ITIF | INFORMATION TECHNOLOGY & INNOVATION FOUNDATION

The Role and Value of Standard Contractual Clauses in EU-U.S. Digital Trade

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

SCCs are a widely used legal tool to transfer personal data out of the EU, but courts and regulators are making them costlier and more complex. This is a sign of Europe's march toward de facto data localization—a threat to transatlantic digital trade that policymakers must avoid.

KEY TAKEAWAYS

- Standard contractual clauses (SCCs), often called "model contracts," are pre-approved legal provisions for transferring personal data from the EU to the rest of the world in compliance with the EU's General Data Protection Regulation.
- SCCs are among the most widely used legal mechanisms for transferring personal data out of the EU. Firms from a broad range of sectors and countries rely on SCCs—not just consumer-facing companies from the United States.
- Europe's high court hasn't invalidated SCCs, but in *Schrems II* it noted the need for "supplementary measures." Now the EU is considering measures that would make SCCs costlier and overly restrictive for transfers to the United States.
- The Irish Data Protection Commission's initial reaction to *Schrems II*—ordering Facebook to stop using SCCs to transfer data to the United States—shows how transatlantic digital trade may be further undermined after Privacy Shield's demise.
- SCCs now face growing scrutiny and potential reforms that could mean U.S. firms will no longer be able to provide services to EU consumers, and EU businesses will be unable to pursue opportunities that may require data transfers to America.
- By making data transfers so complicated, costly, and uncertain, the EU risks creating the world's largest de facto data localization requirement—and SMEs and start-ups will shoulder a disproportionate share of the burden.

INTRODUCTION

Standard Contractual Clauses (SCCs) are a critical, but increasingly threatened, legal tool that many firms use to manage the transatlantic transfers of personal data that drive trade and innovation in the United States and the European Union (EU). SCCs have become even more important since the European Court of Justice (ECJ) invalidated another key tool to transfer data—the EU-U.S. Privacy Shield—which was used by over 5,000 mainly small and medium-sized enterprises (SMEs).[1] Without the EU-U.S. Privacy Shield, SCCs are now the only scalable and widely accessible legal tool available to organizations transferring data from the EU to the United States and most of the rest of the world.[2] Yet, the role and value of SCCs are barely recognized and poorly understood by most policymakers. This creates a risk that EU and U.S. policymakers will be distracted by the legalistic nature of the debate around SCCs and data transfers, missing the bigger picture, and thus failing to marshal the response that creates a clear, coherent, and predictable framework for firms to use to transfer the data that is central to modern trade.

The ability of firms to manage global data governance compliance is critical to maximizing the benefits of data and digital technologies in today's digital economy. Yet, firms face an increasingly difficult challenge in complying with multiple, and often differing, data governance regimes around the world. The greater the number of countries in which firms operate, and the greater their legal divergences, the greater the challenge. And as many countries move forward to enact new data protection regulations, this complexity will only grow in the years to come. The EU-U.S. Privacy Shield and SCCs had helped ease some of that complexity, but now that relief has disappeared.

Just as firms need clear, predictable, and reasonable documentation and procedures for cargo containers carrying the goods that define 19th century trade, so too do firms need a clear, accessible, and predictable legal framework to allow the seamless movement of personal data for 21st century EU-U.S. digital trade. SCCs are among the most popular transfer mechanism for data flows from European countries.[3]

Because so many organizations rely on SCCs to maintain compliance in their data transfers, they form the foundation of a significant portion of transatlantic trade, especially in digital services. For example, a recent 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, DIGITALEUROPE, the European Round Table for Industry, and European Automobile Manufacturers Association found that near 85 percent used SCCs, and only 9 percent did not transfer data outside the EU.[4] Firms handling personal data must have the ability to transfer that data between countries—even if the laws for processing that data differ between them. Interoperability between different data protection regimes is a crucial element of international trade in both digital and non-digital goods and services, be it retail, biopharmaceuticals, manufacturing, automotive, financial, insurance, payments, agriculture, or some other sector.[5] Not all data is personal data, but both personal and non-personal data are often intermingled as part of e-commerce transactions; HR and payroll records; travel bookings; health and medical records (e.g., clinical trials); vehicles and machinery operations and repairs (e.g., tractors, jet engines, trucks, cars, and even parts of factories); and any number of Internet services used by individuals and firms alike on a daily basis.

The schism in data governance rules between the EU, United States, and other countries is not new, but has grown since the implementation of the EU's General Data Protection Regulation (GDPR). Data transfers outside the European Economic Area (EEA), which are EU member states plus Iceland, Liechtenstein, and Norway, are subject to stringent compliance requirements to ensure data receives essentially the same privacy protections in the importing country as it does within the EU. The EU has aggressively pressured other countries to essentially adopt GDPR by generally prohibiting data transfers to any country that it has not deemed as having "adequate" data protection. It's questionable whether this data blockade is tenable given the challenge of forcing so many different sovereign countries to make major changes to their domestic laws—many of which take a different approach to data protection, and where there are reasonable disagreements about what should be included. Indicative of this, only 12 countries—of which, the United States is not one—have been recognized as having this adequate level of protection; all other transfers must use additional legal mechanisms to ensure compliance with EU data laws.[6]

The threat of broad de facto data localization—by making data transfers to other countries so costly and complicated that firms have no other viable option but to store and process data locally—looms on the European horizon.

At inception, GDPR envisaged a broader range of legal tools for firms to use to manage cross-border transfers of personal data. However, more than two years after coming into force, the situation is the reverse: It has failed to develop new transfer tools (such as codes of conduct and certifications), it has remained focused on slow and ad hoc adequacy determinations (the EU has only added Japan in the last few years), and existing legal tools have been challenged and removed one-by-one.[7] Most recently, in *Data Protection Commissioner v Facebook Ireland Limited, Maximillian Schrems* (*Schrems II*), the ECJ upheld SCCs as a valid transfer mechanism, but noted that additional "supplementary measures" may be necessary to ensure adequate protections, depending on the laws and regulations of the importing country (this decision is analyzed in detail ahead).[8] The implications of this case affect much more than just Facebook. The outcome of Facebook's court case, and the broader consideration of SCCs by the European Data Protection Board (EDPB), will greatly affect transatlantic digital trade.

Fundamental changes to the use of SCCs and their central role in EU-U.S. trade are fast approaching. The threat of broad de facto data localization—by making data transfers to other countries so costly and complicated that firms have no other viable option but to store and process data locally—looms on the European horizon as Ireland's Data Protection Commission (DPC) has made a preliminary ruling (which is on hold pending a hearing at Ireland's High Court) ordering Facebook to suspend transfers of European users' data to the United States.

This policy brief provides an overview of SCCs in the transatlantic digital economy, and analyzes the ECJ's decision on SCCs in *Schrems II* and of the Irish DPC's preliminary order against Facebook's use of SCCs. It then analyzes the impact of how these changes and the uncertainty raise the cost and complexity of transatlantic data transfers, protection, and analytics—and how this disproportionately affects SMEs, and makes U.S. firms significantly less competitive than their European peers. It analyzes one of the other remaining transfer mechanisms—binding corporate rules—and shows how they are not a substitute for SCCs, especially for SMEs. It

analyzes how the EDPB's proposal to use encryption for any number of regular data transfers and services is overly broad, misguided, and burdensome. Finally, it analyzes the economic impact if Europe fully embraces de facto data localization, before outlining why EU policymakers need to work with their own member states and the United States to build a clear, predictable, and accessible framework for firms to manage commercial data privacy concerns, while governments build a new mechanism to account for national security and surveillance concerns.

WHAT ARE STANDARD CONTRACTUAL CLAUSES, WHY ARE THEY NECESSARY, AND WHO USES THEM?

A transfer of personal data outside the protection of the GDPR is considered a "restricted transfer." For example, if a German firm passes information about its employees to its subsidiary or a cloud-based human resources service in the United States, this would be a restricted transfer. GDPR allows these transfers under certain circumstances, such as when the European Commission has determined an importing country's data protection laws and regulations are comparable to those in the EU (known as adequacy), and when a data exporter has put sufficient safeguards in place before transferring data to a country with insufficient legal protections. Transfers to the vast majority of countries, including the United States, fall into the latter category.[9]

SCCs (sometimes also called "model contracts") are a set of legal provisions pre-approved by the European Commission. Data exporters and importers must include these provisions in their contracts if they wish to engage in cross-border data transfers. The Commission has three sets of SCCs: two covering transfers of data from data controllers in the EU to data controllers established outside the EU (such as exchanging data within a group of companies), and one covering data transfers from an EU controller to a non-EU or EEA processor (such as exporting data to a third-party vendor).[10] The original 2001 controller-to-controller SCCs were supplemented in 2004 by an alternative set of clauses. In 2010, the Commission established the controller-to-processor SCC to address issues raised by the ever-increasing globalization, outsourcing, and subcontracting involving personal data.[11]

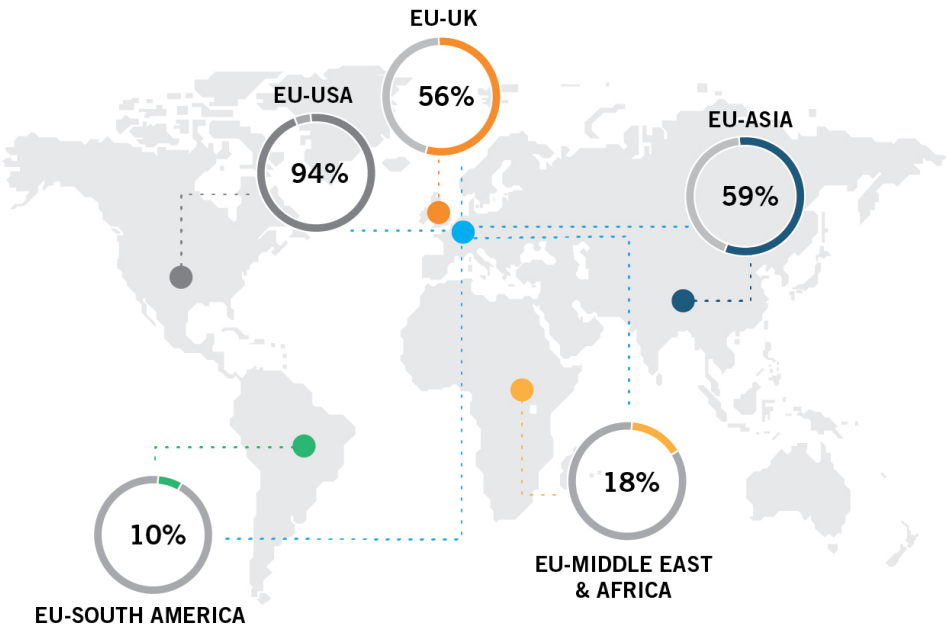
SCCs are useful in many scenarios. For example, a German firm could use a controller-to-processor SCC when it wants to contract with an American payroll company to process its payroll. Or a French travel agency might use a controller-to-controller SCC to send data about a booking to an American hotel.[12] One of the key purposes of the SCCs is to establish rights for the individuals whose personal data firms transfer, and allow these individuals to directly enforce those rights against data importers and data exporters. While firms must include SCCs in their entirety (they cannot alter them), contracting parties can include addendums to further specify the parameters for data transfers. For example, the United Kingdom's Information Commissioner's Office provides both SCC templates and SCC-plus contract builders.[13]

The limitation of SCCs is that they do not restrain mandatory government access to personal data. This limitation at the heart of Max Schrem's legal complaints. The inability of SCCs to prevent lawful requests for data by foreign governments is why the ECJ, the Commission, and the EDPB have put a growing responsibility on data exporters to ensure adequate protection through additional safeguards (whether technical, contractual, or organizational). But ultimately, policymakers should recognize that there are limits to what commercial actors can reasonably do in response to lawful government requests, especially those involving national security.

