid. Also: Patrick S. Ryan, Sarah Falvey, and Ronak Merchant (2013), "When the cloud goes local: The global problem with data localization," IEEE Computer Society, Issue 12, Vol. 46, https://www.computer.org/csdl/mags/co/2013/12/mco2013120054-abs.html.
132. "Mastercard to Expand Euro Tech Hub in Dublin," PYMNTS, February 24, 2020, https://www.pymnts.com/mastercard/2020/mastercard-to-expand-euro-tech-hub-in-dublin.

133. Seth Eisen, "Mastercard Opens Global Intelligence and Cyber Centre in Vancouver," Mastercard Newsroom, January 23, 2020, https://mastercardcontentexchange.com/newsroom/press-releases/2020/january/mastercard-opens-global-intelligence-and-cyber-centre-in-vancouver.
134. The Lab works with its counterparts around the world to test and develop new ideas, such as a payment outlier detection tool (which uses AI and machine learning to monitor payment records and learn how to identify outlier and suspicious transactions that may crop up). See "Countries and Jurisdictions: Ireland," citigroup.com, accessed March 8, 2021, https://www.citigroup.com/citi/about/countries-and-jurisdictions/ireland.html; Jonathan Keane, "Separating the Fintech Wheat from the Chaff – Inside Citi's Dublin innovation Lab," FOR A, July 6, 2019, https://fora.ie/citi-innovation-lab-dublin-4711844-Jul2019.
135. A specific U.S. concern relates to OFAC (Office of Foreign Assets Control) and the demand on financial companies to do terrorist screening—a demand that is not compatible with Swedish regulation on data protection. The Swedish Data Protection Board had to issue an exemption allowing fulfillment of the OFAC demand for certain companies only (members of the Swedish Bankers Association) and for certain categories of data only. See "No Transfer, No Trade: The Importance of Cross-Border Data Transfers for Companies Based in Sweden."
136. Cory et al., "'Schrems II': What Invalidating the EU-U.S. Privacy Shield Means for Transatlantic Trade and Innovation."
137. For example: "Open Letter: Commit to Data Flows & Back it up with Action," Joint Letter by Allied for Startups and others, October 8, 2020, https://alliedforstartups.org/2020/10/08/open-letter-commit-to-data-flows-back-it-up-with-action.
138. "2020 SBEC/TechnoMetrica Small Business Cloud Services Survey," Small Business & Entrepreneurship Council and TechnoMetrica, June 2020, https://sbecouncil.org/wp-content/uploads/2020/06/2020SBECSmallBusinessCloudServicesSurvey-Report.pdf; "Survey Confirms the Need to Support Small and Medium-Sized Businesses on their Path Towards Digitalisation and Sustainability," European Commission, September 23, 2020, https://ec.europa.eu/growth/content/survey-confirms-need-support-small-and-medium-sized-businesses-their-path-towards_en.
139. George Collins and Sara Ma, "Digital Tools a Boon to Small Business," *The Wall Street Journal,* June 21, 2017, https://deloitte.wsj.com/cio/2017/06/21/digital-tools-a-boon-to-small-businesses/; "Small business technology trends: Digital and online tools connect businesses to customers," Deloitte, 2017, https://www2.deloitte.com/us/en/pages/technology-media-and-telecommunications/articles/connected-small-businesses.html; "Impact of Internet and digitalization on SMBs in India," KPMG and Google, January, 2017, https://assets.kpmg/content/dam/kpmg/in/pdf/2017/01/Impact-of-internet-and-digitisation.pdf.
140. Facebook, "State of Small Business Report," May, 2020, https://dataforgood.fb.com/wp-content/uploads/2020/05/SMBReport.pdf; In effect, the impact that restrictions on personal data have on these ecommerce marketplace services become just barriers (alongside existing logistical and customs barriers) to the growing number of small firms that use e-commerce platforms to engage in small package trade. Evdokia Moïsé, "Parcels trade: The good, the bad, and the ugly," OECD blog post, March 14, 2019, https://www.oecd.org/trade/parcels-trade-good-bad-ugly/.
141. "Open Letter: Commit to Data Flows & Back it up with Action," Joint Letter by Allied for Startups and others.
142. Alex Konrad, "Why Silicon Valley Investors Are Bonkers For European Startups," *Forbes,* December 2, 2019, https://www.forbes.com/sites/alexkonrad/2019/12/02/inside-silicon-valleys-european-startup-rush/?sh=5f620d4646f8; Alex Konrad, "Why VC Firm Sequoia Broke With Tradition To Put Down Roots In Europe's Startup Scene," *Forbes,* November 17, 2020, https://www.forbes.com/sites/alexkonrad/2020/11/17/vc-firm-sequoia-puts-down-roots-in-europe-startup-scene/?sh=6fde03155eac.

