# Issue Brief: The Great Transatlantic Data Disruption

*The damage of data localization after Schrems II*

*October 7, 2021*


Authored by:

**Kristian Stout** (Director of Innovation Policy, International Center for Law & Economics)

**Michael Mandel** (Vice President and Chief Economist, Progressive Policy Institute)

**Mikołaj Barczentewicz** (Senior Lecturer in Law at the University of Surrey, Fellow at Stanford Law School, and Research Associate at the University of Oxford)

## I. Executive Summary

Data is, logically enough, one of the pillars supporting the modern digital economy. It is, however, not terribly useful on its own. Only once it has been collected, analyzed, combined, and deployed in novel ways does data obtain its highest utility. This is to say, a large part of the value of data is its ability to flow throughout the global connected economy in real time, permitting individuals and firms to develop novel insights that would not otherwise be possible, and to operate at a higher level of efficiency and safety.

Although the global transmission of data is critical to every industry and scientific endeavor, those data flows increasingly run into barriers of various sorts when they seek to cross national borders. Most typically, these barriers take the form of data-localization requirements.

Data localization is an umbrella term that refers to a variety of requirements that nations set to govern how data is created, stored, and transmitted within their jurisdiction. The aim of data-localization policies is to restrict the flow of data across a nation's borders, often justified on grounds of protecting national security interests and/or sensitive information about citizens.

Data-localization requirements have in recent years been at the center of a series of legal disputes between the United States and the European Union (EU) that potentially threaten the future of transatlantic data flows. In October 2015, in a decision known as *Schrems I*, the Court of Justice of the European Union (CJEU) overturned the International Safe Harbor Privacy Principles, which had for the prior 15 years governed customer data transmitted between the United States and the EU. The principles were replaced in February 2016 by a new framework agreement known as the EU–US Privacy Shield, until the CJEU declared that, too, to be invalid in a July 2020 decision known as *Schrems II*.[1] (Both complaints were brought by Austrian privacy advocate Max Schrems).

The current threatened disruption to transatlantic data flows highlights the size of the problem caused by data-localization policies.[2] According to one estimate, transatlantic trade generates upward of $5.6 trillion in annual commercial sales, of which at least $333 billion is related to digitally enabled services.[3] Some estimates suggest that moderate increases in data-localization requirements would result in a €116 billion reduction in exports from the EU.[4]

---

[1] Case C-311/18, Data Protection Comm'r v. Facebook Ireland Ltd. & Maximillian Schrems, ECLI:EU:C:2019:1145 (CJ, Jul. 16, 2020), *available at* http://curia.europa.eu/juris/liste.jsf?num=C-311/18 [hereinafter "Shrems II"].

[2] *See* discussion in Part IV, *infra* n. 99 - 124 and accompanying text.

[3] *See* DANIEL S. HAMILTON & JOSEPH P. QUINLAN, THE TRANSATLANTIC ECONOMY 2020: ANNUAL SURVEY OF JOBS, TRADE AND INVESTMENT BETWEEN THE UNITED STATES AND EUROPE 13, 31 (2020), *available at* https://www.uschamber.com/sites/default/files/te2020_report_final.pdf.

[4] *See infra*, n. 51 - 57 and accompanying text.

One difficulty in precisely quantifying the full impact of strict data-localization practices is that the list of industries engaged in digitally enabled trade extends well beyond those that explicitly trade in data. This is because "it is increasingly difficult to separate services and goods with the rise of the 'Internet of Things' and the greater bundling of goods and services. At the same time, goods are being substituted by services ... further shifting the regulatory boundaries between what is treated as goods and services."[5] Thus, there is reason to believe that the true value of digitally enabled trade to the global economy is underestimated.

Moreover, as we discuss *infra*, there is reason to suspect that data flows and digitally enabled trade have contributed a good deal of unmeasured economic activity that partially offsets the lower-than-expected measured productivity growth seen in the both the European Union and the United States over the last decade and a half.[6] In particular, heavy investment in research and development by firms globally has facilitated substituting the relatively more efficient work of employees at firms for unpaid labor by individuals.[7] And global data flows have facilitated the creation of larger, more efficient worldwide networks that optimize time use by firms and individuals, and the development of resilient networks that can withstand shocks to the system like the COVID-19 pandemic.[8]

In the *Schrems II* decision, the court found that provisions of U.S. national security law and the surveillance powers it grants to intelligence agencies do not protect the data of EU citizens sufficiently to justify deeming U.S. laws as providing adequate protection (known as an "adequacy" decision).[9] In addition to a national "adequacy" decision, the EU General Data Protection Regulation (GDPR) also permits firms that wish to transfer data to the United States to rely on "standard contractual clauses" (SCC) that guarantee protection of citizen data. However, a prominent view in European policy circles—voiced, for example, by the European Parliament—is that, after *Schrems II*, no SCC can provide a lawful basis for data transfers to the United States.[10]

Shortly after the *Schrems II* decision, the Irish Data Protection Commission (IDPC) issued a preliminary draft decision against Facebook that proposed to invalidate the company's SCCs, largely

---

5 Javier López González & Janos Ferencz, *Digital Trade and Market Openness* at 34 (OECD Trade Policy Papers No. 217, 2018), *available at* http://dx.doi.org/10.1787/1bd89c9a-en.

6 *See, e.g.*, Shawn Sprague, *The U.S. Productivity Slowdown: An Economy-wide and Industry-level Analysis*, MONTHLY LABOR REV. (Apr. 2021), https://www.bls.gov/opub/mlr/2021/article/the-us-productivity-slowdown-the-economy-wide-and-industry-level-analysis.htm ("This high-growth period came to an end during the mid-2000s, when U.S. labor productivity growth rates began to stumble, and in 2006 receded below the long-term average trend line for the first time in a decade. And, notwithstanding 2 years of high growth in 2009 and 2010 following the Great Recession, productivity growth rates have remained stubbornly low in subsequent years.").

7 See, *infra*, notes 80 - 88, and accompanying text.

8 See, *infra*, notes 89 - 94, and accompanying text.

9 Schrems II, *supra* note 1, at ¶¶ 184-202.

10 Eur. Parliament Resolution of 20 May 2021 on the Ruling of the CJEU of 16 July 2020 - Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems ('Schrems II'), Case C-311/18 (2021), *available at* https://www.europarl.europa.eu/doceo/document/TA-9-2021-0256_EN.html.

on the same grounds that the CJEU used when invalidating the Privacy Shield.[11] This matter is still pending, but a decision from the IDPC is expected imminently, with the worst-case result being an order that Facebook suspend all transatlantic data transfers that depend upon SCCs. Narrowly speaking, the IDPC decision only immediately affects Facebook. However, if the draft decision is finalized, the SCCs of every other firm that transfers data across the Atlantic may be subject to invalidation under the same legal reasoning.[12]

Although this increasingly restrictive legal environment for data flows has been building for years, the recent problems are increasingly breaking into public view, as national DPAs grapple with the language of the GDPR and the *Schrems* decisions. The Hamburg DPA recently issued a public warning that the use of the popular video-conference application Zoom violates GDPR.[13] The Portuguese DPA issued a resolution forbidding its National Institute of Statistics from transferring census data to the U.S.-based Cloudflare, because the SCCs in the contract between the two entities were deemed insufficient in light of *Schrems II*.[14]

The European Data Protection Supervisor has initiated a program to "monitor compliance of European institutions, bodies, offices and agencies (EUIs) with the 'Schrems II' Judgement."[15] As part of this program, it opened an investigation into Amazon and Microsoft in order to determine if Microsoft's Office 365 and the cloud-hosting services offered by both Amazon and Microsoft are compatible with GDPR post-*Schrems II.*[16] Max Schrems, who brought the original complaint against Facebook, has through his privacy-activist group submitted at least 100 complaints as of August 2020 alone, which will undoubtedly result in scores of cases across multiple industries.[17]

[11] Sam Schechner & Emily Glazer, *Ireland to Order Facebook to Stop Sending User Data to U.S.*, WALL ST. J. (Sep. 9, 2020), https://www.wsj.com/articles/ireland-to-order-facebook-to-stop-sending-user-data-to-u-s-11599671980.

[12] According to IDPC Commissioner Helen Dixon, "[i]n very general terms, removing from that specific (Facebook) case, there would be massive disruptions for individual companies and organisations." Conor Humphries, *EU-U.S. Data Flows Could Face 'Massive Disruption' - Irish Regulator*, REUTERS, Feb. 24, 2021, https://www.reuters.com/article/us-facebook-privacy-dixon-interview/eu-u-s-data-flows-could-face-massive-disruption-irish-regulator-idUSKBN2AP009

[13] Natasha Lomas, *Stop Using Zoom, Hamburg's DPA Warns State Government*, TECHCRUNCH (Aug. 17, 2021), https://techcrunch.com/2021/08/17/stop-using-zoom-hamburgs-dpa-warns-state-government/.

[14] Liisa M. Thomas & Snehal Desai, *Portugal Puts Halt On Data Transfers Between INE And Cloudflare*, MONDAQ (May 12, 2021), https://www.mondaq.com/data-protection/1067638/portugal-puts-halt-on-data-transfers-between-ine-and-cloudflare.