SCCs are one of the most widely used mechanisms by U.S., EU, and other firms—from a broad range of sectors, not just consumer-facing ones—to transfer personal data from the EU to the rest of the world.

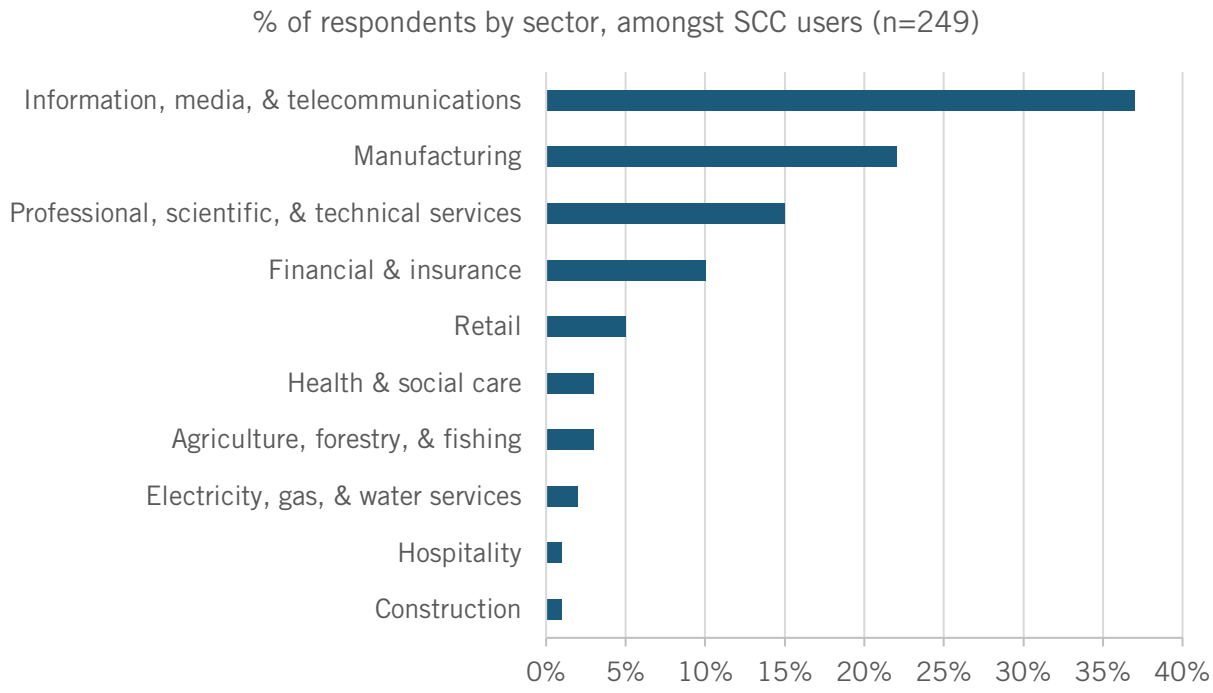
SCCs are one of the most widely used mechanisms by U.S., EU, and other firms—from a broad range of sectors, not just consumer-facing ones—to transfer personal data from the EU to the rest of the world. The International Association of Privacy Professionals (IAPP)-EY Annual Governance Report for 2019 surveyed 370 privacy professionals (from both the EU and United States), showing that 88 percent reported using SCCs in 2019.[14] Similarly, the recent joint survey by Business Europe, DIGITALEUROPE, the European Round Table for Industry, and European Automobile Manufacturers Association found that nearly 85 percent of the 292 respondents used SCCs.[15] Furthermore, while nearly all firms used SCCs to transfer data to the United States, 60 percent also used them to transfer data to Asia or the United Kingdom (figure 1).[16]

Figure 1: DIGITALEUROPE Survey: SCCs are used to transfer data globally (percent of respondents (172) that use SCCs and are aware of which geography they transfer data from the EEA).[17]



The survey also found that SCCs were used by firms of all sizes, including nearly two-thirds of SMEs. SCCs were also used by firms across sectors and mainly for business-to-business purposes—not just by a small group of consumer-facing services that policymakers tend to associate with personal data (figure 2). While firms in the information communication technology sector were the largest user (37 percent), manufacturing firms were the second largest users of SCCs (22 percent). Furthermore, most companies (90 percent) used SCCs for business-to-business sales and service—demonstrating that they're not simply tools for Internet-based consumer services.

Figure 2: DIGITALEUROPE Survey: Nearly all industries rely on SCCs to transfer personal data (percent of respondents, amongst SCC users (249)).[18]



WHAT DOES THE IRISH DATA PROTECTION COMMISSION'S PRELIMINARY ORDER FOR FACEBOOK MEAN FOR SCCS?

SCCs face growing scrutiny and potentially major reforms. Depending on the outcome of Facebook's court case in Ireland and final advice from the EDPB, SCCs may become much more onerous and restrictive in the future—or worse yet, rendered unusable for firms wanting to transfer EU personal data to the United States.

Facebook relied on SCCs to transfer data to countries outside the region, including to the United States.[19] While data protection authorities in EU member states cannot make adequacy determinations (only the Commission can), they can determine whether individual data transfers to countries without an adequacy decision comply with GDPR. In late August 2020, Ireland's DPC sent a preliminary order to Facebook calling for the suspension of all transfers of EU user data to the United States (which has its EU headquarters in Dublin).[20] It is the first significant step EU data protection authorities have taken to enforce the ECJ's *Schrems II* ruling, which the Irish DPC believes "firmly [endorsed] the substance of the concerns … that EU citizens do not enjoy the level of protection demanded by EU law when their data is transferred to the United States," even with the use of SCCs.[21] This follows the ECJ ruling stating that while the use of SCCs to transfer data globally is, in principle, valid, it is clear that in practice, the use of SCCs to transfer personal data to the United States is questionable and depends on the use of supplementary transfer tools to ensure compliance with EU data protection laws.[22]

Facebook's case in Ireland holds potentially broad implication for transatlantic digital trade. Initially, Ireland's high court granted Facebook a temporary halt to the DPC's preliminary suspension order for Facebook to stop transfers of EU personal data to the United States.[23] On

December 15, 2020, the Irish high court is scheduled to hear Facebook's challenge to the Irish DPC's order.[24] If Facebook's challenge is unsuccessful, the Irish DPC will then send the preliminary draft decision to the EDPB for discussion under article 60 of GDPR.[25] The EDPB may approve or amend the order, after which Ireland's DPC will enforce it with regards to Facebook. More importantly, depending on whether the order gets to the EDPB and what it ultimately decides, the order will create a template that other DPAs could use with firms that also rely on SCCs. This means the impact could be EU-wide and affect how all firms use SCCs for international data transfers. In this scenario, SCC-based transfers of EU personal data will be amended—or possibly turned off—on a firm-by-firm basis.

It's more a question of how SCCs will change rather than if they will change, and whether firms will still be able to use SCCs to transfer and process EU personal data in the United States in ways that are broadly similar to those they use now. Facebook has stated that it is not clear how the company could continue providing services in the EU if the Irish order were enforced.[26] If all SCCs are brought into question, the same will likely be true for the other firms that rely on them: U.S. firms will no longer be able to provide their services to European consumers, and European businesses will be unable to pursue opportunities that may require data transfers to the United States.

WHAT DOES THE *SCHREMS II* DECISION MEAN FOR SCCS?

The ECJ, Commission, and the EDPB all have a major role in shaping the future of SCCs and their role in transatlantic trade. While the ECJ decision in *Schrems II* upheld SCCs as a valid transfer mechanism, it added new compliance requirements and exposed individual SCC-based transfer agreements to further legal challenges. Together, these represent a major shift in how both companies and data protection authorities approach SCCs for international transfers of EU personal data.

The ECJ outlined that firms would need to be more careful in managing data transfers and use supplementary measures for SCC for them to remain a valid data transfer mechanism, but didn't specify exactly what these are. The ECJ observed that, in some cases, the laws of an importing country may directly conflict with EU data protection standards. When this is the case, SCCs are insufficient to provide adequate levels of protection for data transferred to that country. Accordingly, it is the responsibility of the "controller or processor to verify, on a case-by-case basis … whether the law of the third country of destination ensures adequate protection, under EU law, of personal data transferred pursuant to standard data protection clauses."[27] By noting this assessment requirement for SCCs, the ECJ indicated that these should serve as a baseline for securing cross-border data transfers. If compliance with the laws of the receiving country requires the data importer to forego adequate protections regardless of the safeguards in place, then "the controller or processor … [is] required to suspend or end the transfer of personal data to the third country concerned."[28]

In *Schrems II*, the ECJ did not elaborate what would constitute "supplementary measures." In the decision, the Court noted:

> *In so far as those standard data protection clauses cannot … provide guarantees beyond a contractual obligation to ensure compliance with the level of protection required under*

> *EU law, they may require … the adoption of supplementary measures by the controller in order to ensure compliance with that level of protection.*[29]

Following *Schrems II*, on November 11, the EDPB published its recommendations on supplementary transfer tools for firms to use to ensure compliance with GDPR, alongside a second document on EU essential guarantees regarding surveillance measures.[30] The EDPB's recommendations are an attempt to offer a step-by-step roadmap for the companies using SCCs. Regarding surveillance, the EDPB summarizes the essential guarantees as follows: Processing should be based on clear, precise, and accessible rules; necessity and proportionality with regard to the legitimate objectives pursued need to be demonstrated; an independent oversight mechanism should exist; and effective remedies need to be available to the individual. Together, these two documents outline—sometimes explicitly, but in many cases with a lack of specificity—an assessment process for the sufficiency of foreign protections under EU law when personal data is sent abroad and a set of EU-approved safeguards companies can implement even when foreign protections are judged lacking compared with EU legal standards.

The EDPB's supplementary measures include a six-step plan. Steps one and two are map transfers and pick a GDPR-compliant transfer mechanism (SCCs, ad hoc contractual clauses, adequacy, binding corporate rules, consent, or another GDPR Article 49 derogation).

Step three is a critical and broad step: Firms should assess the sufficiency of non-EEA protections and whether there's anything that may impinge on the effectiveness of safeguards.[31] The EDPB's essential guarantees document outlines what firms need to take into account as part of this step, such as whether an independent oversight mechanism exists and effective remedies are available to individuals.[32] The EDPA applies the same high-risk, worst-case perspective to all firms no matter their size, sector, or role in managing data, stating that firms shouldn't rely "on subjective factors such as the likelihood of public authorities' access to your data in a manner not in line with EU standards."[33] In other words, legal requirements and authorities should be given greater weight in assessments than the practical likelihood that a firm's data will be of interest to and accessed by authorities.[34] The EDPB offers a brief list of general sources of information—of varying quality and credibility—for firms to refer to in assessing foreign countries' legal frameworks, such as ECJ decisions, adequacy decisions, resolutions and reports from intergovernmental organization (such as the United Nations Human Rights body), national case law, and reports from academics and civil society.

Step four is for firms to identify and adopt supplementary measures where the assessment has deemed this necessary to bring the level of protection up to the EU's standard of essential equivalence.[35] The EDPB provides a non-exhaustive list of such measures, including technical, contractual, and organizational measures.

