2024

The Trade Origins of Privacy Law

Anupam Chander
Georgetown University Law Center, ac1931@georgetown.edu

This paper can be downloaded free of charge from:
https://scholarship.law.georgetown.edu/facpub/2576
https://ssrn.com/abstract=4714663


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 Intellectual Property Law Commons, International Trade Law Commons, and the Privacy Law Commons
The Addison C. Harris Lecture

The Trade Origins of Privacy Law

ANUPAM CHANDER*

The desire for trade propelled the growth of data privacy law across the world. Countries with strong privacy laws sought to ensure that their citizens’ privacy would not be compromised when their data traveled to other countries. Even before this vaunted Brussels Effect pushed privacy law across the world through the enticement of trade with the European Union, Brussels had to erect privacy law within the Union itself. And as the Union itself expanded, privacy law was a critical condition for accession.

But this coupling of privacy and trade leaves a puzzle: how did the U.S. avoid a comprehensive privacy law yet retain access to trade? The Article explains U.S. exceptionalism as resting on its enormous economic leverage, which enabled it to negotiate sui generis regimes to ensure access to foreign data.

Even those accepting this historical account as account might yet argue that privacy should not be subjected to trade law disciplines. “Privacy is not bananas,” as the great Spiros Simitis famously proclaimed. But food safety is also a human right, and trade law has shown that we can protect human health even when we consume food produced abroad. Similarly, we can protect privacy even while enabling trade in digital services. Trade disciplines need not undermine privacy, but rather help ensure that claims of privacy protection are not merely disguised protectionism.

* Scott K. Ginsburg Professor of Law and Technology, Georgetown University. I want to thank the Indiana Maurer School of Law faculty for the honor of delivering the Addison Harris lecture, a lecture delivered by many of my own teachers. I want to thank in particular Dean Christy Ochoa, Jayanth Krishnan, Asaf Lubin, Shruti Rana, and Deborah Widiss for being superb hosts even during a snowstorm. I am grateful for the excellent research assistance of Daniel CsigirinSZKJ and Andy Yin and very helpful editing by Joe Ledford and the rest of the Indiana Law Journal staff. I also owe an enormous debt to Paul Schwartz, for carefully reviewing a draft, teaching me so much about global privacy law, and for being a mensch at every turn. I have a special connection to Indiana University, Bloomington: my mother, Yash Garg, received her master’s degree in library and information science there. Thus, it was a special honor for me to return to my mother’s alma mater to give a named lecture. I dedicate this lecture to her.
INTRODUCTION

There is a growing fissure between two important values—privacy and trade—which seem to be dividing the world rather than uniting it. I want to suggest that the two are far more intertwined than one might expect. Indeed, I will argue that far from despoiling the human right to privacy with worldly commercial interests, the desire for international trade has propelled privacy law over the last few decades. Privacy law has grown in large part in service of trade. Indeed, it is trade that will likely continue to propel the growth of privacy law over the next few years as well.

In a recent paper, Paul Schwartz and I argue that privacy and trade are currently on a collision course, with a regulatory thicket of differing privacy laws across the world making it harder and harder to trade.\(^1\) Governments worry that foreign jurisdictions may not have the same protections for privacy available at home, and thus increasingly intervene to block the data from flowing to countries they believe lack sufficient protections. In the process, governments are effectively declaring many foreign companies unwelcome because they may transfer personal data to foreign shores that lack adequate protections. Only the largest companies are likely to be able to have the resources to traverse this regulatory thicket.

This framing of trade as a threat to privacy is misleading. In fact, it is belied by the history of the two domains, which show that the desire to enhance trade helped drive privacy protections both across Europe and across the world. Rather than undermining privacy, the economic imperative for commerce across borders has driven the adoption of privacy law over the last four decades.

The article proceeds as follows. Part I motivates the inquiry by describing current privacy/trade conflicts, focusing in particular on the major international controversies over TikTok and Facebook, and then turns back the clock to privacy/trade conflicts from the 1970s and 1980s. Part II shows that concerns over privacy as a constraint on international trade spurred the growth of privacy law across the world. But this leaves a puzzle: if privacy law were essential to promoting

---

international trade, how did the U.S. avoid an omnibus privacy law? Part III recounts early U.S. consideration and rejection of broad privacy bills, and its use of its economic leverage to continue trade flows. Part IV observes the EU’s official effort to insulate data protection from trade law. This adopts the thesis of a famous aphorism from data protection pioneer Spiros Simitis, who argued that privacy was not like bananas. Part V responds to this claim.