[15] Press Release, Eur. Data Protection Supervisor, *Strategy for EU Institutions to Comply with "Schrems II" Ruling, European Data Protection Supervisor* (Oct. 29, 2020), https://edps.europa.eu/press-publications/press-news/press-releases/2020/strategy-eu-institutions-comply-schrems-ii-ruling_en.

[16] Press Release, Eur. Data Protection Supervisor, *The EDPS Opens Two Investigations Following the "Schrems II" Judgement* (May 27, 2021), https://edps.europa.eu/press-publications/press-news/press-releases/2021/edps-opens-two-investigations-following-schrems_en.

[17] *101 Complaints on EU-US Transfers Filed*, NOYB (Aug. 17, 2020), https://noyb.eu/en/101-complaints-eu-us-transfers-filed; *see also* Natasha Lomas, *EU Websites' Use of Google Analytics and Facebook Connect Targeted by Post-Schrems II Privacy Complaints*, TECHCRUNCH (Aug. 18, 2020), https://techcrunch.com/2020/08/18/eu-websites-use-of-google-analytics-and-facebook-connect-targeted-by-post-schrems-ii-privacy-complaints/.

The United States and European Union are currently negotiating a replacement for the Privacy Shield agreement that would allow data flows between the two economic regions to continue.[18] But EU representatives have warned that, in order to comply with GDPR, there will likely be nontrivial legislative changes necessary in the United States, particularly in the sensitive area of national-security monitoring.[19] Federal legislation addressing a wide range of domestic and cross-border privacy issues and trade abuses—such as foreign-based ransomware and cyber-theft of intellectual property—is desirable and important. Clearly, some regulation is necessary for public-interest and crime-control reasons. However, such legislation, by itself will, not deal with *Schrems II*-related issues. In effect, the European Union and the Unites States are being forced to rethink the boundaries of national law in the context of a digital global economy.

This issue brief first reviews the relevant literature on the importance of digital trade, as well as the difficulties in adequately measuring it. One implication of these measurement difficulties is that the impact of disruptions to data flows and digital trade are likely to be far greater than even the large effects discovered through traditional measurement suggest.

We then discuss the importance of network resilience, and the productivity or quasi-productivity gains that digital networks and data flows provide. After a review of the current policy and legal challenges facing digital trade and data flows, we finally urge the U.S. and EU negotiating parties to consider longer-term trade and policy changes that take seriously the role of data flows in the world economy.

## II. The importance of digital trade and the effects of data-localization policies

Over the last decade, policies intended to restrict trade in digital services have become increasingly popular.[20] Between 2017 and 2021 alone, the number of countries imposing restrictions on cross-border data flows nearly doubled.[21] To some extent, this has stemmed from policymakers misunderstanding the highly diffuse nature of data and how it is deployed by industries beyond obviously digital services. At the same time, it cannot be denied that restrictions on digital trade also

---

[18] Ryan Chiavetta, *Hoff: EU, US 'Not At The Beginning' of Privacy Shield Negotiations*, IAPP (July 1, 2021), https://iapp.org/news/a/hoff-eu-us-not-at-the-beginning-of-privacy-shield-negotiations/.

[19] Catherine Stupp, *Officials Warn Privacy Shield Replacement May Be a Long Way Off*, WALL ST. J. (Sep. 8, 2020), https://www.wsj.com/articles/officials-warn-privacy-shield-replacement-may-be-a-long-way-off-11599557400.

[20] *See* OECD SERVICES TRADE RESTRICTIVENESS INDEX: POLICY TRENDS UP TO 2021, at 11 (2021); *See also* Daniela Chikova & Erik Peterson, *The economic costs of restricting the cross-border flow of data*, at 23 ECIPE (2021), *available at* https://www.kearney.com/de/web/global-business-policy-council/article/?/a/the-economic-costs-of-restricting-the-cross-border-flow-of-data ("Over the past 20 years, the number of data protection regulations around the world has increased. Based on our analysis of sources such as the UNCTAD, DLA Piper, and local regulators, more than 220 data protection regulations were enacted across the globe in the past 20 years and are still in force today.").

[21] *See, e.g.*, Nigel Cory & Luke Dascoli, How Barriers to Cross-Border Data Flows Are Spreading Globally, What They Cost, and How to Address Them, at 3, INFORMATION TECH. & INNOVATION FOUND. (Jul. 2021), *available at* https://itif.org/sites/default/files/2021-data-localization.pdf.

offer nations an opportunity, intentional or otherwise, to exert leverage over trading partners, often by implementing some form of data-localization requirement.

## A. The growth of data-localization requirements

Data localization is an umbrella term that refers to various measures governing how data may be created, stored, and transmitted within and between jurisdictions. The aim of data-localization policies is to restrict the flow of data across a nation's borders, often justified on grounds of protecting national security interests and/or sensitive information about citizens.[22]

Localization policies take various forms. Cory & Dascoli compiled a useful list of localization policies from around the world, including an overview of the five most typical policies employed:

> **Local data mirroring**. Firms must first store a copy of data locally before transferring a copy out of the country. This may also involve keeping the most updated version of the data locally.
>
> **Explicit local data storage**. Firms must physically locate data in the country where it originates. Some cases allow foreign processing of data (after which data must be stored locally).
>
> **De facto local storage and processing**. Firms store data locally as stringent data transfer requirements (such as getting pre-approval for transfers and explicit consent) and legal uncertainty about data transfers, which, when combined with hefty fines and arbitrary enforcement, create unacceptable risk for firms.
>
> **Explicit local data storage and processing**. Countries prohibit transfer to other countries.
>
> **Explicit local—and discriminatory—data processing, routing, and storage**. Some countries use discriminatory licensing, certification, and other regulatory restrictions to require local data storage and exclude foreign firms entirely from managing and processing local data.[23]

This taxonomy of data-localization policies is broadly similar to the types of restrictions tracked by the OECD as part of compiling its "services trade restrictiveness index" (STRI):

> Cross-border transfer of personal data is possible when certain private sector safeguards are in place...

---

[22] *See, e.g.*, Telekommunikationsgesetz [HGB] [Commercial Code], § 89, *available at* https://germanlawarchive.iuscomp.org/?p=692 ( Mandating local storage in Germany by telecommunications firms of data related to phone numbers and phone calls for a fixed period of time); *see also Russian Government Imposes 2-Year Ban on Buying Foreign Data Storage Devices for State Needs*, SPUTNIK INT'L (Feb. 12, 2019), https://sputniknews.com/20191226/russian-govt-imposes-2-year-ban-on-buying-foreign-data-storage-devices-1077869453.html (In 2019, Russia imposed a ban on state entities from procuring data storage from foreign firms on security-concern grounds). For an exhaustive list of data-localization requirements around the world, along with their stated objectives, *see* Cory & Dascoli, *supra* note 21, at 3.

[23] Cory & Dascoli, *supra* note 21, at 4.

> Cross-border transfer of personal data is possible to countries with substantially similar privacy protection laws…
>
> Cross-border transfer is subject to approval on a case-by-case basis…
>
> Certain data must be stored locally [, and]
>
> Transfer of data is prohibited.[24]

If one referred to the "localization" of physical products such as avocados and automobiles, it would be obvious that the underlying subject was protectionist trade barriers. Policymakers might then have a good idea of the potential economic costs and benefits. "Localizing" a product like natural gas might even sound absurd if the country in question did not produce it.

### B. The digital economy is much larger than official measurements suggest

Yet, given the difficulty of measuring digital trade, it is perhaps no wonder that data-localization requirements have become increasingly popular as governments focus on non-economic rationales for their alleged necessity, such as privacy or the desire to exert control over what some consider a national asset. The estimates of digital trade that do exist are large. In 2019, by one estimate, the "digital economy" accounted for 9% of the overall U.S. economy, a share that translates to more than $1.8 trillion.[25] In the European Union, the estimated contribution of digital goods and services to GDP is a more modest (but nonetheless substantial) 7%.[26] Also of note is that two of the three fastest-growing areas of global research and development—software/artificial intelligence and biotechnology—are both data-driven, both tend to rely on cross-border data flows, and both are central to the digital economy.[27]

But references to the "digital economy" themselves conceal the multifaceted, crosscutting nature of this sector. Data and data flows are integral components at every stage of the value chain. Digital commerce accounts for an incredibly wide swath of commercial activities, from direct trade in the "data value chain" that includes data collection, aggregation, analysis, and sales/licensing; to relying

---

[24] These are the restrictiveness measures tracked by the OECD under "Restrictions on foreign entry" that are relevant to this paper. *See Services Trade Restrictiveness Index Regulatory Database*, OECD, https://qdd.oecd.org/subject.aspx?Subject=063bee63-475f-427c-8b50-c19bffa7392d (last visited Sep. 29, 2021).

[25] Jessica R. Nicholson, *New Digital Economy Estimates*, at 2, BUREAU OF ECONOMIC ANALYSIS (2020), *available at* https://www.bea.gov/system/files/2020-08/New-Digital-Economy-Estimates-August-2020.pdf.

[26] Robert Anderton et al., *The Digital Economy and the Euro Area*, ECB ECONOMIC BULLETIN (Aug. 2020), https://www.ecb.europa.eu/pub/economic-bulletin/articles/2021/html/ecb.ebart202008_03~da0f5f792a.en.html.