In each category, the EDPB outlines appropriate additional safeguards, as well as scenarios in which none might be available, suggesting data transfers should be stopped. For technical measures, the EDPB focuses on encryption, outlining a six-part analysis of an effective encryption protocol, including a forced encryption key storage mandate in the EEA.[36] It also includes pseudonymization and split- or multiparty processing. Particularly concerning is the EDPB has (initially at least) found no effective technical safeguards for use cases six and seven, which involve data processing in the clear by cloud service providers (i.e., unencrypted

processing) or remote access and use of data in the clear from a third country for business purposes, such as human resource processing.

For contractual safeguards, the EDPB makes clear that given the SCCs don't bind government authorities, contractual remedies must be part of a broader package of supplementary measures. Contractual safeguards include transparency, notification, and legal reaction requirements or actions around government requests for data. Other examples include enhanced audits to verify whether data has been provided to government authorities; commitments to notify the data exporter if the importer can no longer comply with its commitments due to changes in law or practice; or a "warrant canary," meaning continual notification that a government access request has not been received, until and unless it has.

Several large U.S. tech companies already provide transparency reports about government access to data that the EDPB calls for as part of transparency obligations.[37] But it's hardly widespread. These reports detail the number of requests for data from governments around the world and the companies' responses (to the extent legally allowed). The EDPB pairs this approach with a call for transparency regarding the laws governing government access to data in the recipient jurisdiction and potentially certification that the importer has not created "back doors" enabling direct government access to its data. While the former may be possible for firms, the latter is simply not something the private sector can address.

For organizational measures, the EDPB again highlights how internal policies, staff training, and other organization measures regarding data transfers and protection must be part of a broader package of supplementary measures to provide essentially equivalent protections, which in each case will depend on the case-by-case assessment in the context of the specific transfers. This could include the appointment of EU-based teams to assess and respond to government access requests, procedural steps to challenge unlawful or disproportionate requests, as well as transparency to the data subject.

Finally, after organizations have conducted these extensive assessments and put in place additional safeguards (where that is realistically possible), the EDPB calls on them to document their approach and seek authorization, where required by the chosen transfer mechanism (step five) and to reassess their approach on a regular basis (step six).

But Wait, There Are More Changes Coming: The Commission's Revisions to SCCs

Firms have been waiting a long time for the Commission to provide updated SCCs given GDPR's implementation—it has been over 10 years since the last major revisions and nearly 20 years since SCCs were initially introduced. Many firms (especially data controllers) have already added extra contractual requirements to their SCCs to account for likely GDPR-related requirements. The Commission is currently in the process of updating SCC templates to reflect changes to data protection laws under GDPR, perhaps by the end of this year. It may also create additional SCCs, such as to address processor-to-processor data transfers. Understandably, the Commission chose not to finalize the SCC revisions given the likely impact of *Schrems II*. While the Commission is generally expected to include considerations of the *Schrems II* decision in these updated measures, it is unlikely that the new SCCs will fully address the wide-reaching discrepancies and outstanding concerns from this decision.[38]

The Commission's revised SCCs will have a major impact, as they'll most likely include the repeal of the decisions adopting current SCCs. It's unknown how firms will have to implement changes in that if the revisions are limited to a few additional clauses, firms may be able to add them to an annex to supplement existing SCCs, thus reducing the compliance burden—although they would still need to execute new contracts with all data controllers and data processors. But if the changes are significant and throughout the text of SCCs, firms may need to replace entire SCCs. It's also unclear what the timeline for implementation will be and whether there'll be a grace period. For example, in 2010, firms were given a three-month grace period to replace old SCCs with new SCCs when the Commission replaced the SCCs for processors.[39] Organizations relying on SCCs as their primary data transfer mechanism may receive additional guidance from the Commission and the EDPB, but the heightened compliance requirements the *Schrems II* decision imposed will likely remain for some time.

RAISING THE COST AND COMPLEXITY OF DATA TRANSFERS AND ANALYSIS: EUROPE FURTHER TILTS THE BALANCE TOWARD LOCALIZATION.

Firms—both large and small, from across all sectors of the transatlantic trade relationship—face considerably higher costs and uncertainty in transferring EU personal data internationally after Privacy Shield was invalidated. A large and growing number of firms want to use SCCs, which are now significantly harder and more onerous to use, while also facing an uncertain future. No doubt, many policymakers in the EU, the Commission, and the EDPB have learned lessons from GDPR in recognizing its economic and trade impact and the need to provide more timely and detailed guidance for firms trying to comply with new data protection rules (such as those for SCCs). But it's still far short of what's necessary, especially given the lack of a transition period and the impact it'll have on SMEs. However, as much as it is necessary, this focus on the legal technicalities can cause policymakers in Europe to miss the bigger picture—by making data transfers so difficult and costly—that the EU is well down the path to closing itself off from the global digital economy. This section analyzes an alternative to SCCs and the potential impact on SCCs of recent ECJ decisions and Commission guidance.

Growing and Ongoing Compliance Costs Will Impact All Foreign Firms

With Privacy Shield invalidated, many firms will use SCCs as their primary mechanism to transfer EU personal data to the United States. A survey by Fieldfisher (a European law firm with an office in Silicon Valley) conducted shortly after the *Schrems II* decision indicates that the majority of data controllers do not intend to reduce use of non-EU based service providers, and the majority plan to shift to SCCs. Understandably, many firms are uncertain and awaiting further guidance.[40] SCCs were already a key bridge for EU-U.S. digital trade, but after the ECJ blew up Privacy Shield, it has become one of the few remaining pathways left, and this bridge desperately needs repairs.[41] The legal uncertainties and heightened compliance costs of SCCs post-*Schrems II* have left the many organizations that rely on them—and indeed, the future of most international data transfers of EU personal data—in a precarious and uncertain position.

All contracts between organizations that use U.S-based data services will need to be amended. Nearly all respondents of the IAPP-EY Annual Governance Report for 2019 (90 percent) stated their firms rely on third parties for data processing, and the top method for ensuring vendors have appropriate data protection safeguards is "relying on assurances in the contract" (named by 94 percent of respondents).[42] Firms will revise their SCCs to update the basis for data transfers

from Privacy Shield to SCCs. The compliance burden will spread through the broader digital ecosystem. Firms will ask their IT service providers for third-party assessments of their security, evidence of their commitment to data protection (such as via certifications and international standards), additional measures (such as more extensive use of encryption), checks on their data retention and destruction policies, and help setting up audit trails for data. To provide additional assurances, many firms will pursue or seek vendors with outside certifications (such as a SOC2, Type II certification), and undergo annual penetration tests to assure best-in-class administrative and technical safeguards.[43]

The legal and compliance cost will vary by firm, but in many cases it will be significant. Especially during COVID, firms may struggle to find the additional resources to adjust. For small businesses and start-ups, this challenge is particularly acute. A November 2020 report by the UCL European Institute and New Economics Foundation "The Cost of Data Inadequacy: The Economic Impacts of the U.K. Failing to Secure an EU Adequacy Decision" provides relevant data points for U.S.-EU data flows. It estimates that the average compliance costs of shifting to SCCs would be nearly $4,000 for micro businesses, $13,300 for small businesses, nearly $26,000 for medium-sized businesses, and $216,000 for large businesses.[44] This estimate is based on the European Commission's own cost estimates for firms doing the data protection impact assessments (DPIAs) required by GDPR. However, given SCCs will be less work than DPIAs, the UCL European Institute and New Economics Foundation's estimate assumes they would only involve half the labor costs, but the same IT costs. Interviews with lawyers and experts provided advice that supported these estimates. As the study stresses, these costs vary, and for many, the costs of drafting the actual SCC are negligible, and the bulk of time and costs come from preparing the information and negotiating and drafting the contracts. How resource-intensive this process will vary by firm and sector. It will be more expensive for organizations in sectors that deal with a lot of sensitive personal data. For example, the study outlines how a medical research organization at a university might need to spend $66,000 to $132,000 to negotiate a data-sharing agreement with a US-based organization receiving data and tissue samples.[45]

Firms—both large and small, from across all sectors of the transatlantic trade relationship—face considerably higher costs and uncertainty in transferring EU personal data internationally after Privacy Shield was invalidated. A large and growing number of firms want to use SCCs, which are now significantly harder and more onerous to use, while also facing an uncertain future.

Similar to the impact of GDPR's implementation, the cost of already limited third-party legal advisory services will no doubt increase, which will affect SMEs the most as they are the most likely to not have in-house legal expertise. It'll no doubt be a boon for privacy lawyers. Never mind that even where firms decide to try to hire people with these skills, there remains a significant shortage of trained staff. The IAPP-EY 2019 survey shows that spending on privacy technology was significantly higher among U.S. respondents than those from the EU.[46] The IAPP-EY annual governance report for 2017 (the year leading up to GDPR) finds that firms expected to hire two full-time employees just to help with GDPR compliance and spend a mean of roughly $5 million in adapting products and services as part of GDPR compliance. The mean budget for IAPP respondents was $21 million.[47] Firms will inevitably see growth in spending and hiring of privacy experts following *Schrems II*, which advantages large firms over SMEs and start-ups. The

irony for the many large firms that already have extensive privacy protections and staff in place is the review and adjustment will result in few substantive changes to actual data protection practices.

Potential government access to data underpins EU concerns about international data transfers, and governments on both sides have interpreted and reacted to the ECJ ruling in very different ways. In September 2020, the U.S. Commerce Department, Justice Department, and the Office of the Director of National Intelligence provided their own guidance to help firms understand U.S. privacy protections in what it described (or hopes) will be a concrete, detailed, and good faith effort to conceptualize a possible path forward for restoring legal certainty around transatlantic data flows.[48] They essentially stated that the majority of companies could satisfy European privacy laws by simply flagging that they've never received requests from government agencies for their records.[49]

The EDPB's supplementary guidance was welcomed, but insufficient in outlining exactly what firms should do. However, it is a separate question as to whether its guidance is technically and commercially feasible for firms that rely on the Internet and centralized global IT systems. Ultimately, it could change the calculus for firms as they decide whether it is worthwhile to remain engaged in trade with the EU. However, the EDPB's advice could be interpreted mostly as guidelines, while the Commission's proposals on SCCs will end up becoming the law of the land. But those draft rules could change as comments come back. So considerable uncertainty remains.

Many firms, especially SMEs, will understandably dislike the fact that they are expected to become experts in third-country surveillance and other data-related laws.

To use SCCs, organizations will have to prove to EU privacy regulators that their customer data is not subject to U.S. surveillance laws, which based on current guidance, will prove to be an uphill battle. Existing SCCs require the data importer to inform the data exporter of material changes to third-country laws when they have a substantial effect on the guarantees provided by the SCCs. This requirement will become stronger, clearer, and ongoing. Many firms, especially SMEs, will understandably dislike the fact that they are expected to become experts in third-country surveillance and other data-related laws.

Many firms are working on so-called "transfer impact assessments," which they hope to use as part of revised SCCs.[50] This type of assessment is hardly straightforward as there is no single, updated database of global data surveillance and privacy laws—and considerable differences in interpretation of how different countries enforce these laws. Conducting such an assessment is tough for even the largest and most sophisticated firms. Firms will likely have to go through a costly and complicated process to develop their own approach—and these costs will not be one-off, as firms will need to regularly seek legal expertise in the future to do case-by-case assessments for data transfers and to maintain awareness of changing legal situations in third countries (never mind the EU).