I. The Privacy Challenge for Trade

Are privacy and trade in inevitable conflict? Is your data unsafe because it leaves your country? Does trade undermine privacy? That is the premise of many contemporary internet conflicts. I demonstrate these tensions between privacy and trade in contemporary conflicts. I then show that such concerns are hardly new, emerging with the advent of computing itself.

A. Contemporary Challenges from Facebook to TikTok

Privacy concerns are driving rifts in international trade. The conflict between privacy and trade can be seen in recent disputes involving two of the most popular apps in the world, Facebook and TikTok. Both apps have run into trouble because of concerns about insufficient privacy protections as data travels internationally. I have described this as the “dangerous waters theory of the Internet”—it’s unsafe to send your data across the Pacific (to China) or across the Atlantic (to the United States). In other words, it’s unsafe for us to send our data abroad, and unsafe for others to send their data here.

Consider the cross-border data flow travails of Meta Platforms, Inc., the U.S.-based company that runs Facebook, and TikTok, which is owned by ByteDance, a company based in China.

The imposition of the largest data protection fine in European history demonstrates the risks to trade emanating from privacy. In May 2023, the Irish Data Protection Commissioner issued a fine of €1.2 billion (approximately $1.3 billion) against Meta Platforms, Inc.’s Irish subsidiary. Meta’s offense was the transfer of Europeans’ personal data to the United States, where it would not have sufficient protections against the U.S. national intelligence services. (It’s still unclear whether even keeping data in the European Union would avoid the theoretical risk of U.S. surveillance capture. The CLOUD Act, after all, authorizes a judicial process to obtain data held abroad.) This represents a clear impediment to foreign trade, as

companies increasingly must establish data infrastructures within Europe to avoid a similar fate.

Even as Ireland was fining an American company for transferring personal data to the United States, U.S. states were actively seeking to bar the use of an app with origins in China. When Maine became the twenty-eighth state to ban TikTok on state devices, it cited “unspecified risks to the ‘sensitive and confidential data that we are entrusted to protect.’”5 The University of Texas went further than some by banning TikTok from the campus Wi-Fi networks. The University’s technology advisor explained, “TikTok . . . offers this trove of potentially sensitive information to the Chinese government.”6 Of course, some students simply switched to their cellular data plans,7 apparently risking their own privacy and the security of Texas and the country in the process.

The flurry of state bans of TikTok began with South Dakota Governor Kristi L. Noem, who ordered a ban on all state devices on November 29, 2022.8 South Dakota’s PBS and public radio station also deleted their TikTok accounts.9 South Dakota’s tourism department also “deleted its 62,000-follower account showing off the state’s natural beauty.”10 The privacy and security risk of South Dakota’s tourism department’s TikTok seems pretty remote. After all, the Presidents on Mount Rushmore are made of stone.

But the United States is hardly alone in declaring a foreign-owned service to be a threat to privacy or security. Even before Governor Kristi Noem had declared a foreign app illegal, French authorities last November declared it illegal to use Microsoft Office 365 or Google Workspace in French schools.11 In announcing the ban, the French Minister of National Education cited a ruling by the French data

9. Harwell, supra note 5.
10. Id.
protection authority, the Commission Nationale de l’Informatique et des Libertés (CNIL), that recommended that French authorities choose companies that “do not transfer [data] to the United States.” While the official guidance targets the free versions of these services, the rationale extends to all versions, as long as they transfer data to the United States.

France was following the lead of Germany, which in 2019 had banned schools from using an even broader array of cloud services from Google, Microsoft, and Apple. When Denmark implemented a ban on Google services in education in 2022, it created chaos because half of Danish schools used Chromebooks, and they delayed its implementation until later that year to give the schools and cities time to bring processing activities in line with the General Data Protection Regulation (GDPR). Data protection authorities in Austria and Italy, too, have ruled that the use of Google Analytics to understand website use violates EU data protection law because personal data is transferred to the United States for processing.

The European bans flow largely as a consequence of a ruling by the Court of Justice of the European Union in 2020. In a case brought by Max Schrems, the European Court held that the principal mechanisms used by Facebook to transfer data to the United States were illegal under European privacy law.