143. Start Up Genome, "State of the Global Startup Economy (2020)," https://startupgenome.com/article/state-of-the-global-startup-economy.
144. Kim Baroudy et al., "Europe's start-up ecosystem: Heating up, but still facing challenges," McKinsey and Company article, October 11, 2020, https://www.mckinsey.com/industries/technology-media-and-telecommunications/our-insights/europes-start-up-ecosystem-heating-up-but-still-facing-challenges; "State of the Global Startup Economy (2020)."
145. Ufuk Akcigit et al., "Fencing Off Silicon Valley: Cross-Border Venture Capital and Technology Spillovers," National Bureau of Economic Research, September, 2020, https://www.nber.org/system/files/working_papers/w27828/w27828.pdf.
146. A VC firm's home country increased patenting in the U.S. start-up's technology by 5.6 patents per year and increased citations by 14.7 percent (as compared with the prior year). Akcigit et al., "Fencing Off Silicon Valley: Cross-Border Venture Capital and Technology Spillovers."
147. Baroudy et al., "Europe's start-up ecosystem: Heating up, but still facing challenges."
148. European Commission, "Survey confirms the need to support small and medium-sized businesses on their path towards digitalisation and sustainability," September 23, 2020, https://ec.europa.eu/growth/content/survey-confirms-need-support-small-and-medium-sized-businesses-their-path-towards_en.
149. Baroudy et al., "Europe's start-up ecosystem: Heating up, but still facing challenges."
150. Oliver Patel, Duncan McCann, and Javier Ruiz, "The Cost of Data Inadequacy: The economic impacts of the UK failing to secure an EU data adequacy decision" (UCL European Institute report with the New Economics Foundation, November 23, 2020), https://www.ucl.ac.uk/european-institute/sites/european-institute/files/ucl_nef_data-inadequacy.pdf.
151. The low-cost, straightforward Privacy Shield framework was favored by small businesses, with SMEs comprising 65% of all certified firms in 2019. "Open Letter: Commit to Data Flows & Back it up with Action," Joint Letter by Allied for Startups and others, October 8, 2020, https://alliedforstartups.org/2020/10/08/open-letter-commit-to-data-flows-back-it-up-with-action.
152. Ibid.
153. One study predicts that U.K. companies requiring only a small number of SCCs would still incur at least £2,000 in legal fees if the United Kingdom does not receive an adequacy decision. Patel, McCann, and Ruiz, "The Cost of Data Inadequacy: The economic impacts of the UK failing to secure an EU data adequacy decision."
154. The estimated costs are based on the European Commission's own estimate of the cost of doing data protection impact assessments (DPIAs) as required by GDPR. The study estimates that a small-scale DPIA would cost €14,000, a medium-scale DPIA would cost €34,500, and a large-scale DPIA would cost €149,000. Setting up SCCs for data transfers could entail costs of a similar range. In order to account for the fact that an SCC will be less work than a DPIA, we assumed just 50% of the labour costs and retained the full IT costs. However, the European Commission data does not give an estimate for a DPIA done at the micro-firm level. To get a value for micro-firms, we took the midpoint in terms of employees for both micro and small, 5 and 25, respectively, and adjusted accordingly. This resulted in the micro average data flows mapping cost being 20% of the average small-firm mapping costs. Drawn from: European Commission, "Impact Assessment: Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) and Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data," January 25, 2012, https://www.europarl.europa.eu/cmsdata/59702/att_20130508ATT65856-1873079025799224642.pdf; Patel, McCann, and Ruiz, "The Cost of Data Inadequacy: The economic impacts of the UK failing to secure an EU data adequacy decision."

