



Georgetown University Law Center
Scholarship @ GEORGETOWN LAW


2020

Is Data Localization a Solution for Schrems II?

Anupam Chander

This paper can be downloaded free of charge from:
<https://scholarship.law.georgetown.edu/facpub/2300>
<https://ssrn.com/abstract=3662626>

This open-access article is brought to you by the Georgetown Law Library. Posted with permission of the author.
Follow this and additional works at: <https://scholarship.law.georgetown.edu/facpub>

 Part of the [Computer Law Commons](#), [International Trade Law Commons](#), [Internet Law Commons](#), [Law and Economics Commons](#), and the [Privacy Law Commons](#)

IS DATA LOCALIZATION A SOLUTION FOR *SCHREMS II*?

ANUPAM CHANDER*

Abstract

For the second time this decade, the Court of Justice of the European Union has struck a blow against the principal mechanisms for personal data transfer to the United States. In Data Protection Commissioner v Facebook Ireland, Maximilian Schrems, the Court declared the EU-US Privacy Shield invalid and placed significant hurdles to the process of transferring personal data from the European Union to the United States via the mechanism of Standard Contractual Clauses. Many have begun to suggest data localization as the solution to the problem of data transfer; that is, don't transfer the data at all. I argue that data localization neither solves the problem of foreign surveillance, nor enhances personal privacy, while undermining other values embraced by the European Union.

INTRODUCTION.....	1
I. <i>SCHREMS II</i> AS SOFT DATA LOCALIZATION.....	2
A. <i>Schrems II</i> and Mechanisms for Cross-Border Data Flows.....	2
B. Alternative Mechanisms for Cross-Border Data Flows.....	4
C. A Soft Data Localization.....	7
II. WHY DATA LOCALIZATION DOESN'T SOLVE SURVEILLANCE	8
A. US Surveillance Continues Abroad.....	8
B. European Surveillance at Home: The More Spies, the Merrier.....	8
C. Data Transfers Will Still Occur.....	11
D. The Border Hopping of Internet Routing.....	11
III. WHY DATA LOCALIZATION CREATES ITS OWN PROBLEMS	12
CONCLUSION.....	14

Introduction

In a presentation via LinkedIn the day after his victory before the Court of Justice of the European Union (“CJEU”) in the case of *Data Protection Commissioner v Facebook Ireland, Maximilian Schrems* (“*Schrems II*”), Schrems himself suggested what seems to be an easy fix for

* Professor of Law, Georgetown University Law Center; A.B., Harvard College; J.D. Yale Law School. I am grateful to Nigel Cory, Christopher Kuner, Asaf Lubin, Kenneth Propp, and Thomas Streinz for expert suggestions. I am also grateful to a Google Research Award a number of years ago that supported related research. All views, and all errors, are mine alone.

companies transferring data outside Europe to the United States—don't. Leave the data in the EU.¹

Is data localization the easy fix for the difficult problems raised by crossborder data flows? If Facebook is merely a tool for the U.S. government to grab European data, then perhaps keeping the information in Europe placates those fears. Add the “accidental” side benefit of data localization—a greater demand for European digital services. A win (for privacy) and win (for economic development)! Or so the story goes.

That is the proposition I wish to test in this paper.

The validity of the proposition has broad significance for international economic law. Trade is increasingly digital—in the form of digital services, e-commerce, and the internet of things.² If data localization becomes the de facto solution to the absence of internationally interoperable privacy regimes, then many of the benefits of the global internet and the increased trade it brings will be at risk. The proliferation of data localization measures will undermine the crossborder data flows that power global trade. Thus, issues of data localization are on the agenda at the World Trade Organization in the Joint Statement Initiative on e-commerce,³ though this case shows that security and privacy exceptions can indeed be so large that they swallow the rule.

This analysis proceeds as follows. Part I begins by describing the emergence of a “soft data localization” mandate in the European Union based on *Schrems II*. By “soft data localization,” I mean a legal regime that puts pressure on companies to localize, not by directly requiring localization of data or processes, but by making alternatives legally risky and thus potentially unwise. Part II then asks whether such soft data localization advances either privacy or economic development, concluding that there are reasons to think that it undermines both. Data localization, Part III argues, raises costs for businesses, especially smaller ones, undermines the European Union’s goals of increased trade, invites reprisal from trading partners, undermines cybersecurity, and harms many local businesses while favoring a few.

I. *Schrems II* as Soft Data Localization

Schrems II strikes a body blow to the principal existing mechanisms for cross-border data transfer from the EU to the US, and, in the process, complicates data transfers from the EU to much of the rest of the world as well. The practical effect is to put pressure on companies to keep the data inside the European Union. This Part explains how *Schrems II* creates this pressure.

A. *Schrems II* and Mechanisms for Cross-Border Data Flows

The CJEU’s decision in *Schrems II* is both lengthy and complicated, and we will focus on certain practical implications of the decision here.⁴ This case was Max Schrems’ second round

¹ <https://www.linkedin.com/video/live/urn:li:ugcPost:6689891492103798784/>.

² See generally Anupam Chander, *Trade 2.0*, 34 YALE J. INT’L L. 281 (2009); ANUPAM CHANDER, THE ELECTRONIC SILK ROAD: HOW THE WEB BINDS THE WORLD IN COMMERCE (2013).

³ World Trade Organization, *Joint Statement on Electronic Commerce* (WT/L/1056) (Jan. 25, 2019).