For firms with complex structures, such as multinational firms, the shift to SCCs will mean they may need hundreds of contracts to cover transfers between all affiliates. The ability of firms to revise or adapt SCCs also varies by DPA, some of which in the past have provided different

advice as to whether firms could use SCCs for multiparty (as opposed to bilateral) arrangements, which limits the scope for companies to reduce the number of contracts required. This highlights how SCCs may not be fit for use in a complex web of processing activities.

Looming large over this rush and confusion over compliance is the fact that the EU has declined to afford any sort of enforcement grace period for the thousands of firms involved in Privacy Shield and SCCs. In contrast, within 10 days of the ECJ's *Schrems I* decision in 2015, the EU issued guidance announcing a pause in coordinated enforcement actions during EU-U.S. Privacy Shield negotiations.[51] This formal grace period is even more important now as firms face an increasingly fragmented EU regulatory framework, and growing litigation as different DPAs jump to different conclusions and initiate their own legal challenges. Indicative of this, in its response to the ECJ decision, Hamburg's DPA criticized the judges for not also striking down SCCs, saying it was "inconsistent" for them to invalidate Privacy Shield yet allow this other mechanism for international transfers.[52]

The net impact is that foreign companies will be at a significant disadvantage compared to their European peers.

On top of growing compliance costs, firms that manage a lot of EU personal data will likely have to develop extensive and expensive litigation strategies for the scenario that once the rules are settled (or even before they are settled), they could face legal challenges from activist DPAs and individuals. For example, Max Schrems' NGO "none of your business" (noyb) filed 101 identical complaints with multiple data protection authorities against major companies in 30 EU/EEA member states.[53] The cost and complexity of this type of reaction is only possible for the very largest and most sophisticated firms—it is inconceivable that the vast majority of firms could afford this type of contingence planning.

The net impact is that foreign companies will be at a significant disadvantage compared to their European peers. First, many European firms may simply choose not to do business with U.S. firms to minimize their potential liability. Second, many European firms may choose to do business with U.S. firms to avoid the associated legal complexity and uncertainty of using SCCs, especially given the possibility that the EU may restrict their use in the future. Finally, many European firms will simply be able to offer more competitive pricing than their U.S. peers because they will not be subject to all of these compliance costs. Thus, the overall impact of the EU's privacy rules is to tilt the playing field against U.S. firms.

Binding Corporate Rules: Far From a Perfect, Accessible, and Reliable Alternative

Firms are evaluating alternative transfer mechanisms, but there are few options. EU data privacy law allows for exceptions, or derogations, on a case-by-case basis (such as explicit consent), but they are highly specific and not intended to support regular and ongoing transfers of data for data exporters. One option for firms is shifting data transfer activities to countries with adequacy decisions, which is only a small and disparate group of 12 countries (mainly former colonies).[54] The only other main alternative is binding corporate rules (BCRs), which some (large) firms already use to transfer EU personal data overseas, but BCRs are only for intra-firm data transfers.

BCRs affect data transfers throughout a firm. They grew out of the need for a more streamlined, efficient process for managing intra-firm transfers to avoid needing hundreds of SCCs to

otherwise cover internal transfers of EU personal data. They apply to restricted transfers of personal data from the group's EEA entities to non-EEA group entities.[55] BCRs demonstrate that a firm has put in place adequate safeguards for protecting personal data throughout the organization. If they're drafted widely enough, BCRs provide a degree of flexibility not found in adequacy mechanisms and SCCs, as the competent supervisory authority does not need to approve non-material updates (such as to organizational structure and types of data flows) to BCRs.[56]

But they are far from accessible for the vast majority of firms because they tend to take a long time to get approved, would still need to be used alongside SCCs, and may face their own legal challenges. The resources, expertise, and time to get BCRs approved mean they're mainly used by large companies, such as Cisco, American Express, Citigroup, Equinix, Mastercard, and General Electric.[57] Firms must submit BCRs for approval to their lead DPA authority (usually in their EEA head office country), which may involve several DPAs, as the firm may have entities in more than one EU member state.[58] Indicative of this, the joint Business Europe, DIGITALEUROPE, the European Round Table for Industry, and European Automobile Manufacturers Association survey shows that only 5 percent of firms use BCRs (or adequacy decisions
or derogations).[59]

The BCR approval process tends to take around two years, is far from predictable, and varies by local laws and DPA staffing. Some DPAs lack the resources to deal with BCR applications, which contributes to the long processing times. Firms also report that the process and outcome depend in no small part on the political context around U.S. tech firms at the time of the review. These factors no doubt contributed to the fact that the U.K.'s Information Commissioner's Office (as of November 2017) had approved about 25 percent of all BCR's in Europe.[60]

If successful, at the end of the process, the main DPA supervisory authority sends its draft decision to the EDPB (which issues a non-binding opinion on whether it approves the BCR or not, along with any suggested changes). BCRs also require regular audits and that a training program for staff handling personal data be maintained. If a firm makes major changes to its organizational structure or the data flows that go beyond the scope of the BCR authorization, it has to reapply for authorization.

Looming over all this is whether BCRs are next in line to attract legal challenges and scrutiny. The ECJ has not directly referenced BCRs; however, BCRs still raise similar concerns about firms' ability to secure data against foreign government surveillance.[61]

It's Not Just About Data: Overly Broad Encryption Requirements Can Affect Business Operations

Encryption should play a central role in the EU's domestic and international data protection policy. But if encryption is essentially required for any and all international data transfers and analytics, it acts as an unnecessary and burdensome barrier to both business operations (by inhibiting the use of non-EU-based data analytic services) and regulatory compliance (in potentially preventing firms from providing data to government authorities as part of legitimate, non-surveillance-related regulatory oversight, such as to the U.S. Federal Drug Administration and the Securities and Exchange Commission, among others). The EU needs to strike a sensible

middle ground in requiring firms to use best-in-class encryption to protect data, but allow them to manage it such that it doesn't unnecessarily affect their ability to operate across markets and jurisdictions.

Encryption is a critical tool firms use to protect data in transit and when stored.[62] It is the process whereby plaintext data is converted to ciphertext using an algorithm that is sufficiently complicated to make the data unreadable without a decryption key. It can be stored and transmitted in this format, and recipients can decrypt it, provided they have the key. Once encrypted data is needed for analysis, compliance, or any other use case, it must be converted back to plaintext. But firms manage this process to minimize risk and maintain compliance with local non-surveillance-related legal requirements.

The EU needs to strike a sensible middle ground in requiring firms to use best-in-class encryption to protect data, but allow them to manage it such that it doesn't unnecessarily affect their ability to operate across markets and jurisdictions.

Encryption is also a critical and common way for firms to demonstrate to regulators and courts that they're committed to data protection (such as in the EU).[63] For example, a 2019 Ponemon Institute study finds that 45 percent of the nearly 5,900 firms it surveyed reported having an encryption strategy applied consistently across their organizations (up from 27 percent in 2015). Slightly less (42 percent) mentioned having a limited encryption strategy used for certain applications or types of data (up from 25 percent in 2015).[64] Firms in Germany, followed by the United States, Australia, and the United Kingdom, were the most likely to have an enterprise encryption strategy. The study shows that encryption is especially crucial in protecting sensitive data, and payment-related data and financial records are most likely to be encrypted (given the impact of high-profile data breaches), followed by employee and human resources and intellectual property data.[65] Forty-four percent of respondents stated that encryption was performed on-premises prior to sending data to the cloud using keys their organization generates and manages. However, 35 percent of respondents perform encryption in the cloud, with cloud provider generated and managed keys.[66]

While encryption is already widely used, implementing encryption-related technical measures will be one of the biggest issues for many firms adapting to the EDPB's guidelines on supplementary measures.[67] The Ponemon study shows that encryption key management is already challenging for the majority (61 percent) of firms.[68] The EDPB's guidance on the use of encryption as a supplementary technical measure is overly broad, with EU-based firms or operations (even within the same company) only able to access EU personal data from the EU. For example, the EDPB's "use case 3" describes encryption safeguards for data routed through a non-adequate country in transit to an adequate one, as if firms control the explicit path that data takes over the Internet. The guidance (again) reinforces why the EU's focus on geography is misguided, as such a broad encryption requirement undermines how encryption tools are used, and would impact the Internet's basic functionality in that data sent from country A to B is routed through the most efficient route, which may be through countries C and D. Firms can't predict where data will go. The guidance also stipulates that data avoid countries (and any firm that abides by these measures) that require "backdoors" in software and hardware to facilitate government access to

data, such as those in Australia.[69] Never mind that some policymakers within Europe support policies that would undermine end-to-end encryption.[70]

This means the EDPB is suggesting a nearly universal need for encryption, and that it only be decrypted within the EU or the small number of countries it deems adequate. In "use case 6" and "use case 7," the EDPB outlined how this would essentially preclude the use of U.S.-based data analytics services as part of normal business operations. In both cases, it stated that "where unencrypted personal data is technically necessary for the provision of the service by the processor, transport encryption and data-at-rest encryption even taken together, do not constitute a supplementary measure that ensures an essentially equivalent level of protection if the data importer is in possession of the cryptographic keys."[71] The EDPB's encryption key requirement (that they remain under the control of entities residing in the EEA or a country deemed adequate) reinforces the de facto localization impact.[72]

Some EU policymakers may point to new technologies such as homomorphic encryption to address this issue, but while this technology has many important applications, it is not feasible for all uses cases. Homomorphic encryption allows analysis of data in its ciphertext form. In short, a third party can perform complicated processing of data without being able to see it.[73] However, the computational requirements for homomorphic encryption can be significantly greater, making the process inefficient or impractical for certain uses.[74] In 2009, a researcher estimated that doing a Google search with encrypted keywords would increase computing time a trillion-fold.[75]

EU policymakers need to realize that it is already possible for firms to use encryption services to undertake secure operations on data without the cloud provider or other third-party service providers being able to access the data, whether for commercial purposes, hacking, or to hand over to local governments. Firms and individuals have access to a growing range of user-friendly and client-side protected end-to-end encryption services, such as those from Virtru, which can be integrated into such existing third-party services as Gmail and Google Drive and Microsoft Office.[76] Many cloud providers (such as Microsoft, Google, IBM, Amazon, and many others) also offer both dedicated hardware security modules for customers to protect their cryptographic keys (from the providers and others) and confidential computing services that protect data in use, within a trusted environment that safeguards data from outside viewing or interference.[77] These tools show that what matters is firms and their service providers are committed to using best-in-class cybersecurity measures and not the geography of data storage.

SMEs and SCCs: The Disproportionate Impact

SMEs and start-ups will be disproportionately affected by the invalidation of Privacy Shield, the need to shift to SCCs, and the broader uncertainty about data transfers and digital trade with the United States and the rest of the world. SMEs lack the resources and expertise to adjust to complicated legal compliance issues. SMEs are also most likely to be unaware of legal changes underway.[78] For example, a 2019 FSB (a U.K. SME-focused trade association) survey of 1,062 SMEs shows that only a small portion were aware they could use SCCs to transfer EU data internationally.[79] The UCL European Institute and New Economy research reinforces this point.[80] The more expensive and complex international data transfer tools become, the less SMEs and start-ups will use them, thus undermining the economies of scale that come from trade. Overall, the resource and expertise advantage of existing large firms is reinforced.