155. Patel, McCann, and Ruiz, "The Cost of Data Inadequacy: The economic impacts of the UK failing to secure an EU data adequacy decision."
156. Those that could afford to renegotiate contracts to bring their data transfers into compliance may still be hesitant to do so with SCCs themselves under scrutiny post-*Schrems II.* While the EDPB has offered some guidance, the process remains complex and uncertain. Caitlin Fennessy, "A breakdown of EDPB's recommendations for data transfers post-'Schrems II'," IAPP blog post, November 11, 2020, https://iapp.org/news/a/a-break-down-of-edpbs-recommendations-for-data-transfers-post-schrems-ii/.
157. "Open Letter: Commit to Data Flows & Back it up with Action," Joint Letter by Allied for Startups and others.
158. Allied for Startups and Truth, "The Impact of Regulation on the Tech Sector Informing a regulatory environment which leads to a stronger tech ecosystem in Europe," December, 2018, http://coadec.com/wp-content/uploads/2018/12/The-Impact-of-Regulation-on-the-Tech-Sector.pdf.
159. Atomico, "Presenting the 2019 State of European Tech report," https://www.atomico.com/presenting-the-2019-state-of-european-tech-report/; Atomico, "2019: State of European tech," https://2019.stateofeuropeantech.com/chapter/policy/article/techs-take-policy/.
160. "*Schrems II*: Impact Survey Report," Business Europe, DIGITALEUROPE, the European Round Table for Industry, and European Automobile Manufacturers Association, https://www.digitaleurope.org/wp/wp-content/uploads/2020/11/DIGITALEUROPE_Schrems-II-Impact-Survey_November-2020.pdf.
161. Cory et al., "'Schrems II': What Invalidating the EU-U.S. Privacy Shield Means for Transatlantic Trade and Innovation."
162. OECD, "Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value," OECD Digital Economy Papers, No. 220, OECD Publishing, Paris, 2013, https://doi.org/10.1787/5k486qtxldmq-en.
163. Ibid.
164. Similarly, privacy concerns have been raised about Facebook and Google, with fictional claims of the companies selling its users' data because of misunderstandings about the mechanisms of targeted advertising. Most targeted advertising works by matching ads to users based on the information in their profile. The simple fact is that many consumers choose ad-supported content, applications, and services because they prefer it to the alternatives. But while the online ad-supported business model may not be a perfect funding mechanism, many online content, applications, and services simply would not exist without it. Robert Atkinson, "Google E-mail, What's All the Fuss About?" (Washington, D.C.: Progressive Policy Institute, 2004), www.ppionline.org/ppi_ci.cfm?knlgAreaID=140&subsecID=288&contentID=252511.
165. Jessica Davies, "After GDPR, The New York Times cut off ad exchanges in Europe — and kept growing ad revenue," *Digiday,* January 16, 2019, https://digiday.com/media/gumgumtest-new-york-times-gdpr-cut-off-ad-exchanges-europe-ad-revenue/.
166. See "Cloud Connect > Google Apps," https://www.google.com/support/enterprise/static/gsa/docs/admin/70/admin_console_help/cloud_google_apps.html.
167. For example, a survey of 1,000 U.S. adults by Epsilon and GBH Insights found that the vast majority of respondents (80 percent) want personalization from retailers. "New Epsilon research indicates 80% of consumers are more likely to make a purchase when brands offer personalized experiences," press release, January 9, 2018, https://us.epsilon.com/pressroom/new-epsilon-research-indicates-80-of-consumers-are-more-likely-to-make-a-purchase-when-brands-offer-personalized-experiences; Erik Lindecrantz, Madeleine Tjon Pian Gi, and Stefano Zerbi, "Personalizing the customer experience:

Driving differentiation in retail," McKinsey and Company article, April 28, 2020, https://www.mckinsey.com/industries/retail/our-insights/personalizing-the-customer-experience-driving-differentiation-in-retail; Julien Boudet et al., "Consumer-data privacy and personalization at scale: How leading retailers and consumer brands can strategize for both," McKinsey and Company article, November 7, 2019, https://www.mckinsey.com/business-functions/marketing-and-sales/our-insights/consumer-data-privacy-and-personalization-at-scale.