⁴ For expert analyses, see Christopher Kuner, <https://europeanlawblog.eu/2020/07/17/the-schrems-ii-judgment-of-the-court-of-justice-and-the-future-of-data-transfer-regulation/>; Kenneth Propp & Peter Swire, *Geopolitical Implications of the European Court’s Schrems II Decision*,

at the CJEU. Both rounds centered on the legality of transferring personal data from the European Union to the United States pursuant to particular mechanisms—the EU-US Safe Harbor in *Schrems I*, and the EU-US Privacy Shield and the Standard Contractual Clauses in *Schrems II*. The European Union’s data protection law has constrained transfers of personal data from the European Union, first in the Data Protection Directive beginning in 1998, and, since 2018, in the General Data Protection Regulation (“GDPR”). The Safe Harbor and the Privacy Shield were *sui generis* agreements negotiated only with the United States to permit data transfers to companies certifying compliance with the rules provided in those arrangements. The Clinton Administration negotiated the Safe Harbor in 2000, and when that was struck down by the CJEU in *Schrems I* in 2015 as insufficiently protective of EU residents’ rights, the Obama Administration negotiated the Privacy Shield as its replacement in 2016. In both rounds, the CJEU repudiated the European Commission-approved arrangements for data transfer to the United States as inadequate. In *Schrems II*, the CJEU ruled that the Standard Contractual Clauses—a set of contractual terms that obliged the parties to contractually enforceable data protection obligations—could still be used to transfer data to the United States, as long as “essentially equivalent” protections for EU personal data could be assured.⁵

The end-result of the court’s ruling in *Schrems II* is to reduce the available channels for transferring personal information from the European Union to the United States: two of the principal mechanisms for transferring personal data to the United States have either been repudiated outright or made unstable. The CJEU struck down the EU-US Privacy Shield, an agreement that more than 5,300 companies (both European and American⁶) use to transfer data across the Atlantic. And while the CJEU upheld the validity of Standard Contractual Clauses (SCCs) for transferring data outside the EU, it conditioned that transfer on a determination by the transferring parties that the transfer would not risk unwarranted surveillance by the U.S. government. While the putative defendant in the case was Facebook, it was the U.S. government that was on trial.⁷

In critiquing U.S. surveillance law, the CJEU examined, in particular, Foreign Intelligence and Surveillance Act Section 702, Presidential Policy Directive 28, and Executive Order 12333. This set of rules authorizing and regulating foreign intelligence provide inadequate protection in comparison to that required under EU law, the court held. The CJEU concluded that “Section 702 of the FISA does not indicate any limitations on the power it confers to implement surveillance programmes for the purposes of foreign intelligence or the existence of guarantees for non-US persons potentially targeted by those programmes.” And with respect to PPD-28, the CJEU observed that it “does not grant data subjects actionable

<https://www.lawfareblog.com/geopolitical-implications-european-courts-schrems-ii-decision>; Daniel Solove, <https://teachprivacy.com/the-schrems-ii-decision/>; Jennifer Daskal, <https://www.justsecurity.org/71485/what-comes-next-the-aftermath-of-european-courts-blow-to-transatlantic-data-transfers/>. For an analysis of the Attorney General opinion preceding the CJEU decision, see Peter Swire, <https://www.lawfareblog.com/foreign-intelligence-and-other-issues-initial-opinion-schrems-ii>.

⁵ *Schrems II*, para. 203 (“[A]ppropriate safeguards ... must ensure that data subjects whose personal data are transferred to a third country pursuant to standard data protection clauses are afforded a level of protection essentially equivalent to that guaranteed within the European Union by that regulation, read in the light of the Charter of Fundamental Rights of the European Union.”).

⁶ Propp & Swire, *supra* note 4.

⁷ Technically, both Facebook and Max Schrems are defendants in the original case, which the Irish Data Protection Commissioner brought to clarify EU law by way of preliminary reference to the EU Court of Justice. I am grateful to Thomas Streinz for this observation.

rights before the courts against the US authorities.” And the CJEU concluded the same with respect to the EO 12333, that it “does not confer rights which are enforceable against the US authorities in the courts either.” (183) With respect to EO 12333, the CJEU went further, arguing that it fails to “delimit in a sufficiently clear and precise manner the scope of such bulk collection of personal data.” All of this led the CJEU to conclude:

It follows therefore that neither Section 702 of the FISA, nor E.O. 12333, read in conjunction with PPD-28, correlates to the minimum safeguards resulting, under EU law, from the principle of proportionality, with the consequence that the surveillance programmes based on those provisions cannot be regarded as limited to what is strictly necessary. (184)

With this analysis, the CJEU invalidated the Privacy Shield Decision as failing to “ensure a level of protection essentially equivalent to that arising from the Charter [of Fundamental Rights of the European Union].” And it declared that transfers under the Standard Contractual Clauses should be suspended if the supervisory authority determines that “in light of all of the circumstances of the transfer” the data cannot be appropriately protected.

