ICLE International Center for Law & Economics

Issue Brief: The Great Transatlantic Data Disruption
October 7, 2021
Kristian Stout, Michael Mandel and Mikołaj Barczentewicz

(This issue brief is a joint publication of the International Center for Law & Economics and the Progressive Policy Institute)

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*. (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. 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.

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." 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. 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. 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.

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). 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.

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. 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.

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. 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*.

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." 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.* 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.

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. 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. 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.

Read the full issue brief here.

View Article