[27] EUR. COMM'N, THE 2020 EU INDUSTRIAL R&D INVESTMENT SCORECARD 16 (2020), *available at* https://op.europa.eu/en/publication-detail/-/publication/73e624aa-406c-11eb-b27b-01aa75ed71a1/language-en.

on data to refine existing production and distribution methods; to the sale of "data-enabled" products like connected cars.[28]

There is also an important distinction between "digital services" and "digitally enabled services."[29] In 2016, the U.S. Bureau of Economic Analysis (BEA) began to track a more expansive set of data regarding services it refers to as Information and Communications Technology (ICT):

> ICT services are those services that are used to facilitate information processing and communication. ICT services… include three categories of services from BEA's published statistics on international trade in services: telecommunications services, computer services, and charges for the use of intellectual property associated with computer software… ICT-enabled services are "services with outputs delivered remotely over ICT networks."[30]

Further, the BEA also began to include services that are *potentially* digitally enabled:

> For many types of services, the actual mode of delivery is unknown. Potentially ICT-enabled services include services types that can predominantly be delivered remotely over ICT networks without identifying the services that are delivered over ICT networks.[31]

As of 2020, the BEA included yet more categories of activity in its digital trade statistics, including additional infrastructure goods, expanded categories of ecommerce activity, support and consulting services that support the digital economy, and cloud services.[32]

There is good reason for the agency to be expansive here. Even where trade in goods and services is not explicitly around a digital offering, digital services and data flows can be used to significantly augment the value of other trade.[33] The BEA notes that, in 2014, U.S. digital trade exports were $68.4 billion and imports were $37.8 billion, while exports for digitally enabled trade were $385.1 billion and imports were $230.9 billion.[34] As of 2019, "digitally-enabled services accounted for 59%

---

[28] For a further discussion, *see, e.g.*, HILARY MINE & CECILIA BONEFELD-DAHL, THE VALUE OF CROSS-BORDER DATA FLOWS TO EUROPE: RISKS AND OPPORTUNITIES 12-16 (2021), *available at* https://www.digitaleurope.org/wp/wp-content/uploads/2021/06/Frontier-DIGITALEUROPE_The-value-of-cross-border-data-flows-to-Europe_Risks-and-opportunities.pdf.

[29] *See* Daniel S. Hamilton & Joseph Quinlan, T*he Importance of Digital Services to the U.S. and European Economies*, WILSON CTR. (Apr. 8, 2021), https://www.wilsoncenter.org/article/importance-digital-services-us-and-european-economies.

[30] Alexis N. Grimm, *Trends in U.S. Trade in Information and Communications Technology (ICT) Services and in ICT-Enabled Services*, at 1-2, BUREAU OF ECONOMIC ANALYSIS (2016), *available at* https://apps.bea.gov/scb/pdf/2016/05%20may/0516_trends_%20in_us_trade_in_ict_serivces2.pdf.

[31] *Id.* at 2.

[32] *See* Nicholson, *supra* note 25, at 6-10.

[33] Note that, for simplicity's sake, we will refer to "digital trade" and "digitally enabled trade" to refer to the more fine-grained distinctions that the BEA highlights.

[34] *See* Nicholson, *supra* note 25, at 2.

of all U.S. services exports, 50% of all services imports, and 76% of the U.S. global surplus in trade in services."[35]

By one estimate, digitally enabled services account for up to 45% of EU GDP.[36] Limiting the analysis to small and medium-sized enterprises (SMEs) engaged in manufacturing, their digitally enabled exports were valued at €280 billion.[37] EU leaders have explicitly acknowledged that the digital economy is central to the region's future. In its "digital targets for 2030," the European Commission set ambitious goals for the EU zone, including having three-quarters of EU companies relying on AI and cloud services, doubling the number of tech unicorns, and making sure that 90% of SMEs have at least a basic level of digital intensity.[38]

Further, digitization is undoubtedly pervasive throughout the EU:

> In the European Union, for example, nearly 60% of enterprises providing accommodation services sell online, and more than half of these sell across borders (in this case defined as selling to other EU countries and the rest of the world)…On average, about one third to one fifth of the digital sales of manufacturing firms are cross-border.[39]

It would not be overstated to claim that technology and data flows are among the prime drivers of the global economy.[40] Many services "are now being 'de-localized' and 'globalized' to an extent and on a scale that may surpass even most globe-spanning multinational goods manufacturers[,]"[41] with all of that activity directly dependent on healthy data flows. Again, digitally enabled activity is not limited solely to trade in digital goods. Rather, it encompasses a flow of heterogeneous goods and services "underpinned by a range of measures that are horizontal to all transactions."[42]

---

[35] Hamilton & Quinlan, *supra* note 29, at Table 1.

[36] MINE & BONEFELD-DAHL, *supra* note 28, at 20.

[37] *Id.* at 35.

[38] Eur. Comm'n, *Europe's Digital Decade: Digital Targets for 2030*, at 10, COM (2021) 118 final (September 3, 2021), *available at* https://eur-lex.europa.eu/resource.html?uri=cellar:12e835e2-81af-11eb-9ac9-01aa75ed71a1.0001.02/DOC_1&format=PDF.

[39] González & Ferencz, *supra* note 5, at 19.

[40] WORLD TRADE ORGANIZATION, WORLD TRADE REPORT 2019, THE FUTURE OF SERVICES TRADE 14 (2019), *available at* https://www.wto.org/english/res_e/booksp_e/00_wtr19_e.pdf ("The main driver of [increased global trade] is technological change. Thanks to digitalization, the internet and low-cost telecommunications, many services sectors that were once non-tradable – because they had to be delivered face-to-face in a fixed location – have become highly tradable – because they can now be delivered remotely over long distances.").

[41] *Id.* at 14-15

[42] González & Ferencz, *supra* note 5, at 6.

### C. Estimating the effects of data localization on digital trade

But even as digitally enabled services have grown increasingly pervasive, the problem of how to adequately capture this economic activity in official statistics has grown, as well.[43] For example, the OECD notes that the "rapid increase in the production and availability of data has resulted in firms operating business models that 'would not exist without access to large amounts of data and advanced data analytics'."[44] The World Trade Organization (WTO) has observed that "[d]igital technologies are blurring the distinction between trade in goods and services activities, while increasing the importance of data flows and intellectual property."[45] This results in a situation where "almost all businesses use data 'to improve products and processes to enhance productivity, improve performance, and increase profitability'."[46] Thus, it becomes increasingly difficult to extract the exact "digital" value-added component of digitally enabled services across the economy, which can lead to skewed measurements of other metrics, like productivity growth or firm valuations.[47]

Complicating matters further, unlike traditional, discretely measured goods like cars, TVs, or toasters, data tend to be highly idiosyncratic. Particularly in situations where data or data-enabled services are zero-priced—that is, offered to consumers at no cost—deriving appropriate valuations is difficult.[48] While there are efforts to standardize how to perform such valuations, there is no broadly available solution.[49]

As data and data-enabled services proliferate, among their largest impacts is on the efficiency of simple daily activities. At the micro level, this can mean smartphone-based apps saving an individual consumer seconds or minutes each day as she undertakes mundane tasks. For firms, it can take the form of software that enables employees to do more with less, or in less time. In either case, the time savings enjoyed by either consumers or firms is not directly captured by aggregate measures like GDP.

---

[43] *See id.* at 18 ("Although efforts are underway to better capture digital trade in official trade statistics, it will take some time before robust measures are identified. At the same time, measuring the nature and spread of digitalisation is also difficult. Here too, efforts are underway… but there is no single measure that captures all facets of this phenomenon. This implies that, until better measures are available, analysis of digital trade has to proceed with caution and using existing statistics to shed light on particular aspects of trade in the digital era.").

[44] Louise Hatem, Daniel Ker, & John Mitchell, *A Roadmap Toward A Common Framework For Measuring The Digital Economy, Report for the G20 Digital Economy Task Force*, at 52 (OECD 2020), *available at* https://www.oecd.org/sti/roadmap-toward-a-common-framework-for-measuring-the-digital-economy.pdf.

[45] Trade Organization, *supra* note 40, at 101.

[46] *Id.*

[47] *Id.* at 52-53.

[48] *See, e.g.*, Hatem, Ker, and Mitchell, *supra* note 44, at 52 ("Indeed, the characteristics of data differentiate it from other inputs in production: this includes the way data comes into existence, their varied use in the production process and the unknown value that can be derived therefrom. These unknown variables are due to both the uniqueness of each dataset and the varieties of business models using it.").

[49] *See id.* at 61 (Discussing the OECD's effort to develop "G20 Toolkit for Measuring the Digital Economy" in an effort to overcome the measurement problems faced by researchers studying the digital economy).

Of course, as data-enabled innovations become more established, the time they save inevitably will be reflected in greater economic productivity, to at least some extent. But as these innovations are bundled into other products or are otherwise zero-priced, parsing exactly how much the data and data flows contribute to that enhanced productivity will remain difficult to measure. Thus, "an unknown but potentially large proportion of cross-border data flows do not show up in the export and import statistics because they do not leave a monetary footprint."[50]

The measurement problem associated with digitally enabled goods also makes precisely estimating the impact of data-localization policies challenging. Nonetheless, some research suggests that data localization can have dramatic effects.