Christopher Kuner points out that the CJEU “suggests using ‘supplementary measures’ (para. 133) to protect data under the SCCs, but does not explain what measures these could be.”⁸ Indeed, Kuner goes on to say that, in effect, all SCCs become “mini adequacy decisions.” The complexity of this process may well lead companies, especially smaller ones, to avoid this route entirely. While large firms will be able to afford the expensive legal advice reviewing a foreign nation’s surveillance law for compatibility with EU law, smaller firms will not. The not-for-profit organization with which Max Schrems is associated goes further to declare, “SCCs are thus de facto dead for outsourcing to US companies.”⁹

Even while it upholds Standard Contractual Clauses as a possibly valid vehicle for transfer, *Schrems II* complicates the process. This is very important for practical purposes because a large fraction of data exports from the EU rely on Standard Contractual Clauses.¹⁰

B. Alternative Mechanisms for Cross-Border Data Flows

What of the alternative mechanisms for data transfer? While the GDPR contemplates a variety of mechanisms to permit cross-border data transfer, many of those mechanisms may not be readily available in any particular case. I consider the most prominent alternatives below.

Adequacy decision. Given that most of the countries of the world have not been recognized with an adequacy ruling, the simplest mechanism for the export of data will not be available with respect to transfers to most of the world. The only country that the Commission

⁸ Kuner, *supra* note 4.

⁹ <https://noyb.eu/en/fact-check-facebook-can-no-longer-rely-scc>.

¹⁰ The International Association of Privacy Professionals surveyed members and reported that “Seven in 10 respondents say their organization transfers data out of the EU to non-EU countries.... The most popular of these tools — year over year — are overwhelmingly standard contractual contracts: 88% of respondents in this year’s survey reported SCCs as their top method for extraterritorial data transfers, followed by compliance with the EU-U.S. Privacy Shield arrangement (60%).”

is currently considering for adequacy at this moment is South Korea.¹¹¹² Even countries that have adequacy rulings in place may see those adequacy rulings withdrawn in the face of *Schrems II* if they are unable to satisfy the European Commission that their protections against unwarranted surveillance are robust and justiciable. All of the eleven other countries with adequacy decisions (Andorra, Argentina, Canada, Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Switzerland, Uruguay, and the United States of America) have been undergoing a review since 2017, and *Schrems II* will necessarily require even greater scrutiny of those countries surveillance law and practice.¹³ Indeed, for many, it may be difficult to show that their laws and practices constrain surveillance in ways that *Schrems II* seems to require. The United Kingdom, long insulated from a similar inquiry, now will have to satisfy the European Commission that it deserves an adequacy ruling post-Brexit. For its part, the U.S. government will be engaged in negotiations with the European Commission to seek a successor to the EU-US Privacy Shield, just as it did in the wake of the CJEU's invalidation of the Safe Harbor that preceded the Privacy Shield. The European Commission would then, if those negotiations are successful, follow with an adequacy decision, allowing data flows to the U.S. for companies complying by those special arrangements. But in the interim, that avenue is foreclosed for transfers to the United States and most of the rest of the world.¹⁴

Binding Corporate Rules. One prominent mechanism for cross-border transfer under the GDPR, the Binding Corporate Rules, is available only for intra-company transfers. But companies often need to share information with third parties—for example, through application processing interfaces (APIs) for various permissible uses, to enable data portability, and to outsource business processing.

Consent or Necessity. As Thomas Streinz has pointed out,¹⁵ the CJEU itself suggests Article 49 derogations as a basis for transfers to the United States in the wake of its own ruling in order to avoid “the creation of a legal vacuum.”¹⁶ Article 49 offers two main paths for what

¹¹ Christopher Kuner calls the slow process of adequacy approvals “clearly absurd,” and notes that the process “is complicated by political factors.” Christopher Kuner, *Developing an Adequate Legal Framework for International Data Transfers*, in *Reinventing Data Protection?* (Serge Gutwirth et al (eds), 2009). Indeed, if we compare the history of both adequacy decisions and the expansion of the EU itself since 1995, 13 countries (five of which are small island dependencies of European states) have attained adequacy (including one, the United States, which has twice lost that status), while 16 countries have joined the EU, therefore bypassing any need for review of their surveillance laws in order to receive EU personal data freely. https://www.europarl.europa.eu/external/html/euenlargement/default_en.htm. It is only a slight exaggeration to say that if a country wishes to receive personal data freely from the EU, it may be easier to apply to join the EU rather than to seek an adequacy ruling.

¹² https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en.

¹³ Catherine Stupp, Commission conducting review of all foreign data transfer deals, Euractiv.com Nov. 9, 2017, <https://www.euractiv.com/section/data-protection/news/commission-conducting-review-of-all-foreign-data-transfer-deals/>.

¹⁴ There is no reason to assume that transferring to countries with an existing adequacy decision from the European Commission is a surefire way of satisfying the EU's data protection law requirements. After all, the EU-US Privacy Shield had been blessed by an adequacy decision from the Commission, before falling in *Schrems II*. That said, adequacy decisions remain the most secure of the various options for cross-border data transfer under the GDPR.

¹⁵ Thomas Streinz, https://twitter.com/t_streinz/status/1283894104988872704.

¹⁶ *Schrems II* at para. 202.

it calls “derogations” that permit transfer despite a lack of an adequate data protection law: consent or necessity.