168. Melody Dye et al., "Supporting content decision makers with machine learning," Netflix blog post, December 10, 2020, https://netflixtechblog.com/supporting-content-decision-makers-with-machine-learning-995b7b76006f?source=social.tw; "How Netflix's Recommendations System Works," https://help.netflix.com/en/node/100639.
169. "Facebook tells Irish court that probe threatens its EU operations," *Reuters,* September 20, 2020, https://www.reuters.com/article/us-facebook-privacy-idUSKCN26B0CV.
170. Facebook and the Asia Business and Trade Association, "Enabling Small and Medium Enterprises in the Digital Age," https://static1.squarespace.com/static/59cb8dbe37c581113d249e01/t/5cac589dee6eb07d57414221/1554798756159/Enabling+SMEs+in+the+Digital+Age+%28SME+Summit+June+2018+-+ABTA%29.pdf.
171. Eurostat (December 2019): Social media use by type, internet advertising.
172. United States International Trade Commission (USITC), *Digital Trade in the U.S. and Global Economies, Part 1* (USITC, July, 2013), https://www.usitc.gov/publications/332/pub4415.pdf.
173. 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/.
174. 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.
175. "Data Excellence: Transforming manufacturing and supply systems," The World Economic Forum, January, 2021, http://www3.weforum.org/docs/WEF_Data_Excellence_Transforming_manufacturing_2021.pdf.
176. Colin Mitchell et al., "The GDPR and genomic data: The impact of the GDPR and DPA 2018 on genomic healthcare and research," PHG Fondation report, May, 2020, https://www.phgfoundation.org/documents/gdpr-and-genomic-data-report.pdf.
177. Charles Friedman, Adam Wong, and David Blumenthal, "Achieving a nationwide learning health system," *Sci. Translat. Med.* 2, 2010, https://pubmed.ncbi.nlm.nih.gov/21068440/; William Price II, "Drug approval in a learning health system," *Minn. L. Rev*, Research Paper No. 598, https://papers.ssrn.com/abstract_id=3152570.
178. Casey Ross, "Covid-19 is pushing pharma to the cloud — and convincing the industry of its value," *Stat+,* October 22, 2020, https://www.statnews.com/2020/10/22/pharma-cloud-aws-google-ucb/.
179. Connie Lin, "3 top executives discuss how tech transformed business during COVID-19," *Fast Company,* October 22, 2020, https://www.fastcompany.com/90566853/facebook-pfizer-and-genpact-executives-discuss-how-tech-has-changed-during-covid-19.
180. Heather Landi, Providence St. Joseph Health, "Microsoft form strategic alliance to leverage cloud, AI technology," *Fierce Healthcare,* July 8, 2019, https://www.fiercehealthcare.com/tech/providence-st-joseph-health-microsoft-form-strategic-alliance-to-leverage-cloud-ai-technology; Isaac Jahns, "'For the benefit of all': Mayo partners with Amazon, Microsoft and others in the fight against COVID-19*," MedCityBeat,* 2020, https://www.medcitybeat.com/news-blog/2020/for-the-benefit-of-all-mayo-partners-with-amazon-microsoft-and-others-in-fight-against-covid-19; Robert Wachter and Christine Cassel, "Sharing Health Data with Digital Giants: Overcoming Obstacles and Reaping Benefits While

Protecting Patients," *JAMA,* 323, 507–508 (2020), https://jamanetwork.com/journals/jama/article-abstract/2759415.