The impact on SMEs will depend on what data protection policies they already have in place. Even then, making changes is unlikely to be straightforward and cheap given the complexity and uncertainty about what's actually required. It's expensive for SMEs to train or hire dedicated staff and go through an audit of data management practices with external legal and consultancy services. Specialist data compliance and consultancy firms state that initial data mapping is the biggest issue in their work with clients, as their clients don't have the tools or know-how to identify and capture all the data that requires specific legal, technical, and administrative management. Data mapping is a system of cataloguing what data a firm collects, how it's used, where it's stored, and how it travels throughout the organization and beyond.[81] Data mapping is a critical first step to fulfill ever-changing and rising legal compliance in the EU. Yet, it's not straightforward to do. Highlighting the technical, administrative, and cost implications of this process, the IAPP-EY 2019 survey shows that manual methods are still common for activities such as data inventory and mapping.[82]

SMEs and start-ups will be disproportionately affected by the invalidation of Privacy Shield, the need to shift to SCCs, and the broader uncertainty about data transfers and digital trade with the United States and the rest of the world.

SME's experience of GDPR should be instructive for policymakers grappling with building a new framework for transatlantic data flows.[83] A survey of EU SMEs two years after GDPR's implementation showed that the two areas they wanted more guidance on were "organizational measures for data protection" and "technical measures for data protection"—both of which are central to current changes to SCCs.[84] The EU can ill afford a repeat performance of its efforts during GDPR's implementation if it wants its SMEs to use transatlantic digital trade to grow and become globally competitive. SMEs will need specific, timely, and practical guidance on what they should do (not only what they shouldn't do) to be in compliance to help them remain engaged in transatlantic digital trade, especially as many battle for survival during COVID-19.

For SMEs, staying in compliance will require a review of existing contracts and business practices, and where necessary, developing, enacting, and demonstrating new procedures and processes. SMEs will need to identify, review, and contact third-party contractors and providers to see what needs to change in determining how to shift from Privacy Shield to SCCs or to revise existing SCCs. It may involve changing or setting up new IT services. SMEs need to be able to demonstrate compliance as a matter of course in developing or shifting to services that provide revised documentation, such as a new data protection policy, new consent forms, and the ability to produce appropriate documentation about relationships with third parties (e.g., controllers/processors). The UCL European Institute and New Economics Foundation study cites legal experts demonstrating how an SME could potentially go to a small data protection firm and get an off-the-shelf document for $1,000–2,000, but that in most cases this is not enough because processor agreements, data documentation, tailored annexes, and privacy notice changes are needed. With each change, the SCC's costs increase.[85]

This is not straightforward for many SMEs and start-ups—the vast majority of which don't have a staff member dedicated to data protection issues. For many SMEs, compliance will involve hiring outside legal counsel and recruiting or designating and training staff to manage data protection issues. Usually one staff member has it as one of a number of responsibilities. Many SMEs relied

on external legal advice to ensure compliance with GDPR, in part, as they struggle to find clear guidance in the GDPR itself and from local authorities. This'll inevitably be the case with international data transfers. But as demand and price for legal services inevitably rises, SMEs will be the ones priced out of—and left without much needed—advice. Furthermore, many SMEs have more pressing budgetary demands, such as marketing, that may provide more immediate benefit, especially as they try to survive COVID.

Helping SMEs adjust so that they can remain engaged in transatlantic digital trade is challenging. European policymakers should apply the many lessons from GDPR's implementation and its impact on SMEs in adjusting to the impact of Privacy Shield's invalidation and any shift to SCCs. Indicative of the challenge facing the Commission, EDPB, EU member states, and DPAs is that studies two years after GDPR's implementation showed that many SMEs thought that GDPR was done and settled. Also, similar to GDPR, while some EU SMEs may be aware of recent legal changes to data transfers, this is different from SMEs actually knowing what they need to do in practice.[86] SMEs reported that they found it challenging to assess proportionality and data protection risks of their operations with GDPR—and this was before *Schrems II.* The ECJ's decision to shift this responsibility to make assessments to organizations only compounds this impact.[87] While GDPR ensured that more businesses that operate in the EU are used to assessing data protection as part of their work, it's a whole other challenge to make them responsible for analyzing changing laws in Brazil, India, or some other country to see if it offers a comparable level of protection.[88]

Firms with limited resources need clear guidelines, contact points, and assistance. The EDPB has produced timely and detailed guidance on supplementary measures, but this is far from what's required to truly help SMEs. To its credit, the Commission recognizes the vulnerability of SMES regarding GDPR in stating, "There is in particular a need to step up awareness and accompany compliance efforts for SMEs."[89] However, SME awareness of GDPR was highly variable across sectors and member states, and was driven by DPA activity, which overall was lacking.[90] Many DPAs don't have dedicated research and outreach targeting SMEs. For examples, as of 2019, less than one quarter of EU DPAs provided specific guidance on GDPR to SMEs.[91] Even if SMEs were aware of GDPR (or in this case, changes to international transfers), GDPR's implementation showed that awareness doesn't always lead to compliance—it's just a first step. Absent other drivers and the knowledge to put compliance into practice, it's not enough.[92]

As surveys and studies of GDPR's impact on SMEs shows, SMEs need targeted assistance that differs from general guidance documents. If it's too academic or legalistic, it won't be seen as useful, and it'll reinforce the perspective that DPA guidance is tailored to large data controllers, not SMEs. Studies show that SMEs dealing with GDPR prized clear advice and concrete steps they could take to comply. This included recommendations for an SME handbook with examples and templates, sector-specific handbooks, and a risk-focused handbook.[93] They need practical advice entailing a step-by-step approach of what they need to do.[94] This will inevitably be the case again with changes to international data transfers. SME reactions will depend in large part on whether their home country DPA engages in outreach and communication activities, and whether they provide clear and specific guidance in local languages.[95]

U.S. and EU policymakers need to prioritize the development of clear, practical, and realistic advice and guidance—both interim and final—for SMEs if they want to build a truly inclusive

transatlantic digital trade framework. EU policymakers were overly optimistic in thinking that a two-year lead-in time for organizations (including SMEs) preparing for GDPR was sufficient.[96] Policymakers should also provide some form of grace period and engagement program during negotiations on a revised or new Privacy Shield. Time is needed for recent changes. After GDPR, EU SMEs that had previously existed outside any meaningful compliance regime other than tax and finance now face a new level of accountability to the public and DPAs.[97] Perhaps after a future Privacy Shield 2.0 and changes to SCCs, SMEs will go through a similar learning and adaption process. But policymakers need to take immediate and specific action to ensure attrition—in terms of SMEs that withdraw from transatlantic trade—during this time of change and uncertainty is minimized.

The specific impact on SMEs will vary. With SCCs, there is a cutoff point: At a certain size, companies are too small and lack the necessary expertise and connections to take on the cost of adopting SCCs. For mid-sized firms that do have the capacity to implement SCCs, EDPB guidance has so far been insufficient for practical implementation. Meanwhile, many start-ups are hesitant to adopt SCCs while they remain under scrutiny. The longer uncertainty lingers, or the higher the cost of adapting to SCCs becomes, the more likely it is that the cost side of the cost-benefit analysis will cause these firms to simply withdraw from trade and the use of non-EU best-in-class data services. The relative cost of compliance—between big and small firms, and between firms in Europe and the United States and other markets—will become a bigger factor over time.

People involved in tech start-ups are typically problem solvers, but the more they look at the changing legal framework for data transfers, the less impressed they're likely to be given the changes and uncertainty. It must be a sobering experience for most start-ups to consider and enact the type of changes the EU is contemplating for data transfers, never mind when other pending legislation regarding AI regulation and data governance is added to the equation.[98] In the longer term, prohibitive costs and uncertainty will make more start-ups think about whether they set up in the United States or somewhere else in order to test their ideas and grow and achieve critical economies of scale before potentially entering and operating in Europe (after they've grown past the cutoff point beyond when it makes sense).

GDPR's implementation shows what is required to minimize or avoid the disproportionate impact these changes and the legal uncertainty have on SMEs. Policymakers should ensure SMEs can engage in data transfers and digital trade just as easily as large firms, especially with this happening during a time when data flows and digital tools are more critical than ever (i.e., COVID). The cost and complexity of transfers becoming and remaining high would essentially preclude all but the largest firms from engaging in digital trade with the EU, thus undermining one of the central benefits of the Internet: mitigating the impact that geography has on trade and commerce.

The EU's End Game? The Misguided Drive for Data Localization Will Impact Productivity and Trade

Faced with a lack of viable and robust alternatives, many firms may decide to suspend data transfers to avoid violating GDPR. The ECJ noted that data exporters and their supervisory DPA are required to invalidate a transfer pursuant to SCCs wherever they cannot guarantee adequate protection. In practice, this means relevant DPAs can challenge an exporter's contractual

relationship with importers in any country without an adequacy decision. And with Privacy Shield invalidated, this includes the United States. Firms may be uncertain about supplementary measures to address outstanding concerns about U.S. and other countries' surveillance laws, thus leading them back to localization.[99] Given the uncertainty and large potential fines, it's understandable that many firms will take an overly risk-averse and conservative approach to data management, and require EU personal data to be stored and processed locally. Ultimately, by making data transfers so complicated, costly, and uncertain, the EU will create the world's largest de facto data localization requirement. It would put Europe alongside China—the leader of explicit data localization.[100]

Ultimately, by making data transfers so complicated, costly, and uncertain, the EU will create the world's largest de facto data localization requirement. It would put Europe alongside China—the leader of explicit data localization.

Unfortunately, data localization has long been the misguided goal for some policymakers in the EU, and increasingly the rhetoric in Europe is not about protecting European data, but about creating policies that unfairly promote European economic growth.[101] In Germany, the Commissioner for the DPA in Berlin declared that "the hour for Europe's digital independence has arrived" after the *Schrems II* decision was announced.[102] Hamburg's DPA noted that "difficult times are looming for international data traffic." [103] France's DPA said that organizations processing health data should not use American cloud hosting companies.[104] And Thierry Breton, European Commissioner for the Internal Market, argued that "European data should be stored and processed in Europe because they belong in Europe."[105] The implications are not just for EU-U.S. data flows, but global. Berlin's DPA mentioned China, Russia, and India as countries EU DPAs will also have to assess.[106]

The Irish DPA's preliminary order shows that data localization is not a hypothetical outcome given its advice to cut off Facebook's transfers of EU user data back to the United States. Cutting off data transfers would significantly limit or even entirely restrict the availability of Facebook services to millions of European users. Facebook has stated that it "[has] absolutely no desire, no wish, no plans to withdraw [Facebook's] services from Europe"—but if the Irish DPC's order is ultimately enforced, Facebook (and other firms confronting similar difficulties) may no longer be able to provide services in the EU.[107] The impact goes well beyond individuals' profile pages in that in Europe, Facebook has 25 million companies using its apps and tools (largely for free).[108] But the impact goes far beyond Facebook when other DPAs pursue similar investigations and come to similar conclusions.