A June 2021 report by Mine & Bonefeld-Dahl estimated the value of cross-border data flows in the European Union and modeled the potential impact of changes to current EU data-localization policies.[51] Their models used a more expansive notion of "data-reliant" industries, similar to the BEA's "ICT-enabled" firms noted above, insofar as their analysis focused on sectors of the economy that are heavily reliant on cross-border data flows.[52] The authors modeled a baseline restrictiveness derived, in part, from the OECD's STRI, and measured changes to that baseline as increases or decreases in the number of restrictions, as tracked by the OECD.[53] They then modeled two different scenarios: a "challenge" scenario, in which data-flows restrictions are increased, and a "growth" scenario, in which restrictions are removed.[54]

Overall, the authors found annual impacts from a moderate increase in restrictiveness results in €116 billion of reduced exports, or 4% of total EU exports.[55] By contrast, in their moderate "growth" scenario, the authors found that liberalizing data-flow restrictions would result in a €62 billion increase in exports, equivalent to 2.15% of current EU exports.[56] Over a decade, this analysis "points to losses of €1.3 trillion in the challenge scenario, and gains of €720 billion in the growth scenario."[57]

In another attempt to estimate the impact of changes to the restrictiveness of current data-localization policies around the world, Chikova & Peterson found that, in the case of an effective "full ban" on data flows between the United States and the European Union, there would be a 31%

---

[50] Michael Mandel, *Moving Beyond the Balance-sheet Economy*, at 21, *in* POLICY CHOICES FOR A DIGITAL AGE, TAKING A WHOLE ECONOMY, WHOLE SOCIETY APPROACH (discussion paper) (2017), *available at* https://ec.europa.eu/futurium/en/system/files/ged/netfuturesclosing_4ir_report_web_final.pdf.

[51] *See* MINE & BONEFELD-DAHL, *supra* note 28.

[52] *Id.* at 19.

[53] *Id.* at 22.

[54] *Id.*

[55] *Id.* at 26.

[56] *Id.* at 29.

[57] *Id.* at 32. The authors also modeled an "extreme" challenge scenario in which maximal restrictions were applied. In that scenario, they found a 9.6% reduction in total exports worth €270 billion per year. Id. at 36. Although unlikely to be a scenario in either the EU or the United States, the extreme case does underscore the importance of data flows to international trade.

decline in digital services imports.[58] This would be a "a substantial impact given digital services add up to 39 percent of the total imports from the United States."[59] The authors, moreover, note that other sectors would likely be affected to the extent that they rely on data transfers,[60] which, as we note above, comprises a large and growing share of the economy. Such a scenario would result in a 2.4% decline in EU GDP, or about €327 billion annually.[61] Another attempt to model the value of data flows suggested that, by 2014, "cross-border data flows may have raised world GDP by roughly $2.8 trillion. … This surpasses the $2.7 trillion impact of the global goods trade."[62]

In a third study, econometric modeling indicated that:

> [A] one-unit increase in a country's [data restrictiveness index] is associated with a 1.5 percent increase in the prices of goods and services that downstream industries produce (in aggregate, over five years). This result means that as data becomes more heavily restricted, the remaining output among industries becomes more expensive to consumers than would otherwise be expected in a scenario wherein there exists free flows of data and data-driven goods and services. [63]

These results are intuitive. After all, forced data localization effectively constitutes a mandate to reduce the benefits that comparative advantage generally provides. For example, requiring firms to use only the cloud providers that operate within their own jurisdictions potentially forces them to rely on less efficient providers.[64] Half of all EU SMEs currently use externally hosted software as a service.[65] Some significant share of those firms will be directly affected by data-localization policies.[66]

Indeed, SMEs are one of the segments most vulnerable to disruptions caused by data-localization policies. Roughly 30% of EU and U.S. SMEs export goods and services abroad.[67] According to one estimate, among SME exporters, 24% of EU firms and 70% of U.S. firms are in "data-intensive digital service sectors."[68] As noted above, digitally enabled goods and services are growing to

---

[58] Chikova & Peterson, *supra* note 20, at 30.

[59] *Id.*

[60] *Id.*

[61] *Id.* at 31.

[62] JAMES MANYIKA ET AL., DIGITAL GLOBALIZATION: THE NEW ERA OF GLOBAL FLOWS 77 (2016), *available at* https://www.mckinsey.com/~/media/mckinsey/business%20functions/mckinsey%20digital/our%20insights/digital%20globalization%20the%20new%20era%20of%20global%20flows/mgi-digital-globalization-full-report.pdf.

[63] Cory & Dascoli, *supra* note 21, at 15.

[64] For a discussion of this sort of outcome, *see Quantifying the Cost of Forced Localization*, LEVIATHAN SECURITY GROUP (2015), *available at* https://static1.squarespace.com/static/556340ece4b0869396f21099/t/559dad76e4b0899d97726a8b/1436396918881/Quantifying+the+Cost+of+Forced+Localization.pdf.

[65] Chikova & Peterson, *supra* note 20, at 21.

[66] For instance, about 12% of EU SMEs currently host data outside of the EU. *Id.* at 18.

[67] *Id.* Note that 40% of EU SMEs "trade abroad" and "eight in ten" of those firms export, while 33% of U.S. SMEs export abroad.

[68] *Id.*

encompass far more than explicitly designated "data-intensive" services. Thus, the scope of SMEs affected by cross-border data restrictions is likely much greater.

### *1. The large indirect impacts of data-localization requirements*

There are important indirect impacts of data localization, as well. It is exceedingly expensive to develop advanced software, with costs that include quality control, user support, and post-release bug fixes and security maintenance. All other things being equal, the broader the market, the higher the level of optimal investment. Data localization has the effect of "sharding" global markets in ways that increase costs and reduce investment, a natural consequence of reducing the size of applicable markets.

The effects of data-localization requirements are disruptive to far more than just firms' ability to export or import. Transnational data flows are of paramount importance to firms and consumers in both the United States and the European Union that operate in an increasingly interconnected way.[69] Firms rely on market research that crosses borders, to assist in everything from the selection of which mix of products to manufacture, to enabling more tailored fits for particular customer segments.[70] Similarly, operational data from different business units or points in an enterprise are aggregated and analyzed in order to optimize business performance and customer service.[71]

Pieces of data on one's screen or in one's server often aren't labeled with their point of origin, or even the path they took to arrive there. This is especially true in a world increasingly reliant on cloud computing, whose entire premise is that distance is irrelevant to the user. Indeed, localization requirements ultimately may significantly affect the cloud infrastructure on which modern digital services are built. The radical approach to localization favored by some EU policymakers would require foreign service providers not only to store clients' data locally, but also to eschew any technical capacity to access that data from abroad. While this might be achieved by pure data-hosting services, many of the cloud services crucial to the modern Internet are not pure hosting services. It may be significantly more cumbersome, if not prohibitively costly, for a U.S. firm that develops some online service (e.g., converting speech to text, or detecting potential hacking attacks by analyzing network traffic logs) to offer an EU-version of that service while ensuring that it does not have even a theoretical technical capacity to access EU data from the United States.

Even assuming that the technical challenges of data localization can be overcome efficiently, the costs to adjust such services in ways that would make them compliant may be so great as to render these services inaccessible to EU companies, especially those that are startups or SMEs. Expecting that, for every valuable U.S.-produced service, there will be an equally good and quickly developed EU alternative is probably unrealistic. Moreover, major U.S. cloud providers offer entire ecosystems

---

[69] WORLD TRADE REPORT 2019, *supra* note 40, at 104-105 ("[D]igital era, services are part of a business ecosystem in which collaboration with customers, partners and contractors is the key to innovation and productivity.").

[70] MINE & BONEFELD-DAHL, *supra* note 28, at 12.

[71] *Id.* at 10-12.

of services and EU engineers already accept them as technological standards. A wholesale transition would force engineers to devote significant time to learning how to use non-U.S. services, all with no perceptible benefit for users. A more pragmatic approach to data protection would certainly allow for technical access to EU data by U.S. developers, albeit with some safeguards.

Health care and medical research offer stark examples of digitally enabled industries that would be disrupted by data-localization requirements, as medical research depends upon scientists' ability to share data across national boundaries.[72] During the COVID-19 pandemic, data flows supported the ability of firms like BioNTech and Pfizer to collaborate in analyzing the virus and developing a vaccine. It's widely recognized that data sharing is "necessary for studying and comparing genetic and epidemiological risk factors for the optimization of prevention or treatment."[73]

Reliance on cross-border data flows is also particularly important for just-in-time manufacturing, where intermediate goods suppliers tailor production flexibly to changes in the supply chain.[74] The rise of on-demand production depends on firms' ability to interact with customers across borders to gather detailed specifications.[75] Increasingly, Internet-of-Things (IoT) sensors are embedded in machines throughout the production and distribution process.[76] These sensors generate huge amounts of data and, depending on the context in which they are used, could contain the personal data of users. For example, tracking inventory or worker safety makes it necessary to keep logs containing identifiable information of workers as they interact with different devices with IoT capabilities. Firms that have offices in jurisdictions with restrictive data-localization policies are prevented from using their data flows, despite the positive effects such use could have on the health and safety of the workforce, or the efficiency of the production process.