Consent would seem a promising candidate for data transfer, but there are three hurdles. First, consent must be vigorous: “Consent of the data subject means any freely given, specific, informed and unambiguous indication of the data subject’s wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.” (Art. 4(11).) This description is further qualified by another set of conditions in Article 7, creating a number of hurdles for consent to be satisfactory. As the UK data protection authority, the Information Commissioner’s Office (ICO), advises: “Given the high threshold for a valid consent, and that the consent must be capable of being withdrawn, this may mean that using consent is not a feasible solution.”¹⁷ Second, the fulsome consent needed from every data subject can be expensive and time-consuming. Third, early interpretations of consent and related derogations by European authorities tend to be quite restrictive.¹⁸ That said, the European Data Protection Board acknowledges that “[a]ccording to Article 49 (1)(a) GDPR, explicit consent can lift the ban on data transfers to countries without adequate levels of data protection law.”¹⁹ There is some basis for arguing that the GDPR does in fact allow for the use of consent for “systemic” data transfers.²⁰

Necessity, too, seems narrowly construed. Necessity cannot be used for systemic transfers, but must be reserved for “occasional” transfers.²¹ The European Data Protection Board says, for example, that necessity “cannot be used for example when a corporate group has, for business purposes, centralized its payment and human resources management functions for all its staff in a third country as there is no direct and objective link between the performance of the employment contract and such transfer.”²² Max Schrems’ not-for-profit organization lists a variety of cases of cross-border transfer that it believes are in fact necessary: “[b]ooking a hotel or other accommodation directly in the US or through a travel agency in the EU (e.g. a room in San Francisco); [b]ooking a flight to the US; [r]eservation for a rental car in the US; [o]rdering goods online from a US-based company; [u]sing online services provided by a US-based company (with no establishment in the EU); [s]ending an email to the US; [s]ending your data to your lawyer in the US in the context of a lawsuit; [c]ontacting a Facebook friend that is located in the US; [v]ideo calls to the US.”²³ Some of these actions, for example, using an online service in the U.S. or sending an email might appear to be systemic rather than occasional. Indeed, if sending an email to the U.S. is permitted via the derogation

¹⁷ <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/international-transfers/>

¹⁸ European Data Protection Board, EDPB Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679 Adopted on 25 May 2018.

¹⁹ European Data Protection Board, *Guidelines 05/2020 on consent under Regulation 2016/679 Version 1.1*, May 4, 2020, p. 20, n. 47.

²⁰ <https://www.natlawreview.com/article/does-gdpr-allow-use-consent-international-transfer-data> (“Consent may now be used even in case of repeated, massive or structural transfers.”).

²¹ European Data Protection Board, *supra* note 18, at 9; European Data Protection Board, *Frequently Asked Questions on the judgment of the Court of Justice of the European Union in Case C-311/18 - Data Protection Commissioner v Facebook Ireland Ltd and Maximilian Schrems*, July 23, 2020, p. 4.

²² European Data Protection Board, *supra* note 18, at 8.

²³ NOYB, *Next Steps for users & FAQs*, July 24, 2020, <https://noyb.eu/en/next-steps-users-faqs>.

for necessity, might not communicating with your Facebook network in the U.S. be similarly necessary?

Certifications and Codes of Conduct. While the GDPR introduces the possibility of certifications and codes of conduct as mechanisms to enable cross-border transfer, no such mechanisms have yet been officially offered.²⁴

C. A Soft Data Localization

The review of the main alternatives for data transfer shows that the process is quite fraught in the wake of *Schrems II*. *The end result of this decision is thus pressure towards data localization.* Why? Because data localization seems to avoid the problems that the decision raises. If there is no data transfer outside the European Union, then there is no need to take the risk that the transfer will be found invalid by a data protection authority or a court. Indeed, the day after the *Schrems II* decision was handed down, the Berlin German data protection authority called for “data controllers based in Berlin storing personal data in the US to transfer the same to Europe.”²⁵

By soft data localization, I do not mean to suggest that *Schrems II* requires data localization or that it is even the recommended response. The CJEU, of course, explicitly contemplates (but does not specify) that there are additional measures that the data controller can take to ensure that the risks of data being gathered by the U.S. government without sufficient protection remain quite low. However, by failing to offer any guidance as to what such additional measures might be, it creates uncertainty. Even any guidance offered by Data Protection Authorities in the near term may not ultimately be enough to satisfy the CJEU in a future challenge. Thus, even while *Schrems II* does not establish a *de jure* requirement for data localization, its encumbrances on cross-border data flows to the United States, and to other foreign countries, seem to point many businesses to use data localization to solve the problems the decision poses.

The not-for-profit organization for which Max Schrems serves as honorary chair would go beyond data localization in the European Union. It suggests avoiding U.S. providers, even those operating in the EU.²⁶ After all, the argument goes, these providers might be compelled to turn over data to the U.S. authorities. This is not merely data localization, as it would ban the use of cloud services such as Amazon Web Services, Google Cloud, and Microsoft Azure even when they use servers in the European Union. The United States has offered a legislative fix for this concern, at least with respect to law enforcement access to information stored across borders. The Clarifying Lawful Overseas Use of Data Act (CLOUD Act) was designed to reduce frictions between countries in just such cases through two mechanisms: first, it permits governments to negotiate executive agreements to govern such exchanges; second, it allows warrants requesting data outside the United States to be challenged on the basis of a comity analysis, including the location, nationality, and

²⁴ Nigel Cory, *Response to the Consultation of the EU Commission on transfers of personal data to third countries and cooperation between data protection authorities* (Information Technology and Innovation Foundation, Nigel Cory and Eline Chivot, April 29, 2020), <https://itif.org/publications/2020/04/29/response-european-commission-consultation-transfers-personal-data-third>.

²⁵ <https://www.dataguidance.com/news/berlin-berlin-commissioner-issues-statement-schrems-ii-case-asks-controllers-stop-data>.