The implications of "fortress Europe" are many and varied. Customer and product support rely on the ability to share and access data across jurisdictions. Firms such as Facebook that rely on cross-border data flows for real-time communications could not fully localize this data without also limiting the reach of their service. EU users would potentially be cut off from friends around the world. From a regulatory perspective, many firms, such as in the financial sector, rely on international data transfers to maintain compliance with reporting requirements. Cutting off international data flows with Europe would have a potentially broad economic and innovation impact as today's economy is increasingly dependent on how firms use data—and if local firms are prevented from using the best data-driven services, this will inevitably affect their survival

and success.[109] As DIGITALEUROPE stated, the millions of transactions that take data in and out of Europe happen every day and are the lifeblood of the modern economy.[110] A situation that leads to fewer, more expensive data analytics services will lead to fewer firms using such services (as cost is a key determinate of ICT adoption and deployment), which will affect data-driven innovation in an economy. The Organization for Economic Cooperation and Development (OECD) has found that the probability of innovation increases with the intensity of ICT use.[111]

Data localization would seriously undermine transatlantic digital trade. It would be impossible for many large U.S. firms to fully localize any line of business in the EU without some degree of impact or disruption. This is besides (or perhaps due to, given EU supporters of digital protectionism) the fact that U.S. cloud providers such as Amazon, Google, IBM, Microsoft, and Salesforce are market leaders in Europe.[112] Besides cost, flexibility, and value-added services, a key benefit to using leading cloud service providers is a lot of the responsibility for managing the complexities of global regulations falls on them. For example, some firms offer clients data-residency options so they can choose to store data only within certain regions.[113] While, for example, it may be technically possible for a firm (particularly a large one) to fully localize local data storage, there would still be major disruptions and changes to the types and quality of the data analytic service, especially between those used in and outside of Europe. While the underlying data center infrastructure does not necessarily rely on the ability to exchange data across borders, the services built on it certainly do.

These cloud-based services are central to economic productivity and innovation. Cutting off access to cloud-based, best-in-class services in the United States would impact firm competitiveness and economic productivity and innovation. Firms cannot be competitive if they cannot use cloud-based services, including email, calendaring, and office-productivity tools. Whether directly or indirectly, thousands of firms use other more specialized software-as-a-service (SaaS) providers that rely in part on U.S.-based operations, such as Adobe, Atlassian, DocuSign, Dropbox, Mailchimp, Salesforce, Slack, SurveyMonkey, and Zoom. For many firms, key cloud-based business services include enterprise resource planning, customer relationship management, human resource management, and supply chain management. These cloud-based services provide cost savings, flexible utilization, easier user management, and better coordination between decentralized teams. Without these services during COVID, businesses would have seen massive disruptions when people transitioned to remote work.

Moreover, data localization limits firms from maximizing the benefits of data analytics. First, it prevents EU firms from accessing best-in-class analytics services that are located abroad because they cannot transfer the data to these data processors. Second, it prevents EU-based firms with a global footprint from making use of in-house analytics because they cannot pull their data together due to data localization requirements. This has broad ramifications, as today's data economy is transitioning into the algorithmic economy in which many more organizations invest in artificial intelligence (AI) to automate processes, develop new products and services, improve quality, and increase efficiency.[114] Payments, financial, insurance, Internet consumer services, automotive firms, retailers, marketing, mining, agriculture, and any other number of sectors benefit from improved data analytics. Forcing firms that manage EU personal data to relocate all data processing to the EU would require them to reconstruct their analytics operations, including the associated cybersecurity and other IT systems, such that they would transfer no personal data

out of the EU or other countries with adequacy decisions. Such an endeavor would be an incredibly costly and complicated process.

Barriers that make it costlier, more complex, or illegal for firms to export and use data as part of centralized data analytics platforms undermine their ability to use data from the broadest range of sources to provide secure, innovative, and standardized services to customers around the world. These restrictions prevent firms from working with global datasets and providing quicker and more effective data-driven services.

In the case of data, the whole is greater than the sum of its parts. Data localization policies reduce data quality by reducing completeness of datasets, and lower data quality results in poorer analytics. For example, these data localization policies can undermine the ability of payment firms to use data analytics on global datasets to combat payment fraud, which is a problem for consumers, financial institutions, and regulators. When a transaction is initiated, hundreds of pieces of information (for example, about the customer, merchant, place, and time, all compared against years' worth of prior transactions) are gathered and sent for analysis by the payments processer's predictive model to determine whether it is likely a genuine or fraudulent transaction. For payments firms, this process may happen tens of thousands of times daily, which ultimately involves billions of pieces of data. 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) to proactively identify risks. [115] For firms to build the best-quality fraud models and gain insights for fraud prevention, payment service firms need unimpeded access to the analytics platforms and relevant data, no matter where in the world the data originates. Ultimately, forcing payment service firms to use a limited dataset for analysis would lower the quality and accuracy of their prediction models for fraud and other services. Firms that use analytics in other sectors would be affected in similar ways.

Attempts to run parallel data analytics operations to circumvent data localization policies are inefficient at best, and ineffective at worst. In addition to the costs of running and maintaining duplicative analytics platforms, firms would also have to manage multiple analytics platforms, including separately validating the accuracy of their models, updating their models, testing for biases, and more, creating major operational challenges.[116] These problems are compounded if the firms have to manage multiple data analytics operations across multiple countries and regions. Ultimately, given the cost and complexity involved in setting up duplicative local data storage and analytic services, firms will have to decide whether it's feasible to stay in the market, and if so, what scaled-down products to offer, or to just leave.

CONCLUSION

Uncertainty reigns supreme in relation to Europe's evolving approach to the global digital economy. Firms involved in EU-U.S. trade are already starting transfer impact assessments and contingency planning (no matter how provisionally) to figure out what they need to do to update or replace the SCCs they currently use, consider changes to data storage and analytics practices between Europe and the rest of the world, prepare potential legal challenges (and for litigation), or otherwise decide it's become too much and leave altogether. Absent some other major policy intervention (such as a Privacy Shield 2.0), staying engaged in transatlantic transfers will likely require a growing army of people and resources to ensure compliance.

Policymakers should not passively accept the slow-motion train wreck that seems to be taking place, nor allow the EU to escape its responsibility for serving as the train's conductor.

The repeated, drawn out, and legalistic nature of the challenges to EU-U.S. data flows has lulled policymakers into a dangerous sense of complacency (or perhaps, fatalism). Policymakers should not passively accept the slow-motion train wreck that seems to be taking place, nor allow the EU to escape its responsibility for serving as the train's conductor. It obscures the fact that the role and value of data flows and digital trade only continue to grow. As mentioned in the prior briefing on Privacy Shield, it also distracts from the broader recognition that the two sides actually share much more in common than many policymakers realize, including values of democracy and rule of law and deeply intertwined objectives for economic growth and technological advancement.

As the EDPB states, SCCs and other transfer tools mentioned under GDPR do not operate in a vacuum.[117] But it's a matter of determining what should be reasonably expected of the various actors in filling this void. The private sector can only do so much. The United States and EU should take the lead in removing this legal uncertainty by finding a better way to account for legitimate national security and surveillance concerns. Policymakers need to redouble efforts to create the legal tools and overarching frameworks to reasonably, clearly, and coherently manage data privacy and national security issues related to transatlantic transfers.

Acknowledgments

This report was made possible in part by generous support from Facebook. Any errors or omissions are the authors' responsibility alone.

About the Authors

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

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

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

About ITIF

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

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

ENDNOTES

1. 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. "An early analysis of *Schrems II*–key questions and possible ways forward," DIGITALEUROPE, August 31, 2020, https://www.digitaleurope.org/wp/wp-content/uploads/2020/08/DIGITALEUROPE_An-early-analysis-of-Schrems-II_Key-questions-and-possible-ways-forward.pdf.
3. "IAPP-EY Annual Governance Report 2019," IAPP, 2019, https://iapp.org/resources/article/iapp-ey-annual-governance-report-2019.
4. "*Schrems II*: Impact Survey Report," Business Europe, DIGITALEUROPE, the European Round Table for Industry, and European Automobile Manufacturers Association, November 26, 2010, https://www.businesseurope.eu/sites/buseur/files/media/reports_and_studies/2020-11-26_schrems_ii_impact_survey_report.pdf.
5. Daniel Castro and Alan McQuinn, "Cross-Border Data Flows Enable Growth in All Industries" (ITIF, February 24, 2015), https://itif.org/publications/2015/02/24/cross-border-data-flows-enable-growth-all-industries; Cory, Castro, and Dick, "'Schrems II': What Invalidating the EU-U.S. Privacy Shield Means for Transatlantic Trade and Innovation."
6. "Adequacy decisions," European Commission, https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en.
7. The GDPR endorses the use of approved codes of conduct and certification mechanisms to demonstrate compliance with its requirements. The EDPB has produced guidance on codes of conduct. However, no approved codes of conduct are yet in use. "Code of Conduct," European Data Protection Board, November 10, 2020, https://edpb.europa.eu/our-work-tools/our-documents/topic/code-conduct_en; "Codes of Conduct," U.K. Information Commissioner's Office, https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/codes-of-conduct/; Eline Chivot and Nigel Cory, "Response to European Commission Consultation on Transfers of Personal Data to Third Countries and Cooperation Between Data Protection Authorities" (ITIF, April 29, 2020), https://itif.org/publications/2020/04/29/response-european-commission-consultation-transfers-personal-data-third.
8. "Data Protection Commissioner v Facebook Ireland Limited, Maximillian Schrems (Schrems II)," ECJ judgement on case C-311/18, July 16, 2020, http://curia.europa.eu/juris/document/document.jsf?text=&docid=228677&doclang=en.
9. "Adequacy decisions," European Commission, https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en.
10. "What is a data controller or a data processor?," European Commission, https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/controller-processor/what-data-controller-or-data-processor_en; "Standard Contractual Clauses," European Commission, https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en.
11. Ibid.
12. "International transfers," U.K. Information Commissioner's Office, https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/international-transfers/.

13. "Keep data flowing from the EEA to the UK – interactive tool," U.K. Information Commissioner's Office, https://ico.org.uk/for-organisations/data-protection-at-the-end-of-the-transition-period/keep-data-flowing-from-the-eea-to-the-uk-interactive-tool/.
14. "IAPP-EY Annual Governance Report 2019," IAPP.
15. "*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.
16. Ibid.
17. Ibid. Many respondents selected 'other,' mentioning countries such as Australia, Russia, and others. Switzerland, Canada, and Japan are among the third countries recognized by the European Commission as providing adequate protection; they therefore do not appear on this list as transfers to those countries do not require SCCs.
18. Ibid.
19. Nick Clegg, "Securing the Long Term Stability of Cross-Border Data Flows," blog post, Facebook, September 9, 2020, https://about.fb.com/news/2020/09/securing-the-long-term-stability-of-cross-border-data-flows/.
20. Sam Schechner and Emily Glazer, "Ireland to Order Facebook to Stop Sending User Data to U.S.," *Wall Street Journal,* September 9, 2020, https://www.wsj.com/articles/ireland-to-order-facebook-to-stop-sending-user-data-to-u-s-11599671980.
21. "DPC statement on CJEU decision," Irish Data Protection Commission, press release, July 16, 2020, https://www.dataprotection.ie/en/news-media/press-releases/dpc-statement-cjeu-decision.
22. Ibid.
23. "Irish High Court: Judicial Review against DPC admitted," noyb, press release, September 14, 2020, https://noyb.eu/en/irish-high-court-judicial-review-against-dpc-admitted.
24. "EU-US Data Transfers - Judicial Review Proceedings," Irish Data Protection Commission, press release, December 3, 2020, https://www.dataprotection.ie/en/news-media/press-releases/eu-us-data-transfers-judicial-review-proceedings.
25. *Article 60 EU GDPR:* "Cooperation between the lead supervisory authority and the other supervisory authorities concerned."
26. "Facebook tells Irish court that probe threatens its EU operations – newspaper," *Reuters,* September 20, 2020, https://www.reuters.com/article/us-facebook-privacy/facebook-tells-irish-court-that-probe-threatens-its-eu-operations-newspaper-idUSKCN26B0CV.
27. "Data Protection Commissioner v Facebook Ireland Limited, Maximillian Schrems (Schrems II)," ECJ.
28. Ibid.
29. Ibid.
30. Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data" are applicable immediately. "Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data," European Data Protection Board, November 10, 2020, https://edpb.europa.eu/sites/edpb/files/consultation/edpb_recommendations_202001_supplementarymeasurestransferstools_en.pdf.
31. The EDPB: "assess if there is anything in the law or practice of the third country that may impinge on the effectiveness of the appropriate safeguards of the transfer tools you are relying on, in the context of your specific transfer." Ibid.