## III. The hidden productivity gains from resilient networks

Over the last decade and a half, measured productivity growth in the advanced countries has been much slower than anticipated.[77] The growth rate of real GDP per hour in the G7 countries fell from

---

[72] Dara Hallinan et al., *International Transfers of Personal Data for Health Research Following Schrems II: A Problem in Need of a Solution*, 29 EUR. J. OF HUMAN GENETICS, 1502, 1502-03 (2021) *available at* https://www.nature.com/articles/s41431-021-00893-y.pdf.

[73] Heidi Beate Bentzen et al., *Remove Obstacles to Sharing Health Data with Researchers Outside of the European Union*, 27 NATURE MED. 1329 (2021), https://www.nature.com/articles/s41591-021-01460-0.

[74] *See, e.g.*, Kunpeng Zhu, Sanjay Joshi, Qing-Huo Wang & Jerry Fuh Ying Hsi, *Guest Editorial Special Section on Big Data Analytics in Intelligent Manufacturing*, 15 IEEE TRANSACTIONS ON INDUS. INFORMATICS 2382, 2382-85 (2019), *available at* https://ieeexplore.ieee.org/abstract/document/8681686.

[75] *See, e.g.*, Brian Rainey, *3 Benefits of On-Demand Manufacturing*, TOTALRETAIL (Jan. 28, 2021), https://www.mytotalretail.com/article/3-benefits-of-on-demand-manufacturing/.

[76] Muhammad Syafrudin, Ganjar Alfian, Norma Latif Fitriyani, & Jongtae Rhee, *Performance Analysis of IoT-Based Sensor, Big Data Processing, and Machine Learning Model for Real-Time Monitoring System in Automotive Manufacturing*, 18 SENSORS 2946 (2018), *available at* https://www.mdpi.com/1424-8220/18/9/2946.

[77] *See, e.g.*, Shawn Sprague, *supra* note 6 ("This high-growth period came to an end during the mid-2000s, when U.S. labor productivity growth rates began to stumble, and in 2006 receded below the long-term average trend line for the first time in a

an annual pace of 2.1% in the 1990-2000 business cycle, to 1.7% in the 2000-2007 business cycle to a stunningly slow 0.9% pace in the 2007-2019 business cycle, based on OECD figures. [78]

The phenomenon of slower-than-expected measured productivity growth in the European Union and the United States over the last decade and a half highlights the difficulty of quantifying digital trade. Firms have invested heavily in information-technology equipment and intangibles, such as software and R&D, in part to support increasingly globalized operations. Spending on research and development has grown faster than net sales in both the European Union and the United States, as multinationals have created and developed digital services that could be provided across borders.[79] Yet, government data shows flat or declining measured productivity growth.

## A. The productivity boost from data flows

It may be the case that some of the gains from digital trade escape the usual statistical monitors. Indeed, the OECD has recognized that, although "declining rates of productivity growth cannot be explained solely by the mismeasurement of output in the digital age," nonetheless "estimates of output and multifactor productivity could be flawed if the inputs used do not reflect the use of asset-like data products."[80] Thus, given the discussion in Section II, *supra*, it seems likely that at least some of the productivity mystery stems from the digitization of goods and services, making quantification in the official statistics more difficult.

In addition, thanks to technology improvements, productivity gains might be made along margins that are typically unmeasured. For example, social networks such as Facebook may generate large consumer surplus for users that are not picked up in measurements of GDP. One study estimated that "Facebook generates over $500 of consumer surplus per year for the average user in the US and Europe," far more than the amount of advertising revenue per user. [81]

Another relevant example of unmeasured consumer surplus became evident during the recent COVID-19 pandemic, as a growing number of consumers shifted from performing the uncompensated (and therefore unmeasured) labor of shopping in-person to relying on home-delivery services for everything from take-out food to groceries and other staples.[82] And investment by firms

---

decade. And, notwithstanding 2 years of high growth in 2009 and 2010 following the Great Recession, productivity growth rates have remained stubbornly low in subsequent years.").

[78] *Level of GDP Per Hour Worked, Constant Prices*, OECD, *available at* https://stats.oecd.org/Index.aspx?DataSetCode=PDB_LV# (last visited September 30, 2021).

[79] Over the last five years, global R&D investment has been up dramatically, particularly owing to the contributions of large tech firms. *See* THE 2020 EU INDUSTRIAL R&D INVESTMENT SCORECARD, *supra* note 27.

[80] Hatem, Ker, & Mitchell, *supra* note 44, at 52-53.

[81] Erik Brynjolfsson & Avinash Collis, *How Should We Measure the Digital Economy?* (Hutchins Ctr. Working Paper #57, Jan. 2020), *available at* https://www.brookings.edu/wp-content/uploads/2020/01/WP57-Collis_Brynjolfsson_updated.pdf.

[82] *See, e.g.*, Russel Redman, *Increased Use of Online Grocery Shopping 'Here to Stay'*, SUPERMARKET NEWS (Aug. 25, 2021), https://www.supermarketnews.com/online-retail/increased-use-online-grocery-shopping-here-stay.

like Amazon and Walmart in ever smarter, more efficient logistics operations, alongside large and growing product offerings, has enabled home delivery of an increasing amount of goods.

Over the last two decades Amazon has created almost 1 million jobs in the United States, many of them in logistics and shipping.[83] Fulfillment-center workers for Amazon and other ecommerce companies—through technological augmentation that supports more efficient picking, packing, and shipping—increasingly replace the shopping hours previously spent by consumers. Thus, there has been an increase in productivity by shifting the labor burden from relatively inefficient consumers to a smaller base of much more efficient workers at large retailers.

According to the American Time Use survey published by the Bureau of Labor Statistics, Americans spent 4.1 hours per week in 2003 shopping for consumer goods.[84] Over the entire adult population, that comes to approximately 49 billion hours of unpaid shopping time. In that same year, paid retail hours came to 25.5 billion hours, just over half of the unpaid total.[85] Between 2007 and 2018, per-capita time spent shopping for goods other than gasoline and groceries fell by 27%, even as per-capita real consumption of these goods rose by 25%.[86] The net result was a roughly 70% increase in the "productivity" of household shopping hours, most likely the result of the shift to ecommerce.[87] And all of this follows from the large R&D and information technology (IT) investment that firms have poured into logistics and that are inextricably tied—at least in part—to the ability to aggregate and process large data sets.

While household "shopping" is obviously an economic activity—insofar as actually acquiring and transporting goods over the "last mile" between the store and home is a necessary component of an economic transaction—it is one that would not be measured in GDP. Indeed, this information has always been difficult to capture, thanks to wide variance across consumers in both consumption and shopping patterns.[88] Yet, the proliferation of digitally enabled shopping and delivery services, and their ease of uptake during the pandemic, demonstrates that investment in digital infrastructure and data flows has produced productivity gains. Indeed, these gains may allow us to capture new metrics of economic activity.

---

[83] *Amazon.Com Announces Second Quarter Results*, AMAZON (July 29, 2021), https://s2.q4cdn.com/299287126/files/doc_financials/2021/q2/AMZN-Q2-2021-Earnings-Release.pdf.

[84] The Bureau of Labor Statistics began publishing the American Time Use Survey in 2003. *See American Time Use Survey*, Bureau of Labor Statistics (last visited Sep. 29. 2021), https://www.bls.gov/tus/.

[85] Michael Mandel, *Pre-pandemic Retail and Warehouse Productivity and Hours Growth, and Post-pandemic Implications,* PPI (draft, Aug. 28, 2020), *available at* https://www.progressivepolicy.org/wp-content/uploads/2021/10/Mandel-Pre-Pandemic-Retail-Productivity-draft-8-28-20.pdf.

[86] *Id.*

[87] *Id.*

[88] This is to say, there is variability across individuals in their willingness to invest time in shopping. Some derive pleasure from the act, while others invest as little time as possible in the activity. Not only is it difficult to gauge uniform shopping behaviors, thanks to a surfeit of available data on the process, but preferences are so varied as to make it nearly impossible to venture a reasonable guess regarding how much shopping time should count as a "cost." In a very real sense, however, there is indeed an economic cost to shopping that is not accounted for in measures of the economy.

Further, digitally enabled activity has improved along quality dimensions that directly translate into consumer welfare gains that are, again, difficult or impossible to measure, but that nonetheless exist. As more commercial activity moves online, the ability of networks to respond quickly and directly translates into time gains or losses for individual consumers.

At a basic level, the growing spate of networked applications, as well as optimization of those networks, reduce the time workers spend on their tasks. In a networked environment, "milliseconds matter":

> Research by Google in 2016 found that 40 percent of smartphone users would leave a site that takes longer than three seconds to load, and that time has likely shrunk in the last four years. A 2020 study by Deloitte Ireland "Milliseconds Make Millions" showed that a mere 0.1s change in mobile page load time can influence every step of the user journey: "With a 0.1s improvement in site speed, retail consumers spent almost 10% more, while lead generation and luxury consumers engaged more, with page views increasing by 7% and 8% respectively."[89]

Furthermore, large cloud and other infrastructure providers can analyze massive amounts of data flowing across national boundaries to engage in network optimization, which translates into slices of time saved per each user request. These slices of time add up to significant gains over the course of days, weeks, and months. The impact is felt across the entire networked landscape. And as more work has become remote in response to the pandemic, the productivity gains are likely to be even more dramatic.