²⁶ <https://noyb.eu/en/next-steps-eu-companies-faqs>.

connections to the U.S. of the subscriber or customer whose communications are being sought.

To summarize: data localization is a *practical response* to the constraints on cross-border data flow in *Schrems II*. However, as I will argue in the two Parts below, data localization may well not solve the policy objectives identified in *Schrems II*, and creates its own policy problems.

II. Why Data Localization Doesn't Solve Surveillance

Data localization will not prove a panacea for the surveillance that motivates the Court of Justice in *Schrems II*.

It is certainly true that the United States intelligence services lack the legal authorities on the ground inside the European Union to compel information sharing by local digital infrastructure providers. But that does not curtail either the U.S. or the many intelligence services that it partners with or that work on their own behalf from surveilling Europeans.

A. US Surveillance Continues Abroad

U.S. foreign surveillance is least constrained abroad.²⁷ The fact that the data is stored within the boundaries of the European Union does not insulate it from U.S. spying. Germans may recall the revelations that the U.S. government listened in on Chancellor Angela Merkel's phone in Berlin itself.²⁸ As the Edward Snowden revelations helped demonstrate, foreign intelligence services today deploy malware, zero days, insider attacks, and other exploits outside their own shores to target foreign intelligence targets.

B. European Surveillance at Home: The More Spies, the Merrier

European intelligence services also, of course, operate within Europe. In this sense, data localization may not even trade one nation's spies for another's, but rather simply compound the possible sources of spies.

In the wake of the Snowden revelations of widespread electronic communications interceptions by the U.S. government, the European Parliament uncovered widespread bulk collection of "upstream" information via telecommunications networks, concluding that, for the five EU member states it reviewed (UK, Sweden, France, Germany and the Netherlands (Section 2), "[p]ractices of so-called 'upstreaming' (tapping directly into the communications infrastructure as a means to intercept data) characterise the surveillance programmes all the selected EU member states, with the exception of the Netherlands for whom there is, to date, no concrete evidence of engagement in large-scale surveillance."²⁹ The Parliamentary report, for example, observed the following about Sweden's signals intelligence agency, the FRA:

²⁷ Anupam Chander & Uyen P. Lê, *Data Nationalism*, 64 Emory L.J. 677, 714-18 (2015); Foreign Intelligence Surveillance Act, 50 U.S.C. §§ 1801–1885c (2012).

²⁸ *The NSA's Secret Spy Hub in Berlin According, Spiegel*, Oct. 27, 2013, <https://www.spiegel.de/international/germany/cover-story-how-nsa-spied-on-merkel-cell-phone-from-berlin-embassy-a-930205.html>.

²⁹ European Parliament Study, *National Programmes for Mass Surveillance of Personal Data in EU Member States and Their Compatibility with EU Law* 58 (October 2013), <http://www.statewatch.org/news/2013/oct/ep-study-national-law-on-surveillance.pdf>.

The evidence indicates that FRA has been running operations for the ‘upstream’ collection of private data - collecting both the content of messages as well as metadata of communications crossing Swedish borders. The metadata is retained in bulk and stored in a database known as ‘Titan’ for a period of 18 months.³⁰

Joel Reidenberg, too, described rules across Europe that enabled communications surveillance by European governments.³¹

In recent years, the legal framework under which that surveillance occurs has come under severe attack (and in some cases, the absence of any legal framework at all). The European Court of Human Rights ruled in 2016 that the Hungarian system of domestic surveillance violated the European Convention of Human Rights. In the case of *Szabó and Vissy v. Hungary*,³² staff members of a non-governmental watchdog organization had brought suit against surveillance measures by Hungary's Anti-Terrorism Task Force, which was legally authorized “to conduct secret house searches, surveil and record targets, open letters and parcels, and check and record the contents of electronic or computerized communications.”³³ If such surveillance was for national security purposes, it need only be authorized by the Justice Minister. The European Court of Human Rights also found aspects of Bulgarian secret surveillance law to be in contravention of the European Convention of Human Rights.³⁴

A number of cases have challenged national laws across Europe, as well as an EU directive, that require electronic communications service providers to retain traffic and location data for their users. In *Digital Rights Ireland Ltd v. Minister for Communication et al, and Kärtner Landesregierung*, the Court of Justice of the European Union declared the EU Data

³⁰ *Id.* at 58.

³¹ Reidenberg writes:

In Europe, like in the United States, intelligence services are afforded privileged rights of access to data. For example, in the United Kingdom, a secretary of state (typically the foreign secretary or the home secretary) may order interception of communications without a court warrant; the decision is entirely a ministerial choice. Under the Regulation of Investigatory Powers Act, interceptions may even be made “for the purpose of safeguarding the economic well-being of the United Kingdom.”

France similarly has mechanisms for the executive branch to gather communications data without a court order. Although in 1991 France established the National Commission for the Control of Security Interceptions (Commission nationale de contrôle des interceptions de sécurité), the commission only has the power to make recommendations on the legality of interceptions and does not have the power to block them. Thus, there is no truly independent supervision of government access for an important range of surveillance orders. And also like the United Kingdom, security interceptions on the order of the prime minister's office are permitted to safeguard France's economic interests thereby providing a very broad basis to engage in surveillance.