32. "Recommendations 02/2020 on the European Essential Guarantees for surveillance measures," European Data Protection Board, November 10, 2020, https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_recommendations_202002_europeanessentialguaranteessurveillance_en.pdf.
33. "Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data," European Data Protection Board.
34. 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/.
35. The EDPB: "is to identify and adopt supplementary measures that are necessary to bring the level of protection of the data transferred up to the EU standard of essential equivalence." "Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data," European Data Protection Board.
36. These include strong encryption prior to transmission, resilience of the encryption in the face of cryptanalysis by public authorities, "flawless" implementation of the encryption algorithm, and maintenance of the keys in the EEA, among others. "Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data," European Data Protection Board.
37. Ibid.
38. Henriette Tielemans, "What to expect on revised standard contractual clauses," IAPP blog post, September 29, 2020, https://iapp.org/news/a/revised-standard-contractual-clauses-what-to-expect.
39. Ibid.
40. The survey was created on SurveyMonkey and made publicly available online. It comprised 9 multiple choice questions in total. the survey to run anonymously, in the sense that we did not ask any participants to identify themselves, so we do not know the identity of any participants who responded, but it is reasonable to assume that respondents from organizations both within and without the EEA and UK will have participated across a variety of sectors. They turned on a survey feature that prevented the same respondent from completing the survey twice. In total, Field Fisher received 138 responses. "The results are in: How *Schrems II* will impact international data flows in practice," Field Fisher blog post, September 9, 2020, https://www.fieldfisher.com/en/services/privacy-security-and-information/privacy-security-and-information-law-blog/how-schrems-ii-will-impact-international-data-flow.
41. Cory, Castro, and Dick, "'*Schrems II*': What Invalidating the EU-U.S. Privacy Shield Means for Transatlantic Trade and Innovation."
42. "IAPP-EY Annual Governance Report 2019," IAPP.
43. System and Organization Controls 2 (SOC 2) are one of the most sought-after standards in security and compliance. It is a type of audit (done by an independent, third parties) that attests to the trustworthiness of services provided by a service organization. It is commonly used to assess the risks associated with outsourced software solutions that store customer data online. It was developed by the American Institute of CPAs. SOC 1 and SOC 2 reports were introduced by the AICPA (The American Institute of Certified Public Accountants) with the explicit purpose of addressing the growing need of companies to externally validate and communicate their state of security.
44. Duncan McCann, Oliver Patel, and Javier Ruiz, "The Cost of Data Inadequacy: The economic impacts of the UK failing to secure EU data adequacy" (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.
45. Ibid.
46. "IAPP-EY Annual Governance Report 2019," IAPP.

47. "IAPP-EY Annual Governance Report 2017," IAPP, https://iapp.org/resources/article/iapp-ey-annual-governance-report-2017/.
48. "Information on U.S. Privacy Safeguards Relevant to SCCs and Other EU Legal Bases for EU-U.S.Data Transfers after *Schrems II*," (Washington, D.C: U.S. Commerce Department, Justice Department, and the Office of the Director of National Intelligence, September 2020), https://www.commerce.gov/sites/default/files/2020-09/SCCsWhitePaperFORMATTEDFINAL508COMPLIANT.PDF; Bradley Brooker and Sujit Raman, "The Need for Clarity After *Schrems II*," Lawfare blog post, September 29, 2020, https://www.lawfareblog.com/need-clarity-after-schrems-ii.
49. Ibid.
50. Tielemans, "What to expect on revised standard contractual clauses," IAPP blog post.
51. "Statement of the Article 29 Working Party (on the *Schrems I* judgement)," Article 29 Working Party (the predecessor to the EDPB), October 16, 2015, https://www.huntonprivacyblog.com/wp-content/uploads/sites/28/2015/10/20151016_wp29_statement_on_schrems_judgement-2.pdf.
52. [translated] "Difficult times ahead for international transfer of data," Hamburg's Data Protection Authority, July 16, 2020, https://datenschutz-hamburg.de/pressemitteilungen/2020/07/2020-07-16-eugh-schrems.
53. "EU-US Transfers Complaint Overview," noyb website, https://noyb.eu/en/eu-us-transfers-complaint-overview.
54. "Adequacy decisions," European Commission, https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en.
55. "Binding Corporate Rules," European Commission, https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/binding-corporate-rules-bcr_en.
56. "Binding corporate rules," U.K. Information Commissioner's Office, https://ico.org.uk/for-organisations/binding-corporate-rules/; "Binding Corporate Rules," pwc report, https://www.pwc.com/m1/en/publications/documents/pwc-binding-corporate-rules-gdpr.pdf.
57. For example, see: "Opinion 15/2019 on the draft decision of the competent supervisory authority of the United Kingdom regarding the Binding Corporate Rules of Equinix Inc.," European Data Protection Board, October 8, 2019, https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_opinion_201915_equinixbcrs_en.pdf; "List of companies for which the EU BCR cooperation procedure is closed," IAPP website, May 24, 2018, https://iapp.org/media/pdf/resource_center/eubcrprocedureclosed.pdf.
58. The authority will approve the BCRs in accordance with the consistency mechanism set out in Article 63 of GDPR. "Working Document setting up a table with the elements and principles to be found in Binding Corporate Rules," Article 29 Working Party, February 6, 2018, https://ico.org.uk/media/for-organisations/documents/2259711/wp-256-bcr-controllers-referential.pdf; "Working Document setting up a table with the elements and principles to be found in Processor Binding Corporate Rules," Article 29 Working Party, November 29, 2017, http://ec.europa.eu/newsroom/just/document.cfm?doc_id=48799.
59. "*Schrems II*: Impact Survey Report," Business Europe, DIGITALEUROPE, the European Round Table for Industry, and European Automobile Manufacturers Association.
60. "Changes to Binding Corporate Rules applications to the ICO," U.K. Information Commissioner's Office blog post, November 20, 2017, https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2017/11/blog-changes-to-binding-corporate-rules-applications-to-the-ico/.
61. Although the Schrems II ruling does not directly address BCRs, the EDPB has already stated that the BCRs should undergo the same re-assessment by companies as SCCs. "Frequently Asked Questions on the judgment of the Court of Justice of the European Union in Case C-311/18 -Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems," European Data Protection Board,

July 23, 2020, https://edpb.europa.eu/sites/edpb/files/files/file1/20200724_edpb_faqoncjeuc31118.pdf.

62. Daniel Castro, "Why New Calls to Subvert Commercial Encryption Are Unjustified" (ITIF, July 13, 2020), https://itif.org/publications/2020/07/13/why-new-calls-subvert-commercial-encryption-are-unjustified.
63. GDPR emphasizes data governance and accountability when firms manage personal data, requiring firms to assess the risk of data loss and data breach and requires them to consider technical—"state of the art"—measures to mitigate those risks, including encryption. Because encryption is a common security measure and cybersecurity risks are increasing, it is likely that regulators and courts in Europe will find that encryption is necessary to comply with GDPR. The European Union Agency for Information and Network Security (ENISA) recommendation for end-to-end encryption for email supports this likely outcome. Similarly, encryption of cardholder data is an acceptable method of rendering data unreadable in order to meet the Payment Card Industry Data Security Standard (PCI DSS), which is a set of security controls that businesses are required to implement to protect credit card data in the United States. European Union Agency for Network and Information Security, "Privacy and Data Protection by Design" (Heraklion, Greece, January 12, 2015), https://www.enisa.europa.eu/publications/privacy-and-data-protection-by-design.
64. It surveyed 5,856 individuals across multiple industry sectors in 14 countries/regions: Australia, Brazil, France, Germany, India, Japan, Mexico, the Middle East (which is a combination of respondents located in Saudi Arabia and the United Arab Emirates), the Russian Federation, South Korea, the United Kingdom, the United States and, two new regions in Asia for the first time, Southeast Asia (Indonesia, Malaysia, Philippines, Thailand and Vietnam) and Hong Kong and Taiwan. "2019 Global Encryption Trends Study," Ponemon Institute report, 2019, https://go.ncipher.com/rs/104-QOX-775/images/2019-Ponemon-Global-Encryption-Trends-Study-es-ar.pdf.
65. Ibid.
66. Ibid.
67. Sam Sabin, "Months After Privacy Shield's Death, Formal Negotiations on New E.U.-U.S. Pact Said to Start Soon," *Morning Consult,* November 25, 2020, https://morningconsult.com/2020/11/25/privacy-shield-compliance-issues/; Catherine Stupp, "EU Restrictions Could Force Companies to Change Data Transfer Practices," *Wall Street Journal,* November 17, 2020, https://www.wsj.com/articles/eu-restrictions-could-force-companies-to-change-data-transfer-practices-11605609001.
68. "2019 Global Encryption Trends Study," Ponemon Institute.
69. For example: "The exporter could also add clauses whereby the importer certifies that (1) it has not purposefully created back doors or similar programming that could be used to access the system and/or personal data (2) it has not purposefully created or changed its business processes in a manner that facilitates access to personal data or systems, and (3) that national law or government policy does not require the importer to create or maintain back doors or to facilitate access to personal data or systems or for the importer to be in possession or to hand over the encryption key. "Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data," European Data Protection Board.
70. Ashley Johnson, "New Draft Resolution on Encryption Casts Doubt on EU's Commitment to Data Protection," *Innovation Files,* blog post, November 18, 2020, https://itif.org/publications/2020/11/18/new-draft-resolution-encryption-casts-doubt-eus-commitment-data-protection.
71. "Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data," European Data Protection Board.