One of the common techniques for network optimization is load balancing—"splitting the workloads and resources to numerous computer systems or servers so that no single server is overloaded."[90] By increasing the size and geographic spread of a load-balancing network, user requests are sped up by, among other things, linking the user's device to a physically closer regional node.[91] There is wide variation in the types of load-balancing possible, but in a properly optimized environment, user requests see significant improvements in latency.[92] In one analysis by Google, a simulated transatlantic request improved by more than 50% from 230 milliseconds to 123 milliseconds.[93]

---

[89] Conan French, Brad Carr, & Clay Lowery, *Data Localization: Costs, Tradeoffs, and Impacts Across the Economy*, at 6, INST. OF INT'L FIN. (2020), *available at* https://www.iif.com/Portals/0/Files/content/Innovation/12_22_2020_data_localization.pdf.

[90] Mohit Kumar & Bharat Bhushan, *A Methodological Comparison of the Most Efficient Load Balancing Algorithms in Cloud Computing*, at 1 (Proceedings of the International Conference on Innovative Computing & Communications, May 14, 2020), *available at* https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3598908.

[91] *See, e.g.*, David Wragg, *Unimog - Cloudflare's Edge Load Balancer*, THE CLOUDFLARE BLOG (Sep. 9, 2020), https://blog.cloudflare.com/unimog-cloudflares-edge-load-balancer/.

[92] *See, e.g.*, *Optimizing Application Latency with Load Balancing*, GOOGLE, https://cloud.google.com/load-balancing/docs/tutorials/optimize-app-latency (last visited Sep. 29, 2021) (comparing the performance of requests in a simulation with "no load balancing" to two different load balancing strategies).

[93] *Id.*

Not all of that latency will be perceived by the user, since modern browsers employ progressive loading techniques that make a page usable in far less than the total loading time.[94] To offer a sense of the scale of time savings that proper network optimization can yield, there were more than 5 billion visits in the month of June 2021 to just the top 10 ecommerce sites. Even slightly more optimized performance can add up to an enormous collective time savings and improved user experience.

And none of this even covers the additional benefits that stem from a having holistic view of networks across geographies, such as the ability to detect and prevent fraud and cybersecurity threats or enabling the fast settlement of transactions over payment-card networks.

### B. Data flows enable resilient networks

Global digital trade also contributes to greater network resilience. And it is in this regard that the COVID-19 pandemic best highlighted the gains that have been realized over the last decade.

Network resilience refers to a network's ability to absorb large and unanticipated shocks in the demand for data and the ability of the network to transport and deliver that data. Building resilient networks requires the ability to look across global data traffic and plan for sufficient transport, processing, and storage capacity. When a server is overloaded or a particular connection is at capacity, a resilient network can find alternative resources, perhaps located in other countries.

In the early days of the pandemic, a massive amount of economic activity was seamlessly relocated away from physical centers of operation and toward a distributed model in which the workforce was dispersed across the country and the world, all connected through digital networks that were supported by international data flows. This may not be "productivity" in the traditional sense of investment with the intent to realize increased first-order output or decreased costs. But there is no question that firms that have used digital technology to build resilient operations were, in fact, investing in their ability to operate under conditions of uncertainty. Pandemics, climate change, and political and military instability all create vulnerabilities that digital networks and data flows can help to overcome.

## IV. Policy challenges from data localization

Digital trade encompasses an ever-widening category of goods and services, which presents difficulties for lawmakers who continue to frame trade in pre-digitalization terms. As a 2018 OECD report notes:

> Regulatory challenges arise due to the blurring distinction between goods and services in digital trade, and the ensuing uncertainty as to the applicable trade rules. For instance, it is increasingly difficult to separate services and goods with the rise of the "Internet of Things" and the greater bundling of goods and services. At the same time, goods are

---

[94] *See, e.g.*, Dinesh Pandiyan, *Progressive Rendering – The Key to Faster Web*, MEDIUM (Nov. 10, 2019), https://medium.com/the-thinkmill/progressive-rendering-the-key-to-faster-web-ebfbbece41a4.

> being substituted by services – for instance, printed books and DVDs are being replaced by e-books and movie downloading or streaming services –further shifting the regulatory boundaries between what is treated as goods and services. As the GATT and GATS provide different rules and commitments for goods and services, the choice makes a difference. This matters as changes and uncertainties could result in regulatory fragmentation or create the risk of moving towards more restrictive regulation.[95]

Given this increased digitalization of goods and services, data policy needs to contemplate not just the final delivery of goods, but the entire value chain of production.[96] But while 2020 saw a reduction in the number of barriers to cross-border digital trade that were introduced—likely due to the pandemic—the OECD has found that more restrictions on cross-border digital trade were introduced from 2014 through 2019 than were measures to liberalize trade.[97] Moreover, "the global regulatory environment for digital trade in 2020 continues to be complex and diverse across countries."[98] In practical terms, this means that it remains challenging for firms and individuals to easily transfer data across geographies.

### C. *Schrems* and the coming transatlantic data disruption

One of the most important decisions in recent years affecting cross-border data flows was the CJEU's decision in *Schrems II*, in which the court invalidated the Privacy Shield framework—a transatlantic agreement about how to legally transfer data from the European Union to the United States.[99] In that case, the court found that provisions of U.S. national security law and the surveillance powers it grants intelligence agencies do not protect the data of EU citizens sufficiently to justify deeming U.S. laws as providing adequate protection (known as an "adequacy" decision).[100]

An adequacy decision—like the one just adopted for the United Kingdom—means that the level of data protection in the country covered by the decision is essentially equivalent to EU standards so as to allow EU firms to transfer data to that jurisdiction without conducting their own assessments.[101] In addition to relying on national "adequacy" decisions issued by the European Commission, firms seeking to export data from the European Union can rely on "standard contractual clauses" (SCC), or on the narrow exceptions from Article 49 of the General Data Protection Regulation (GDPR).

However, SCCs can only be used if the firms involved in the data transfer conduct due diligence of "the laws and practices" of the receiving country (e.g., the United States) and conclude that EU

---

[95] González & Ferencz, *supra* note 5**Error! Bookmark not defined.**, at 34.

[96] *Id.* at 6.

[97] OECD SERVICES TRADE RESTRICTIVENESS INDEX, *supra* note 20, at 12.

[98] *Id.* at 12.

[99] Schrems II, *supra* note 1**Error! Bookmark not defined.**.

[100] *Id.* at ¶¶ 184-202.

[101] *See* Press Release, Eur. Comm'n, *Data protection: Commission Adopts Adequacy Decisions for the UK* (June 28, 2021), https://ec.europa.eu/commission/presscorner/detail/en/ip_21_3183.

standards of data protection will be safeguarded.[102] Crucially, firms may be liable if the authorities conclude that this assessment of foreign laws and practices was erroneous. Under GDPR, those fines may be as high as 4% of annual global revenues.

Shortly after the *Schrems II* decision, the Irish Data Protection Commission ("IDPC") issued a preliminary draft decision against Facebook that proposed to invalidate the company's SCCs, largely on the same grounds that the CJEU used when invalidating the Privacy Shield.[103] This matter is still pending, but a decision from the IDPC is expected imminently, with the worst-case result being an order that Facebook suspend all transatlantic data transfers that depend upon SCCs. Narrowly speaking, the IDPC decision only immediately affects Facebook. However, if the order is finalized, the SCCs of every other firm that transfers data across the Atlantic may be subject to invalidation under the same legal reasoning.[104]

In principle, if SCCs cannot be used, firms could rely on other mechanisms from Article 46 of the GDPR, including "binding corporate rules" (BCRs), and on derogations from Article 49 of the GDPR. However, BCRs and other options from Article 46 may be even more onerous for firms than SCCs, whereas the Article 49 derogations are interpreted very restrictively by the European Data Protection Board (EDPB).[105]

The EDPB recommendations distinguish between two kinds of data transfers to a non-EU country without an adequacy decision, such as the United States: (1) fully end-to-end encrypted transfers (purely for data-hosting purposes) and (2) transfers where there is a possibility of data processing on the receiving end.[106] On EDPB's guidance, only the first kind of data transfer to the United States may be lawful if "Section 702 FISA applies in practice" to the particular transfer.[107] While this may allow U.S. cloud providers like Amazon AWS, Google Cloud, or Microsoft Azure to continue offering their enterprise cloud-hosting services in the EU, the kinds of consumer-facing services offered by most U.S. firms could be considered illegal. Thus, even if these services continue, they will be subject to significant constraints insofar as customers of the services will still be unable to perform the types of cross-border data transfers necessary for many businesses. The U.S. cloud industry would therefore likely be forced to restructure their EU operations to comply with data

---

[102] Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on Standard Contractual Clauses for the Transfer of Personal Data to Third Countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council, European Commission (2021), *available at* https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2021.199.01.0031.01.ENG&toc=OJ%3AL%3A2021%3A199%3ATOC.

[103] *See* Schechner & Glazer, *supra* note 11.

[104] According to IDPC Commissioner Helen Dixon, "In very general terms, removing from that specific (Facebook) case, there would be massive disruptions for individual companies and organisations." Conor Humphries, *EU-U.S. Data Flows Could Face 'Massive Disruption' - Irish Regulator*, REUTERS, Feb. 24, 2021, https://www.reuters.com/article/us-facebook-privacy-dixon-interview/eu-u-s-data-flows-could-face-massive-disruption-irish-regulator-idUSKBN2AP009

[105] EPDB, Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, Version 2.0 Adopted on 18 June 2021, at para. [24]-[26].