181. Anthony A. Philippakis et al., "The Matchmaker Exchange: A Platform for Rare Disease Gene Discovery," *Human Mutation,* Volume36, Issue 10, October 2015, 915–921, https://onlinelibrary.wiley.com/doi/full/10.1002/humu.22858.
182. Ewan Birney, Jessica Vamathevan, and Peter Goodhand, "Genomics in healthcare: GA4GH looks to 2022," BioRxiv, 2017; 4, https://www.biorxiv.org/content/10.1101/203554v1.
183. Dara Hallinan et al., "International Transfers of Health Research Data Following Schrems II: A Problem in Need of a Solution" (September 7, 2020), https://ssrn.com/abstract=3688392.
184. Birney et al., "Genomics in healthcare: GA4GH looks to 2022."
185. "Matchmaker Exchange Statistics and Publications," https://www.matchmakerexchange.org/statistics.html.
186. Birney et al., Genomics in healthcare: GA4GH looks to 2022"; Philippakis et al., "The Matchmaker Exchange: A Platform for Rare Disease Gene Discovery."
187. BC Cancer, University of British Columbia, University of Washington eScience Institute and the Knight Cancer Institute at Oregon Health & Science University, https://www.fredhutch.org/en/about/about-the-hutch/institutional-partners-collaborations/cascadia-data-alliance.html.
188. John Kahan, "New Cascadia Data Discovery Initiative accelerates health innovation," Microsoft blog post, July 12, 2019, https://blogs.microsoft.com/on-the-issues/2019/07/12/new-cascadia-data-discovery-initiative-accelerates-health-innovation/.
189. Birney et al., "Genomics in healthcare: GA4GH looks to 2022"; Fruzsina Molnár-Gábor et al., "Computing patient data in the cloud: Practical and legal considerations for genetics and genomics research in Europe and internationally," *Genome Medicine*, 2017; 9(1): 1–12, https://genomemedicine.biomedcentral.com/articles/10.1186/s13073-017-0449-6.
190. Ross, "Covid-19 is pushing pharma to the cloud — and convincing the industry of its value."
191. Takeda, "Takeda Accelerates Digital Transformation with Accenture and AWS," press release, October 13, 2020, https://www.takeda.com/newsroom/newsreleases/2020/takeda-accelerates-digital-transformation-with-accenture-and-aws/.
192. Lisa George, "How Can Artificial Intelligence Facilitate New Drug Research and Development?" *Pharmiweb*, November 2020, https://www.pharmiweb.com/article/how-can-artificial-intelligence-facilitate-new-drug-research-and-development?mc_cid=3b15b156a7&mc_eid=1901100594.
193. Doug Henschen, "Merck Optimizes Manufacturing With Big Data Analytics," *InformationWeek*, April 2, 2014, http://www.informationweek.com/strategic-cio/executive-insights-and-innovation/merck-optimizes-manufacturing-with-big-data-analytics/d/d-id/1127901.
194. Ross, "Covid-19 is pushing pharma to the cloud — and convincing the industry of its value."
195. Fruzsina Molnár-Gábor and Jan Korbel, "Genomic data sharing in Europe is Stumbling — Could a code of conduct prevent its fall?" *EMBO Molecular Medicine*, 2020; 12, 1–7, https://doi.org/10.15252/emmm.201911421.
196. Kassa Ayalew, "Presentation: FDA Perspective on International Clinical Trials," https://www.fda.gov/media/91849/download.
197. Molnár-Gábor and Korbel, "Genomic data sharing in Europe is Stumbling — Could a code of conduct prevent its fall?"; Colin Mitchell et al., "The GDPR and genomic data: The impact of the GDPR and DPA 2018 on genomic healthcare and research," PHG Fondation report, May, 2020, https://www.phgfoundation.org/documents/gdpr-and-genomic-data-report.pdf.
198. This is a "snapshot," as it doesn't include U.S. government, individual, or other funders, studies currently or not yet recruiting, or completed studies. "U.S. Food and Drug Administration clinical trials

database," https://clinicaltrials.gov/ct2/results?cond=&term=&cntry=&state=&city=&dist=&recrs=d&fund=2.