Even liberal Sweden allows warrantless wiretapping for intelligence purposes,⁸ as does the Netherlands. And Germany, too, provides special privileges for “strategic surveillance.” According to recent reports, on the order of the German prime minister, the German intelligence agency has a direct tap into the equipment of Internet service providers.

Joel R. Reidenberg, *The Data Surveillance State in the United States and Europe*, 49 Wake Forest L. Rev. 583, 593–95 (2014). Of course, this does not account for subsequent reforms in the law.

³² *Szabó and Vissy v. Hungary*, App. No. 37138/14, Eur. Ct. H. R. (Jan. 12, 2016).

³³ Michael Palmisano, *The Surveillance Cold War: Recent Decisions of the European Court of Human Rights and Their Application to Mass Surveillance in the United States and Russia*, 20 Gonz. J. Int'l L. 1 (2017).

³⁴ *Hadzhiev v. Bulgaria*, No. 22373/04 (Eur. Ct. Human Rights) (2012).

Retention Directive, which “required telecommunications service providers to retain for up to two years all metadata from every EU citizens' emails, text messages, and telephone calls, and to make these available to national security agencies for investigatory purposes—to be in violation of the rights to privacy and data protection enshrined in the European Union Charter of Fundamental Rights.”³⁵ And in 2016, the Court of Justice of the European Union ruled that data retention laws in Sweden and the United Kingdom violated EU law.³⁶

Unlike the other cases, the German Constitutional Court’s ruling in the *BND Act Case* earlier this year focuses on the rights of foreigners. That case requires that German intelligence services acting from Germany to spy on foreigners must abide by the German Grundgesetz (the Basic Law or constitution).³⁷ Because this case focuses on the rights of foreigners vis-à-vis national security surveillance, it is closest to the sort of rights that the Court of Justice of the European Union seems to demand in *Schrems II*.³⁸ After the Snowden revelations, a German Parliamentary inquiry had determined that the *Bundesnachrichtendienst* (Federal Intelligence Service or BND) conducted foreign strategic surveillance without any statutory authorization. A 2016 reform explicitly authorized strategic foreign-foreigner telecommunications surveillance through a legal process, but one which did not have the protections that the German Constitutional Court believed were necessary.

For some, cases such as these will demonstrate that the European Union’s legal protections against surveillance are robust. After all, the cases show that legal system working to declare various legal regimes inadequate. But these cases do not give a sense of the 28, soon 27, Member States’ full panoply of surveillance rules currently in place. Canvassing recent case law, Asaf Lubin concludes that “not only has mass surveillance by governments become the new normal even in Europe, ... but this new normal has now received the Strasbourg Court’s official stamp of approval.”³⁹ Lubin notes, for example, that the European Court of Human Rights sustained Sweden’s mass surveillance regime for foreign intelligence gathering in a 2018 case.⁴⁰ Another study published in 2017 concludes that “national security legal authorities such as Section 12 of the [UK] Counter-Terrorism Act of 2008 have become increasingly powerful since 9/11 in the UK and some European countries, the United States, and globally.”⁴¹

Furthermore, many of the laws may not have been reformed their laws in the wake of adverse decisions. The German Constitutional Court gave the German government till 2021 to reform its laws to provide better rights to foreigners. The European Court of Human Rights’ tracking of the implementation of the European Court of Human Rights decision on

³⁵ Federico Fabbrini, *Human Rights in the Digital Age: The European Court of Justice Ruling in the Data Retention Case and Its Lessons for Privacy and Surveillance in the United States*, 28 HARV. HUM. RTS. J. 65 (2015).

³⁶ *Tele2 Sverige and Watson and Others* (C-698/15) (Eur. Ct. Hum. Rts. 2016).

³⁷ <https://www.lawfareblog.com/german-constitutional-court-nixes-foreign-surveillance/> (“The court has insisted instead that German intelligence services follow the wisdom of a different Old Testament figure, the contemplative king of Ecclesiastes who urged: ‘do good wherever you go.’”).

³⁸ Melissa Eddy, *Right to Privacy Extends to Foreign Internet Users, German Court Rules*, N.Y. Times, May 19, 2020.

³⁹ Asaf Lubin, *Legitimizing Foreign Mass Surveillance in the European Court of Human Rights*, JUST SECURITY, Aug. 2, 2018, <https://www.justsecurity.org/59923/legitimizing-foreign-mass-surveillance-european-court-human-rights/>.

⁴⁰ *Centrum För Rättvisa v. Sweden*, 19 June 2018, application no. 35252/08.

⁴¹ Ira S. Rubinstein, Gregory T. Nojeim, & Ronald D. Lee, *Systematic Government Access to Private-Sector Data: A Comparative Analysis*, in BULK COLLECTION: SYSTEMATIC GOVERNMENT ACCESS TO PRIVATE-SECTOR DATA (eds., Fred H. Cate and James X. Dempsey 2017).

Hungarian surveillance seem to stop in mid-2018, when the Hungarian authorities submitted an action plan.⁴² It is not clear that Hungary has indeed reformed its laws accordingly.