72. From use case 1 and others: "the keys are retained solely under the control of the data exporter, or other entities entrusted with this task which reside in the EEA or a third country, territory or one or more specified sectors within a third country, or at an international organisation for which the Commission has established in accordance with Article 45 GDPR that an adequate level of protectionis ensured." Ibid.
73. Craig Gentry, "Computing Arbitrary Functions of Encrypted Data," *Communications of the ACM*, 53.3 (2010): 97-105, https://crypto.stanford.edu/craig/easy-fhe.pdf.
74. Bruce Schneier, "Homomorphic Encryption Breakthrough," Schneier on Security blog post, 2009, https://www.schneier.com/blog/archives/2009/07/homomorphic_enc.html.
75. Ibid.
76. Nigel Cory, "Fostering an Enabling Policy and Regulatory Environment in APEC for Data-Utilizing Businesses: Chapter 5: Encryption Services" (Asia Pacific Economic Cooperation (APEC) report, July 2019), https://www.apec.org/-/media/APEC/Publications/2019/7/Fostering-an-Enabling-Policy-and-Regulatory-Environment-in-APEC-for-Data-Utilizing-Businesses/TOC/Chapter-5.pdf%20.
77. "Confidential Computing Consortium: Defining and Enabling Confidential Computing," the Confidential Computing Consortium, 2019, https://confidentialcomputing.io/wp-content/uploads/sites/85/2019/12/CCC_Overview.pdf; Stephen Withers, "Confidential computing is part of IBM's cloud vision," *IT Wire*, August 13, 2020, https://www.itwire.com/cloud/confidential-computing-is-part-of-ibm-s-cloud-vision.html; "AWS Nitro Enclaves," AWS, https://aws.amazon.com/ec2/nitro/nitro-enclaves/; "Schrems II additional safeguards: confidential computing," Kuan0 blog post, August 17, 2020, https://blog.kuan0.com/2020/08/schrems-ii-additional-safeguards.html.
78. Indicative of this, 25 per cent of respondents appear not to be aware that they transfer data outside of the EU, most likely through SCCs. This is despite the fact that most contributions to the survey have come from data protection or compliance professionals. SMEs are more likely to be in this group but almost a quarter of bigger companies are also affected. This proves a fairly widespread lack of understanding about personal data transfers and the ensuing obligations, which may expose companies to sanctions for GDPR infringement. "*Schrems II*: Impact Survey Report," Business Europe, DIGITALEUROPE, the European Round Table for Industry, and European Automobile Manufacturers Association.
79. "Destination Digital: How small firms can unlock the benefits of global e-commerce," (fsb, November 1, 2019), https://www.fsb.org.uk/resources-page/destination-digital-report-pdf.html.
80. McCann, Patel, and Ruiz, "The Cost of Data Inadequacy: The economic impacts of the UK failing to secure EU data adequacy" (UCL European Institute report with the New Economics Foundation).
81. "Brexit update – the shape of the United Kingdom's exit," Evershed Sutherland website, January 29, 2020, https://www.eversheds-sutherland.com/global/en/what/articles/index.page?ArticleID=en/Brexit/shape-of-uk-exit-290120.
82. "IAPP-EY Annual Governance Report 2019," IAPP.
83. "General Data Protection Regulation Two-Year Review: Clear guidance for SMEs and stronger European-minded Data Protection Authorities," (European Digital SME Alliance, position paper, June 10, 2020), https://www.digitalsme.eu/digital/uploads/Position-Paper-GDPR-Review-2020.pdf; David Barnard-Wills, Leanne Cochrane, Kai Matturi, and Filippo Marchetti, "Report on the SME experience of the GDPR (Deliverable 2.2)" (joint study by Nemzeti Adatvédelmi és Információszabadság Hatóság, Trilateral Research Ltd., and Vrije Universiteit Brussel Research Group on Law, Science, Technology and Society for the European Commission's Directorate-General for Justice and Consumers, July 2019), https://www.trilateralresearch.com/wp-content/uploads/2020/01/STAR-II-D2.2-SMEs-experience-with-the-GDPR-v1.0-.pdf.
84. Figure 11. Ibid.

85. McCann, Patel, and Ruiz, "The Cost of Data Inadequacy: The economic impacts of the UK failing to secure EU data adequacy" (UCL European Institute report with the New Economics Foundation).

86. "While awareness of the GDPR among SMEs was a need identified by a few DPAs, across the whole of the STAR II research awareness of the basic existence of the GDPR among SMEs seemed to be relatively high (see Deliverable D2.2). The distinction between SME awareness of the existence of the GDPR and SME awareness of the requirements of the GDPR, however, appeared to be significant. This means that while awareness of the GDPR appeared to have grown, that awareness does not translate to an equivalent awareness and/or understanding of specific GDPR provisions. Furthermore, the SMEs that remain unaware of the GDPRs existence are unlikely to approach the DPA for advice or consultation regarding the GDPR." David Barnard-Wills, Leanne Cochrane, Kai Matturi, and Filippo Marchetti, "Report on DPA efforts to raise awareness among SMEs on the GDPR (Deliverable 2.1) (joint study by Nemzeti Adatvédelmi és Információszabadság Hatóság, Trilateral Research Ltd., and Vrije Universiteit Brussel Research Group on Law, Science, Technology and Society for the European Commission's Directorate-General for Justice and Consumers, October, 2019), https://www.trilateralresearch.com/wp-content/uploads/2020/01/STAR-II-D2.1-DPA-awareness-raising-v1.1.pdf; Ashford Warwick, "Most UK small businesses in the dark over GDPR", *ComputerWeekly.com*, November 7, 2017, http://www.computerweekly.com/news/450429625/Most-UK-small-businesses-in-the-dark-over-GDPR.

87. "SMEs find it challenging to assess proportionality and data protection risks of their operations and would rather have clear steps to take to comply with requirements stemming from the GDPR. " Barnard-Wills, Cochrane, Matturi, and Marchetti, "Report on the SME experience of the GDPR (Deliverable 2.2)."

88. Cecilia Bonefeld-Dahl, "Schrems II ruling puts European recovery at risk," *The Parliament Magazine,* September 15, 2020, https://www.theparliamentmagazine.eu/news/article/schrems-ii-ruling-puts-european-recovery-at-risk-22391.

89. "Commission publishes guidance on upcoming new data protection rules," press release, European Commission, January 24, 2018, https://ec.europa.eu/commission/presscorner/detail/en/IP_18_386.

90. Barnard-Wills, Cochrane, Matturi, and Marchetti, "Report on DPA efforts to raise awareness among SMEs on the GDPR (Deliverable 2.1)."

91. Survey conducted for deliverable 1.1 found that most DPAs neither conduct specific research aimed at establishing levels of SME awareness nor general awareness of the GDPR. A quarter of DPAs who responded had SME specific guidance, i.e. 5 out of 18 DPA respondents. (Based on the SME association interviews and additional desktop research, three further DPAs were identified as having SME specific guidance. Out of 28 total DPAs, this retains the percentage at just over one quarter.) Ibid; STAR II, Deliverable 4.1 Draft versions of the guidance & handbook (version 1.1, 2020), cited in: "General Data Protection Regulation Two-Year Review: Clear guidance for SMEs and stronger European-minded Data Protection Authorities," (European Digital SME Alliance, position paper, June 10, 2020).

92. Barnard-Wills, Cochrane, Matturi, and Marchetti, "Report on the SME experience of the GDPR (Deliverable 2.2)."

93. Ibid.

94. Barnard-Wills, Cochrane, Matturi, and Marchetti, "Report on DPA efforts to raise awareness among SMEs on the GDPR (Deliverable 2.1)."

95. "SME awareness depends largely on guidance provided in the language of their jurisdiction: SMEs are likely not aware of guidance from the EDPS or other non-national data protection bodies (e.g., the EDPB). Barnard-Wills, Cochrane, Matturi, and Marchetti, "Report on the SME experience of the GDPR (Deliverable 2.2)."

96. Alan Moore, Leanne Cochrane, and David Barnard-Wills, "What are the challenges that SMEs are facing in complying with the GDPR? A view from the field," Trilateral Research blog post (no date),

https://www.trilateralresearch.com/challenges-facing-smes-in-complying-with-the-gdpr-a-view-from-the-field/.

97. Ibid.
98. For example: Allied for Startups, "Open Letter: Commit to Data Flows & Back it up with Action" (joint letter by Allied for Startups and startup associations from around Europe, October 8, 2020), https://alliedforstartups.org/2020/10/08/open-letter-commit-to-data-flows-back-it-up-with-action.
99. EDPB recommendations regarding points 88 and 89 "scenarios in which no effective measures could be found." And whether they mean effective "technical" measures, such as contractual and organizational (pages 28-37), to account for the lack of sufficient protection's in the importer's country law. And whether they also mean properly applied technological tools that effectively inhibit access to the data content, such as end-to-end encryption and encryption key management. "Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data," European Data Protection Board.
100. Nigel Cory, "Why China Should Be Disqualified From Participating in WTO Negotiations on Digital Trade Rules" (ITIF, May 9, 2019), https://itif.org/publications/2019/05/09/why-china-should-be-disqualified-participating-wto-negotiations-digital.
101. Daniel Castro, "The False Promise of Data Nationalism" (ITIF, December 2013), http://www2.itif.org/2013-false-promise-data-nationalism.pdf; Vincent Manancourt, "Europe's data grab: A once-taboo policy backed by Russia and China is on the cards as Brussels embraces data protectionism — to Silicon Valley's dismay," *Politico,* February 19, 2020, https://www.politico.eu/article/europe-data-grab-protection-privacy.
102. [translation] "According to "*Schrems II*": Europe needs digital independence," press release, Berlin DPA, July 17, 2020, https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/pressemitteilungen/2020/20200717-PM-Nach_SchremsII_Digitale_Eigenstaendigkeit.pdf;
103. [translated] "Difficult times ahead for international transfer of data," Hamburg's Data Protection Authority.
104. Romain Dillet, "France's Health Data Hub to move to European cloud infrastructure to avoid EU-US data transfers," *Tech Crunch,* October 12, 2020, https://techcrunch.com/2020/10/12/frances-health-data-hub-to-move-to-european-cloud-infrastructure-to-avoid-eu-us-data-transfers.
105. Laura Kayali and Florian Eder, "Thierry Breton 'understands' Trump on TikTok, wants data stored in Europe," *Politico,* September 1, 2020, https://www.politico.eu/article/breton-wants-tiktok-data-to-stay-in-europe.
106. Natasha Lomas, "Thierry Breton 'understands' Trump on TikTok, wants data stored in Europe," *Tech Crunch,* July 17, 2020, https://techcrunch.com/2020/07/17/clouds-gather-over-us-cloud-services-after-cjeu-ruling/?guccounter=1.
107. "Rebooting the European Economy," Facebook, press release, September 23, 2020, https://about.fb.com/news/2020/09/rebooting-the-european-economy/.
108. Ibid.
109. Joshua New, "Why the United States Needs a National Artificial Intelligence Strategy and What It Should Look Like" (Center for Data Innovation, December 4, 2018), http://www2.datainnovation.org/2018-national-ai-strategy.pdf.
110. Bonefeld-Dahl, "Schrems II ruling puts European recovery at risk."
111. Organization for Economic Cooperation and Development (OECD), *Measuring Innovation: A New Perspective* (Paris: OECD, pages 84-85, 2010), https://www.oecd.org/sti/measuringinnovationanewperspective.htm.

112. Mike Robuck, "Report: Amazon and Microsoft reign supreme in European cloud market," *Fierce Telecom,* May 7, 2020, https://www.fiercetelecom.com/operators/report-amazon-and-microsoft-reign-supreme-european-cloud-market.

113. Such as Slack: "A note to our customers on international data transfers." Slack blog post, July 31, 2020, https://slack.com/blog/news/a-note-to-our-customers-on-international-data-transfers.

114. Josh New, Why the United States Needs a National Artificial Intelligence Strategy and What It Should Look Like (The Center for Data Innovation, December 4, 2018), http://www2.datainnovation.org/2018-national-ai-strategy.pdf.

115. Bhaskar Chakravorti, Ajay Bhalla, and Ravi Shankar Chaturvedi, "Which Countries Are Leading the Data Economy?" *Harvard Business Review,* January 24, 2019, https://hbr.org/2019/01/which-countries-are-leading-the-data-economy.

116. Nigel Cory, "Fostering an Enabling Policy and Regulatory Environment in APEC for Data-Utilizing Businesses" (ITIF contribution to Asia Pacific Economic Cooperation (APEC) report, July 2019), https://itif.org/publications/2019/07/22/fostering-enabling-policy-and-regulatory-environment-apec-data-utilizing.

117. "Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data," European Data Protection Board.