199. Ibid.
200. Tania Rabesandratana, "European data law is impeding studies on diabetes and Alzheimer's, researchers warn," *Science,* November 20, 2019, https://www.sciencemag.org/news/2019/11/european-data-law-impeding-studies-diabetes-and-alzheimer-s-researchers-warn.
201. "International Genomics of Alzheimer's Project (IGAP)," https://consortiapedia.fastercures.org/consortia/igap/
202. Rabesandratana, "European data law is impeding studies on diabetes and Alzheimer's, researchers warn."
203. U.S. Food and Drug Administration, "Guidance for Industry and FDA Staff: FDA Acceptance of Foreign Clinical Studies Not Conducted Under an IND: Frequently Asked Questions," March 2012, https://www.fda.gov/media/83209/download.
204. For example, on secondary research, which refers to research conducted using data or biospecimens collected either (i) for research studies other than the proposed research or (ii) for nonresearch purposes, such as clinical care. Secondary research is important to biobanks and databanks, which hold biospecimens and accompanying phenotypic and demographic data for distribution to other researchers for secondary research purposes. David Peloquin et al., "Disruptive and avoidable: GDPR challenges to secondary research uses of data," *European Journal of Human Genetics*, 28, 697–705 (2020), https://www.nature.com/articles/s41431-020-0596-x.
205. Ibid.
206. Article 4(26), GDPR.
207. Mitchell et al., "The GDPR and genomic data: The impact of the GDPR and DPA 2018 on genomic healthcare and research."
208. European Data Protection Board. Guidelines 2/2020 on articles 46(2)(a) and 46(3)(b) of Regulation 2016/679 for transfers of personal data between EEA and non-EEA public authorities and bodies. 2020, 47; "Disruptive and avoidable: GDPR challenges to secondary research uses of data."
210. Dara Hallinan et al., "International Transfers of Health Research Data Following Schrems II: A Problem in Need of a Solution."
211. "Guidelines 03/2020 on the processing of data concerning health for the purpose of scientific research in the context of the COVID-19 outbreak," European Data Protection Board, April 21, 2020, https://edpb.europa.eu/our-work-tools/our-documents/ohjeet/guidelines-032020-processing-data-concerning-health-purpose_en; The EDPB's subsequent restrictive (and technically infeasible advice) about the use of SCCs after *Schrems II* also reflects how its narrow, legalistic, and restrictive focus will have a deleterious impact on modern trade and innovation. See Cory et al., "The Role and Value of Standard Contractual Clauses in EU-U.S. Digital Trade."
212. By industry. 293 by 4671 (Kevin's industry tab).
213. Cory et al., "'Schrems II': What Invalidating the EU-U.S. Privacy Shield Means for Transatlantic Trade and Innovation."
214. Oliver Patel, Duncan McCann, and Javier Ruiz, "The Cost of Data Inadequacy: The economic impacts of the UK failing to secure an EU data adequacy decision" (UCL European Institute report with the New Economics Foundation, November 23, 2020), https://www.ucl.ac.uk/european-institute/sites/european-institute/files/ucl_nef_data-inadequacy.pdf.
215. "French Highest Court Rejects Temporary Suspension of France's Health Data Hub; Calls for Additional Guarantees Following Schrems II," National Law Review website, October 19, 2020,

https://www.natlawreview.com/article/french-highest-court-rejects-temporary-suspension-france-s-health-data-hub-calls.