A tour of European Member State surveillance law is relevant for at least three reasons for the question of data localization. First, keeping the information in the EU does not insulate the data from the surveillance of the European Member States' own intelligence services. Second, keeping data in the European Union does not insulate it from data sharing by European intelligence services with the United States.⁴³ Third, if the goal of the GDPR is to assure that the foreign protection is "essentially equivalent" to that available under EU law, it seems fair to ask whether the Member State surveillance law is markedly more protective, if the shoe were on the other foot. Indeed, as other countries model their own data privacy regimes on the EU model, they may also demand that the EU Member States not engage in such surveillance

C. Data Transfers Will Still Occur

Even if the data is stored initially in the EU, there will often be a need to allow access to the data to persons outside the EU. Facebook Europe, for example, will (presumably) permit your friends in the United States to access that data. Similarly, customer service representatives based outside the EU may need to access information about European citizens. It is not clear whether such access across borders constitutes a data transfer subject to the GDPR's Chapter 5, but if they do, and they can be permissible, for example, as "necessary" derogations under GDPR Article 49, it does not insulate that foreign access from U.S. foreign surveillance law. (For the not-for-profit for which Max Schrems is the honorary chair, outsourcing itself seems never "necessary.")

D. The Border Hopping of Internet Routing

Even transmissions between two Europeans might be routed via the United States or other internet infrastructure to which it has access. That is the nature of the internet. Indeed, a few years ago, some suggested Schengen routing to avoid this problem—allowing data to flow only on networks that peered with other networks with physical infrastructure within the Schengen Zone.⁴⁴ But that involves substantial reworking of how the internet operates, and is reminiscent of China's Great Firewall approach to internet traffic, an approach that Russia too

⁴² <https://hudoc.exec.coe.int/eng?i=004-10745>.

⁴³ "[G]overnments routinely share clandestinely intercepted information with each other. The Guardian reports that Australia's intelligence agency collects and shares bulk data of Australian nationals with its partners--the United States, Britain, Canada, and New Zealand (collectively known as the "5-Eyes"). Even while the German government has been a forceful critic of NSA surveillance, the German intelligence service has been described as a "prolific partner" of the NSA. Der Spiegel reports that the German foreign intelligence agency Bundesnachrichtendienst (BND) has been collaborating with the NSA, passing about 500 million pieces of metadata in the month of December 2012 alone. The NSA has collaborated with the effort led by the British intelligence agency Government Communications Headquarters (GCHQ) to hack into Yahoo!'s webchat service to access unencrypted webcam images of millions of users. A German computer expert observes, "We know now that data was intercepted here on a large scale. So limiting traffic to Germany and Europe doesn't look as promising as the government and [Deutsche Telekom] would like you to believe." Anupam Chander & Uyên P. Lê, Data Nationalism, 64 Emory L.J. 677, 716 (2015).

⁴⁴ <https://www.dw.com/en/weighing-a-schengen-zone-for-europes-internet-data/a-17443482>.

is moving towards.⁴⁵ Furthermore, national or regional routing is likely to raise costs for internet access generally. Yet another nations may seek to prevent routing into Germany: “Some of the world’s largest internet exchange points (IXPs) are situated in Germany, thus making the country a central hub for significant portions of the world’s internet traffic.”⁴⁶

III. Why Data Localization Creates Its Own Problems

Not only does it not solve the problem of surveillance, data localization introduces new troubles of its own, as I argue below.

First, data localization is expensive, and its burdens will fall disproportionately on smaller companies. Smaller companies are more likely to not be able to undertake the “mini adequacy reviews” that are now demanded of them if they engage in cross-border data transfers with countries utilizing the standard contractual clauses. They are thus more likely to avoid data transfers at all. Data localization requires companies doing businesses in multiple jurisdictions to localize their infrastructure in multiple jurisdictions, which is likely to be an expensive process. This duplicates infrastructure, and complicates updating and cybersecurity practices.

Second, data localization undermines the goals for increased trade that was at the heart of European data protection law. The GDPR’s predecessor declared that “cross-border flows of personal data are necessary to the expansion of international trade.”⁴⁷ The GDPR’s Recital 101 echoes this goal: “Flows of personal data to and from countries outside the Union and international organisations are necessary for the expansion of international trade and international cooperation.” Data localization lies in tension with the European Union’s own goals of furthering global data flows as a part of promoting both digital and non-digital trade. As then-E.U. Commissioner for Trade Cecilia Malmström stated: “Restrictions on cross-border data flows inhibit trade of all kinds: digital and non-digital, products and services.”⁴⁸ The European Union’s has proposed that the World Trade Organization establish an agreement that would, among other things, not restrict cross-border data flows by “requiring the localization of data in the Member’s territory for storage or processing” (though privacy and data protection would trump this and all other trade disciplines in the EU proposal).⁴⁹

Third, data localization will invite reprisal. Countries that feel the sting of data localization requirements from their trading partners will respond in kind. The European Commission has, for example, complained about India’s plans for data localization in its draft data protection bill: “These data localization requirements appear both unnecessary and

⁴⁵ James Fallows, *The Connection Has Been Reset*, Atlantic (Mar. 2008), <https://www.theatlantic.com/magazine/archive/2008/03/the-connection-has-been-reset/306650/>; <https://www.hrw.org/news/2020/06/18/russia-growing-internet-isolation-control-censorship#>.

⁴⁶ Asaf Lubin, *A New Era of Mass Surveillance is Emerging Across Europe*, JustSecurity, Jan. 9, 2017, <https://www.justsecurity.org/36098/era-mass-surveillance-emerging-europe/>.

⁴⁷ European Union Data Protection Directive recital 56 (1995), Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

⁴⁸ https://trade.ec.europa.eu/doclib/docs/2016/november/tradoc_155094.pdf.