[106] EPDB, Recommendations, *supra* note 105105, at para. 84, 94.

[107] *Id.* at para. 49.

localization. It is, however, unclear whether even data localization would be sufficient to permit operation of U.S. services that process unencrypted data in the cloud.

The worry may be that U.S.-based cloud providers will retain technical means to access such data, even if it is stored with EU-based subsidiaries. It may therefore be possible for the U.S. government to compel access to such data. This concern is implicit in the EDPB's requirement that, in transfers of encrypted data for pure hosting purposes, encryption keys may not be transferred to a country like the United States.[108] In a decision upholding the legality of using Amazon AWS' cloud-hosting service, France's supreme administrative court noted as important that the encryption keys were not even held by Amazon's subsidiary, but instead by a trusted third party in France.[109]

### D. Data-localization requirements may violate trade agreements

The convergence of goods and services with data flows means that even facially neutral data-localization policies aimed at protecting national security or individual privacy may, in fact, serve as surreptitious trade barriers. What's more, it's hard to see how decisions like *Schrems II* and the actions of the IDPC don't potentially put the EU in violation of longstanding international trade agreements.

Article 4 of the Treaty of the European Union vests EU member states with discretion to manage their own national security apparatus—including intelligence gathering.[110] Article 8(2) of the European Convention on Human Rights allows for interference with the right of privacy for "national security, public safety or the economic wellbeing of the country."[111] And the GDPR explicitly exempts members for the purposes of intelligence gathering.[112] But under Article XVII of the General Agreement on Trade in Services (GATS), the EU is bound to afford treatment "no less favourable" to foreign services than it does to the services of member states.[113]

Thus, the EU is potentially prohibited under GATS from preventing U.S. companies from collecting and transmitting data because of the backdrop of U.S. national security laws, when it permits EU

[108] *Id.* at para. 90.

[109] Davinia Brennan, *French Court Considers Lawfulness of Using EU Subsidiary of US Cloud Service Provider Post-Schrems II*, IRELAND IP & TECHNOLOGY LAW BLOG (Apr. 16, 2021), https://www.irelandip.com/2021/04/articles/data-protection/french-court-ruling-considers-lawfulness-of-using-eu-subsidiary-of-us-cloud-service-provider-post-schrems-ii/.

[110] Consolidated Version Of The Treaty On European Union, Art. 4, *available at* https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:12012M004&from=EN.

[111] European Convention on Human Rights, Art. 8(2), Council of Europe, *available at* https://www.echr.coe.int/documents/convention_eng.pdf.

[112] Regulation (EU)2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, OJ L119/1, 04/05/2016 [hereinafter GDPR] at Article 2.

[113] General Agreement on Trade in Services, Apr. 15, 1994, Marrakesh Agreement Establishing the World Trade Organization, Article XVII (1994), *available at* https://www.wto.org/english/docs_e/legal_e/26-gats_01_e.htm#articleXVIII.

companies to collect data under the same or substantially similar circumstances.[114] Indeed, as it is applied to member states, the definition of what constitutes "national security" for the purposes of exceptions to privacy laws like GDPR is expansive.[115] Moreover, the rules vary across member states as to which types of parties can grant bulk data collection via signals analysis, ranging from judicial review, through boards of experts, to mere administrative review by directors:

> As a general rule, when targeting communications' content data, prior oversight is required in most Member States for both targeted surveillance and the use of selectors in the context of general surveillance of communications. This changes, however, when intelligence services solely access metadata through rules governing access to retained data. In these cases, it is usually sufficient for the services' directors to authorise access. This is problematic, because communications data reveal an individual's pertinent personal information in a similar way to content data.[116]

None of this is a judgment on a particular country's approach to national security—indeed, it could be the case that every country collects too much data on citizens and non-citizens alike without providing sufficient safeguards. The point, however, is that some practices by EU member states likely have some, if not all, of the deficiencies that the *Schrems II* judgment identified in the United States. Thus, the de facto data-localization requirements presented by that regime amounts to a form of surreptitious trade barrier.

Moreover, this trade barrier constitutes arbitrary and unjustified discrimination potentially in violation of the GATS in two ways: (1) EU countries are not held to the same standard as some non-EU countries (e.g., the United States) and (2) some non-EU countries are also not held to the same standard as other non-EU countries. The latter conclusion stems from the observation that some countries that have been granted adequacy decisions arguably would fail the standard to which the United States is being held, and that there are countries without adequacy decisions (e.g., South Korea and Israel) with arguably higher standards of data protection than some countries that do have adequacy decisions.[117]

---

[114] *See, e.g.*, EUR. UNION AGENCY FOR FUNDAMENTAL RIGHTS, SURVEILLANCE BY INTELLIGENCE SERVICES: FUNDAMENTAL RIGHTS SAFEGUARDS AND REMEDIES IN THE EU VOLUME II: FIELD PERSPECTIVES AND LEGAL UPDATE 46-48 (2017).

[115] *Id.* at 53.

[116] *Id.* at 97.

[117] The European Commission is now preparing to adopt an adequacy decision for South Korea. Arguably, if that adequacy decision is adopted without requiring significant changes in the South Korean data-protection regime, it will constitute further evidence that the EU is breaching GATS through arbitrary and unjustifiably discriminatory action because of the very significant delay in admitting that South Korean data protection meets the standards applied to EU countries and to other non-EU countries. *See* Press Release, Eur. Comm'n, *Data Protection: European Commission Launches the Process Towards Adoption of the Adequacy Decision for the Republic for Korea* (Jun. 16, 2021), *available at* https://ec.europa.eu/commission/presscorner/detail/en/ip_21_2964.

## E. Data-localization policies have dramatic unintended consequences

The problems presented by the looming data flows restrictions in the wake of *Schrems II* are manifold. Medical research frequently depends upon the use of large, pseudonymized datasets, shared between researchers across continents. Under the GDPR, there is no workable standard to transfer the data necessary for research.[118]

The GDPR's approach to data transfers has also introduced roadblocks to scientists who wish to use data banks and specimens for secondary research[119]—that is, for new and novel research purposes not contemplated when the specimen was gathered. Use of those data for secondary research in collaboration with non-EU researchers is further stymied by data flows restrictions.[120]

The process for EU medical researchers to determine if they are permitted to share data with outside researchers is complex and prone to uncertainty.[121] Even where medical research is possible—for example, where a third-party country meets adequacy standards or other mechanisms are sufficient to meet the GDPR requirements—the additional compliance burdens layer medical research projects with costs and delays.[122]

Restrictions on data flows also negatively impact firms' ability to deter cybersecurity threats and to prevent fraud.[123] And the very driver of digital global prosperity, efficiently run networks, is likewise undermined by data-localization policies:

> When data is mandated to stay inside national borders, it must temporarily be separated from a global data pool, adding additional costs and slowing services. To many in the policy debate, the slight incremental slowing of data flows might not seem like a significant impact; however, measured studies indicate that it can make a world of difference.[124]

Bringing down the barriers to trade in the 1990s with the creation of the WTO has enabled the development of increasingly complex supply chains that draw on global productive resources. Modern automobiles, information technology equipment, pharmaceuticals, even apparently mundane products like hot tubs require parts and materials from around the globe.[125] Producing a

---

[118] *See e.g.*, Bentzen, et al., *supra* note 73.

[119] David Peloquin, et al., *Disruptive and Avoidable: GDPR Challenges to Secondary Research Uses of Data*, 28 EUR. J. OF HUMAN GENETICS 697 (2020), *available at* https://www.nature.com/articles/s41431-020-0596-x.pdf.

[120] *Id.* at 701.

[121] *See* Hallinan, et al., *supra* note 72.

[122] *Id.* at 1504-05.

[123] *See, e.g.*, Chikova & Peterson, *supra* note 20, at 8-9.

[124] French, Carr, & Lowery, *supra* note 89, at 6.

[125] Austen Hufford, Kyle Kim, & Andrew Levinson, *Why Is the Supply Chain Still So Snarled? We Explain, With a Hot Tub*, WALL ST. J. (Aug. 6, 2021), https://www.wsj.com/articles/why-is-the-supply-chain-still-so-snarled-we-explain-with-a-hot-tub-11629987531.

COVID-19 vaccine in India requires a laundry list of imported inputs, such as culture media, raw materials, single-use tubing assemblies, specialty chemicals, and consumables.[126]

We would expect that, in the absence of trade barriers, "data" products would follow a similar arc and incorporate increasingly complex combinations of global data. One key is the incorporation of "live" data connections that allow real-time optimization. For example, a German equipment supplier might sell a piece of manufacturing equipment to a U.S. company that has a direct link to a Munich server to optimize production. A connected car might have multiple live data connections to minimize energy usage in real-time, while also maximizing safety. A health diagnostic product might draw on both U.S. and EU data. By comparison, data localization will lead to products that incorporate less complex uses of data from fewer sources.[127]

## V. Conclusion

As digitally enabled trade becomes ever more central to the health of the global economy, a well-calibrated approach to regulating cross-border data flows becomes critical. The worst result for the world economy would be a set of discrete, firewalled national networks—a so-called "splinternet." As noted above, this isn't just about trade in data, but about the ability to trade in a wide array of digitally enabled goods and services.