216. "Health Data Hub: An Ambitious French Initiative for Tomorrow's Health," Opus Line post, March 25, 2019, https://www.opusline.fr/en/health-data-hub-an-ambitious-french-initiative-for-tomorrows-health/.
217. "French Highest Court Rejects Temporary Suspension of France's Health Data Hub; Calls for Additional Guarantees Following Schrems II."
218. "Joint Press Statement from European Commissioner for Justice Didier Reynders and U.S. Secretary of Commerce Wilbur Ross," August 10, 2020, https://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=684836.
219. Peter Swire, "U.S. Senate Commerce Committee Hearing on The Invalidation of the EU-U.S. Privacy Shield and the Future of Transatlantic Data Flows," December 9, 2020, https://www.commerce.senate.gov/services/files/6E06A2A6-A9D9-4EFA-8390-0A288B7C1DCA.
220. Cory et al., "Principles and Policies for 'Data Free Flow with Trust'"; Alan McQuinn and Daniel Castro, "How Law Enforcement Should Access Data Across Borders" ((ITIF, July 24, 2017), https://itif.org/publications/2017/07/24/itif-calls-united-states-lead-developing-new-approach-international-law.
221. For example, EU data privacy law also allows for exceptions, or derogations, on a case-by-case basis (e.g., explicit consent), but they are highly specific and are not intended to support regular and ongoing transfers of data for data exporters.
222. Cory et al., "The Role and Value of Standard Contractual Clauses in EU-U.S. Digital Trade."
223. European Commission, "Exchanging and Protecting Personal Data in a Globalised World," January 10, 2017, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52017DC0007&from=EN.
224. Ibid.
225. Ibid.
226. "Codes of conduct and certification," https://www.imy.se/other-lang/in-english/the-general-data-protection-regulation-gdpr/codes-of-conduct-and-certification/.
227. "Guidelines 1/2019 on Codes of Conduct and Monitoring Bodies under Regulation 2016/679," European Data Protection Board, February 19, 2019, https://edpb.europa.eu/our-work-tools/public-consultations/2019/guidelines-12019-codes-conduct-and-monitoring-bodies-under_en; "EDPB Document on the procedure for the development of informal Codes of Conduct sessions," European Data Protection Board, November 10, 2020, https://edpb.europa.eu/our-work-tools/our-documents/procedure/edpb-document-procedure-development-informal-codes-conduct_en.
228. "Complementing the EU Cloud CoC to become a safeguard pursuant Art. 46 GDPR," EU Cloud Code of Conduct website, https://eucoc.cloud/en/about/third-country-transfer-initiative/.
229. "A Code of Conduct for Health Research," https://code-of-conduct-for-health-research.eu/; ""GDPR Code of Conduct" for clinical trials: clarifications from the European Federation of CROs," tic pharma post, November 27, 2019, https://www.eucrof.eu/news-eucrof/latest-news/27-11-gdpr-code-of-conduct-for-clinical-trials-in-progress; Dr Michelle Goddard, "Towards a GDPR Code of Conduct for the Research Sector," November 8, 2018, https://www.research-live.com/article/opinion/towards-a-gdpr-code-of-conduct-for-the-research-sector/id/5045562.
230. Fruzsina Molnár-Gábor and Jan O Korbel, "Genomic data sharing in Europe is stumbling-Could a code of conduct prevent its fall?" *EMBO molecular medicine* vol. 12,3 (2020): e11421. doi:10.15252/emmm.201911421.
231. "EU-US cooperation in Justice and Home Affairs – an overview," European Parliament briefing, April, 2016,

https://www.europarl.europa.eu/RegData/etudes/BRIE/2016/580892/EPRS_BRI(2016)580892_EN.pdf.