⁴⁹ EU Proposal for Disciplines and Commitments Relating to Electronic Commerce, Inf/Ecom/22, para. 2.7 (April 26, 2019).

potentially harmful as they would create unnecessary costs, difficulties and uncertainties that could hamper business and investments.⁵⁰ The Commission explained,

such an approach will create significant costs for companies – in particular, foreign ones – linked to setting up additional processing/storage facilities, duplicating such infrastructure etc. and is thus likely to have negative effects on trade and investment. If implemented, this kind of provision would also likely hinder data transfers and complicate the facilitation of commercial exchanges, including in the context of EU-India bilateral negotiations on a possible free trade agreement.⁵¹

While it may appear that European companies would not be harmed as there are few large European internet companies, the reality is that almost all companies today collect and manage data. This includes manufacturers, which increasingly connect their hardware to the internet. If Volkswagen is sending back information from its cars to better support its customers around the world, will countries now insist that that information be stored locally? Will countries require Spotify to store its customer playlists and song preferences locally rather than shared “globally with Spotify group companies” as they currently are?⁵² If EU Member State surveillance law, or EU law itself, fails to protect non-EU residents from national intelligence surveillance within Europe, that would be a ground for stopping all data flows to the EU under the logic of *Schrems II*. Many countries have adopted the European data protection regime’s reviews for transfers to third countries; applying these rules, they could determine that EU Member State surveillance laws place their data at too high risk.

Fourth, data localization often undermines, rather than strengthens, cybersecurity. By requiring a company to establish, update, and defend multiple versions of its systems across continents, it opens a bigger attack surface for malicious hackers in the form of additional hardware, additional vendors, and additional employees, while simultaneously decreasing the defenses against attack as updates lag. As the history of U.S. privacy litigation suggests, one of the most common means for the loss of privacy is a security breach. Data localization may well lead to more such breaches. Consider the example offered above by the European Data Protection Board of a corporate group that would prefer to centralize its payment and human resources functions for all its global staff in one office.⁵³ It is easier to ensure that the staff responsible for these sensitive functions is trained and that cybersecurity protocols are followed closely than to replicate that security at a variety of offices.

Fifth, data localization favors some local businesses at the expense of other local businesses. Governments often see data localization as a clear fillip for local enterprise, failing to recognize that, like most protectionist policies, it raises costs for many businesses, while helping a few. In this sense, data localization can function as a kind of own goal, to borrow a sports analogy.⁵⁴ Much of the benefit of data localization for local enterprise accrues to cloud storage businesses, a relatively small part of the economy. Faced with concerns over the

⁵⁰ European Commission, Submission on draft Personal Data Protection Bill of India (2018). <https://eeas.europa.eu/delegations/india/53963/>.

⁵¹ *Id.*

⁵² <https://www.spotify.com/au/legal/privacy-policy/#s8>. Spotify relies on the Standard Contractual Clauses for its transfers outside the EU. *Id.*

⁵³ See *supra* note 22 and accompanying text.

⁵⁴ For an attempt to quantify the costs of data localization, see Martina Ferracane, J. Kren and Erik van der Marel, Do Data Policy Restrictions Impact the Productivity Performance of Firms and Industries?, *Review of International Economics*, Vol. 28, No. 3, pages 676-722 (2020).

relationship between U.S. internet enterprises and the U.S. government, Microsoft in 2015 offered its European customers an alternative: establishing a data trustee in Germany by working with Deutsche Telekom to hold data.⁵⁵ But by 2018, Microsoft decided to not accept any more clients to this arrangement.⁵⁶ Apparently, the cloud service subcontracted with Deutsche Telekom proved both too expensive and of inadequate quality: “High prices and issues with stability, performance and security seem to have resulted in Microsoft pulling the plug.”⁵⁷

Conclusion

Data localization seems, at first glance, to offer an easy fix to the problem of different approaches to privacy across the world. But a closer examination reveals that it is likely to fail to accomplish the goals of avoiding foreign surveillance and protecting privacy. It raises questions of compatibility with most-favored-nations, national treatment and other obligations in the General Agreement on Trade in Services.⁵⁸ And it risks the virtues of the global internet, splintering the web of connections made possible by electronic communications.

⁵⁵ <https://www.telekom.com/en/media/media-information/archive/deutsche-telekom-to-act-as-data-trustee-for-microsoft-cloud-in-germany-362074>.

⁵⁶ <https://docs.microsoft.com/en-us/azure/germany/germany-overview-data-trustee> (“Since August 2018, we have not been accepting new customers or deploying any new features and services into the original Microsoft Cloud Germany locations.”).

⁵⁷ <https://nextcloud.com/blog/microsoft-and-telekom-no-longer-offer-cloud-storage-under-german-jurisdiction/>.

⁵⁸ For a discussion of these issues, see Mira Burri, *The Governance of Data and Data Flows in Trade Agreements: The Pitfalls of Legal Adaptation*, 51 U.C. Davis L. Rev. 65 (2017); Svetlana Yakovleva and Kristina Irion, *The Best of Both Worlds? Free Trade in Services, and EU Law on Privacy and Data Protection*, *European Data Protection Law Review* 2(2): 191-208 (2016); Neha Mishra, *Privacy, Cybersecurity, and GATS Article XIV: A New Frontier for Trade and Internet Regulation?* (February 2, 2019). *World Trade Review* (Forthcoming, 2019), available at SSRN: <https://ssrn.com/abstract=3383684>.