Unfortunately, the radical approach to data localization promoted by some EU policymakers risks imposing significant and otherwise unnecessary changes in digitally enabled services. Given that most digital services go beyond pure data hosting, it may be practically impossible for a U.S.-based service provider to provide absolute assurance that it could not access user data stored in an EU data center. Having control over the software that processes unencrypted (or decrypted) user data in the cloud, the provider has a theoretical capacity to access and exfiltrate the data. A more pragmatic approach to regulating cross-border data flows would involve a set of clear and reasonable safeguards that would not entail effectively foreclosing U.S. firms from providing cloud services in the European Union through de facto data localization.

There are a range of opinions on both sides of the Atlantic about how the current impasse should be overcome. It's increasingly clear that the United States needs to adopt federal privacy standards to address a wide range of domestic and cross-border business transactions, though consensus legislation has not yet emerged. In addition, there's growing support in the United States for

[126] Anthony King, *Why Manufacturing Covid Vaccines at Scale is Hard*, CHEMISTRY WORLD (Mar. 23, 2021), https://www.chemistryworld.com/news/why-manufacturing-covid-vaccines-at-scale-is-hard/4013429.article.

[127] The continued proliferation of data-localization requirements will also tend to favor countries with larger, more data-rich economies, which will still be able to build complex data products based solely on sources from within their own borders. Considering the geopolitical ramifications of this tendency is beyond the scope of the paper, but it's important to consider how this could affect international trade and international relations more broadly. To take but one example, 5G wireless systems are particularly well-suited to support complex data products. On average, therefore, countries that impose data-localization requirements are undercutting their own investments in 5G and contributing to further technological fragmentation, while also undermining the sort of standardized collaboration that contributes so much to global prosperity and interoperability.

increased regulation of cross-border data flows to deal with such highly publicized criminal abuses such as foreign-based ransomware, cross-border disinformation campaigns, cyber-theft of intellectual property, and the like. Such effective public-interest regulation and crime-control can be done with a "least trade restrictive approach" necessary to achieve the desired policy goals. Nevertheless, such legislation will, by itself, not resolve *Schrems II*-related issues.

On the one hand, certain parties in the EU are promoting a maximalist position that, as noted above, will impose more economic and cultural costs than it will realize benefits in privacy or other values. For instance, the European Parliament issued a nonbinding resolution intended to express its view of how *Schrems II*-related issues should be interpreted by data-protection authorities.[128] On that view, the United States would have to adopt robust legislative changes to fully comply with an expansive interpretation of the *Schrems II* judgment, despite the fact that EU member states are not themselves entirely held to that standard.[129] Alternatively, the resolution suggests that the United States could enter into "no-spying" agreements with all EU member states to satisfy the views expressed in that document.[130]

Short of those measures, it seems the European Parliament believes that the EU should proceed at full steam with data localization and investments in technological self-sufficiency (embracing the creation of a splinternet or cyber-balkanization).[131] This is a self-evidently destructive path for the European Parliament to push.

But there is more nuance to EU data-protection enforcement than the European Parliament's nonbinding maximalist view would suggest. Enforcement remains in the hands of national data protection authorities throughout the EU. In practice, some data protection authorities are relatively more aggressive with enforcement,[132] but certainly not all authorities. Thus, even under *Schrems II*, there exists a diversity of positions within the EU.

In terms of moving the United States toward an adequacy decision, there are some proposals for administrative and legislative changes in the United States that stop short of the maximalist interpretation of the *Schrems II* judgment.[133] Open acknowledgment of the double standard implicit in the maximalist positions of the European Parliament and the EDPB—which, if enforced, would

---

[128] Eur. Parliament resolution on Schrems II, *supra* note 10.

[129] *Id.* at paras. 22, 27.

[130] *Id.* at para. 27.

[131] *Id.* at para. 26.

[132] *See supra* notes 17 - 18, and associated text.

[133] *See, e.g.,* CTR. FOR DEMOCRACY & TECH., SCHREMS II AND THE NEED FOR INTELLIGENCE SURVEILLANCE REFORM (2021), https://cdt.org/wp-content/uploads/2021/01/2021-01-13-CDT-Schrems-II-and-Intelligence-Surveillance-Reform-in-the-US.pdf; see also Sharon Bradford Franklin, Lauren Sarkesian, Ross Schulman, & Spandana Singh, *Strengthening Surveillance Safeguards After Schrems II, A Roadmap for Reform*, New America (2021), *available at* https://www.newamerica.org/oti/reports/strengthening-surveillance-safeguards-after-schrems-ii.

arguably place the EU in breach of GATS—may help to produce a set of politically realistic changes on the U.S. side.

Theodore Christakis of University Grenoble Alpes has postulated that an agreement on essential equivalence could be reached in respect to Section 702 FISA, with the EU accepting that an SCC requirement that data-in-transit is fully encrypted renders moot the adequacy issues raised by Executive Order 12333, signed in 1981 by President Ronald Reagan.[134] Further, in its comments to the EDPB, the United States has pointed out that, under CJEU jurisprudence, national-security laws that do not impose processing requirements on private parties do not affect the adequacy of SCCs.[135] That is to say, national-security laws that empower government agencies to perform direct access on data in transit do not, on their own, invalidate the ability of SCCs to enable transfer by third parties. Related to these ideas, in December 2020 testimony before the U.S. Senate Commerce Committee, law professor Peter Swire of Georgia Tech presented a comprehensive set of proposals that develops ways in which targeted reforms could be used to answer the challenges posed by the *Schrems II* decision.[136]

Policymakers around the world need to think about data localization and data flows more holistically. It's important to understand how data-localization requirements can act in much the same way as other protectionist trade barriers, accept the necessity of data flows across global networks, and seek to balance these realities with other valid concerns, like national security and user privacy.

Episodes like *Schrems II* ideally would recede into the background as policymakers make efforts to move forward in collaboration to develop proper standards for both government surveillance and the private flow of data across national borders.

Part of this must undoubtedly involve the United States working more closely with other governments to create forward-looking digital trade agreements. The Biden administration has signaled, for instance, that it has plans to continue the Obama administration's "pivot to Asia,"[137]

---

[134] *See, e.g.*, Theodore Christakis, *Squaring the Circle? International Surveillance, Underwater Cables and EU-US Adequacy Negotiations (Part 2)*, EUROPEAN LAW BLOG (Apr. 13, 2021), https://europeanlawblog.eu/2021/04/13/squaring-the-circle-international-surveillance-underwater-cables-and-eu-us-adequacy-negotiations-part2/.

[135] *See* Int'l Trade Admin., *supra* note **Error! Bookmark not defined.**.

[136] *See* The Invalidation of the EU-U.S. Privacy Shield and the Future of Transatlantic Data Flows: Hearing Before the Commerce Comm., 116 Cong. (2020) (Statement of Peter Swire), Appendix 1, *available at* https://www.alstonprivacy.com/wp-content/uploads/2020/12/Swire-Full-Testimony-with-Appendices.final-as-submitted.pdf (discussing how "individual redress" for EU citizens can be introduced into US foreign intelligence law in a variety of ways); *see also* Alex Joel, *Protect Privacy. That's an Order.*, LAWFARE (Apr. 6, 2021), https://www.lawfareblog.com/protect-privacy-thats-order (A proposal for developing a fix to *Schrems II* using an executive order).

[137] *See* Yen Nee Lee, *Biden Beefs Up Administration with Asia Experts as the U.S. Prepares to Take on China*, CNBC (Feb. 4, 2021), https://www.cnbc.com/2021/02/05/biden-fills-team-with-asia-experts-as-us-prepares-to-take-on-china.html.

with President Biden calling the U.S. relationship with China the "the biggest geopolitical test of the 21st century."[138]

The Asia-Pacific countries offer a good model for the path forward. Singapore, New Zealand, and Chile have concluded the Digital Economy Partnership Agreement in 2020, which explicitly directs members to experiment with regulations that permit data flows.[139] Similarly, the Australia-Singapore Digital Economy Agreement creates a presumption in favor of data flows and forbids regulations that are a "disguised restriction on trade."[140]

In the end, policymakers around the world—but most immediately in the United States and the European Union—need to take seriously the centrality of data flows to the modern economy. Data policy should be directed toward enabling flows and innovation, but with necessary safeguards. Allowing the world to move toward fragmented splinternets benefits no one.

---

[138] Speech of Antony J. Blinken, U.S. Secretary of State (Mar. 3, 2021), *available at* https://www.state.gov/a-foreign-policy-for-the-american-people/ ("The test is how to negotiate American interests in the face of Chinese expansion into world affairs. In this context, the question is which country's model of trade agreements and, more specifically, digital policy should become preeminent.").

[139] *See* Digital Economy Partnership Agreement (Jun. 11, 2020), at Art 9.4, *available at* https://www.mti.gov.sg/-/media/MTI/Microsites/DEAs/Digital-Economy-Partnership-Agreement/Digital-Economy-Partnership-Agreement.pdf.

[140] *See* Australia-Singapore Digital Economy Agreement (Aug. 6, 2020), at Art. 23, *available at* https://www.dfat.gov.au/sites/default/files/australia-singapore-digital-economy-agreement.pdf.