232. Thankfully, adequacy decisions do not cover data exchanges involved in the EU's cooperation with counterparts on law enforcement. They are governed by the "Police Directive" (article 36 of Directive (EU) 2016/680). See "Answer given by Mr. Reynders on behalf of the European Commission," European Parliament website, December 8, 2020, https://www.europarl.europa.eu/doceo/document/E-9-2020-004472-ASW_EN.pdf.
233. "Frequently Asked Questions: New EU rules to obtain electronic evidence," European Commission website, https://ec.europa.eu/commission/presscorner/detail/el/MEMO_18_3345.
234. European Commission, "Criminal justice: Joint statement on the launch of EU-U.S. negotiations to facilitate access to electronic evidence," press release, September 26, 2019, https://ec.europa.eu/commission/presscorner/detail/en/STATEMENT_19_5890.
235. "Better access to e-evidence to fight crime," European Council website, https://www.consilium.europa.eu/en/policies/e-evidence/.
236. Peter Swire, "EU and U.S. Negotiations on Cross-Border Data, Within and Outside of the Cloud Act Framework," Cross-Border Data Forum post, April 13, 2019, https://www.crossborderdataforum.org/eu-and-u-s-negotiations-on-cross-border-data-within-and-outside-of-the-cloud-act-framework/.
237. European Commission, "EU-US: A new transatlantic agenda for global change," press release, December 2, 2020, https://ec.europa.eu/commission/presscorner/detail/en/ip_20_2279; Mark Scott and Laurens Cerulus, "EU-US 'tech alliance' faces major obstacles on tax, digital rules," *Politico,* December 2, 2020, https://www.politico.eu/article/eu-to-us-president-elect-joe-biden-lets-be-tech-allies/.
238. "Roadmap for EU - USA S&T cooperation," European Commission, October, 2018, https://ec.europa.eu/research/iscp/pdf/policy/us_roadmap_2018.pdf.
239. Robert Atkinson, "A U.S. Grand Strategy for the Global Digital Economy" (ITIF, January 19, 2021), https://itif.org/publications/2021/01/19/us-grand-strategy-global-digital-economy.
240. European Commission, "Commission proposes measures to boost data sharing and support European data spaces," press release, November 25, 2020, https://ec.europa.eu/commission/presscorner/detail/en/ip_20_2102; Eline Chivot, "Why the European Commission Should Revise its Data Governance Act," Center for Data Innovation blog, November 5, 2020, https://datainnovation.org/2020/11/why-the-european-commission-should-revise-its-data-governance-act/.
241. Joshua New, "AI Needs Better Data, Not Just More Data," Center for Data Innovation blog, March 20, 2019, https://www.datainnovation.org/2019/03/ai-needs-better-data-not-just-more-data/.
242. Nick Wallace and Daniel Castro, "The Impact of the EU's New Data Protection Regulation on AI" (ITIF, March 26, 2018), https://itif.org/publications/2018/03/26/impact-eu-new-data-protection-regulation-ai; Joshua New and Daniel Castro, "How Policymakers Can Foster Algorithmic Accountability" (ITIF, May 21, 2018), https://itif.org/publications/2018/05/21/how-policymakers-can-foster-algorithmic-accountability.
243. For a detailed analysis (applied in the context of the United Kingdom and United States, but it applies just the same with the EU) See Nigel Cory, "Written Submission Regarding UK-US Trade" (ITIF, September 25, 2020), https://itif.org/publications/2020/09/25/comments-uk-parliaments-subcommittee-international-agreement-regarding-us.
244. For example, in 1982, regulatory agencies and laboratories from G8 countries (now the G7) and the EU came together as part of the Versailles Project on Advanced Materials and Standards (VAMAS) to develop standardized terminology, reference materials, and testing and measurement protocols for new materials (physical, chemical, electronics etc.). "MOU between the Versailles Project on Advanced Materials and Standards (VAMAS) and the International Organization for Standardization (ISO),"

https://www.nims.go.jp/vamas/refarences/lndldd000000045h-att/MOU_VAMAS_ISO.pdf; "Versailles Project on Advanced Materials and Standards (VAMAS)," http://www.vamas.org/; Other examples of pre-standardization work involve researchers from Germany, Japan, and the United States working together on electrokinetic measurements and quantification of coarse particle content (e.g., those uses in advanced materials, thermal coatings, and drug carriers). "Ceramics Division: Materials Science and Engineering Laboratory: FY 2002 Programs and Accomplishments," U.S. National Institute of Standards and Technology, https://nvlpubs.nist.gov/nistpubs/Legacy/IR/nistir6904.pdf; Another example involves standards-related collaboration between the U.S. National Institute of Standards and Technology's (NIST) and the European Commission's Joint Research Center (ECJRC) for the development of reference materials for nanotechnology and health-related measurement standards. "JRC and NIST explore further common areas of work in certified reference materials for nanotechnology and health-related measurement standards," European Commission website, March 27, 2014, https://ec.europa.eu/jrc/en/science-update/jrc-and-nist-explore-further-common-areas-work-certified-reference-materials-nanotechnology-and.

245. Nigel Cory and Robert Atkinson, "Why and How to Mount a Strong, Trilateral Response to China's Innovation Mercantilism" (ITIF, January 13, 2020), https://itif.org/publications/2020/01/13/why-and-how-mount-strong-trilateral-response-chinas-innovation-mercantilism.
246. Stephen J. Ezell and Robert D. Atkinson, "The Middle Kingdom Galapagos Island Syndrome: The Cul-De-Sac of Chinese Technology Standards" (ITIF, December 2014), https://itif.org/publications/2014/12/15/middle-kingdom-galapagos-island-syndrome-cul-de-sac-chinese-technology.
247. Cory and Atkinson, "Why and How to Mount a Strong, Trilateral Response to China's Innovation Mercantilism."