---

12. “In a letter dated May 27, 2021, the National Commission on Informatics and Liberties (CNIL) recommended that higher education establishments, in the absence of additional measures likely to ensure an adequate level of protection, resort to collaborative suites offered by service providers exclusively subject to European law who host data within the European Union and do not transfer it to the United States.” 16ème Législature Question Écrite N°971 de M. Philippe Latombe, ASSEMBLÉE NATIONALE (Nov. 15, 2022) (my translation), https://questions.assemblee-nationale.fr/q16/16-971QE.htm [https://perma.cc/2764-GSEL].


17. Data Protection Comm’r v. Facebook Ireland Ltd. (Schrems II), Case C-311/18, ECLI:EU:C:2020:559 (July 16, 2020). The issue was so important that when Joe Biden took office on January 21, 2021, he appointed on that day a person to negotiate a new system to transfer data to the U.S. Caitlin Fennessy, Biden Appoints Christopher Hoff to Overseer
The end result is this: If Texan students can’t dance on TikTok, French students can’t use cheap Chromebooks. As these examples show, the dangerous waters theory of the internet undermines the internet’s global nature—it rips apart the World-Wide-Web into Nation-Wide-Webs. From the United States to the European Union, countries are raising alarms about apps and other services that collect personal data with origins in foreign countries.

Even enormous resources may not be enough to meet these alarms, as companies like TikTok are discovering. TikTok has committed $1.5 billion to accomplish a very complicated bifurcation of its company structure, employees, hardware, and software, so that U.S. personal data cannot be accessed from outside the United States except to users elsewhere through the TikTok app itself. It has committed an additional €1.2 billion to doing so in the European Union through Project Clover. Yet, the Biden Administration has apparently warned TikTok and its owner ByteDance that TikTok may be ordered to shutter in the United States unless TikTok is sold to acceptable owners based outside China.

Luckily for U.S. and EU companies transferring data across the Atlantic, the Biden Administration and the European Commission agreed upon a set of U.S. surveillance reforms that led to the restoration in July 2023 of a limited adequacy decision with respect to the United States. Companies adhering to the EU-U.S. Data Privacy Framework can engage in data transfers of personal data of EU persons to the United States. At least for now, Meta does not need its own Project Clover, though it faces other challenges in Europe stemming from its use of personally targeted advertising.

B. Early Privacy/Trade Conflicts

Worries about cross-border data flows are nearly as old as computing itself. Step back to the 1970s. As we’ll see, worries that the need to protect privacy might lead

---


to “data protectionism” can be traced back to as early as 1975. A few cases helped demonstrate the reality of the concerns.

In the late 1970s, a fire alarm in a factory in Malmo, Sweden would trigger an alarm at the local fire brigade. But it would also trigger a message sent via satellite to a General Electric computer in Cleveland, Ohio, which would in turn inform the Malmo fire brigade what it should expect to find in the warehouse when they arrived, allowing them to deploy the appropriate resources and tactics. After some concerns were raised about both network failures and the political risk of this arrangement, the computer server was moved closer to home.

In 1989, Fiat-France sought to consolidate employee information at its headquarters in Turin, Italy. The CNIL, as France’s data protection agency, protested because Italy lacked a national data protection law at the time. To obtain the necessary permissions for data transfer from France, Fiat contractually agreed to provide privacy protections even in Italy. Specifically, Fiat pledged to provide “the protections for human rights and fundamental liberties of the Council of Europe’s privacy convention as well as of the national French data protection law.” In effect, Fiat agreed to abide by French privacy law in Italy.

In 1995, Citibank was launching a credit card with German railway company Deutsche Bahn. The Berlin data protection authority was troubled by the fact that information was to be processed in the United States. Citibank “made headlines” when it entered into an agreement permitting “Germany’s data police to come to the U.S. to inspect its data-processing arrangements.”

As these examples show, conflicts between privacy and trade were well-known even as far back as the 1970s. The risks that privacy rules created for trade were so well-known that policymakers had coined a name for the issue: transborder data flows, with an acronym of “TBDF” or, more often, simply “TDF.” Concerns about how privacy impacted transborder data flows were very much on the international policy agenda especially in the 1980s and beyond.

24. See infra note 95 and accompanying text.


28. PAUL M. SCHWARTZ, MANAGING GLOBAL DATA PRIVACY: CROSS-BORDER INFORMATION FLOWS IN A NETWORKED ENVIRONMENT 11 (2009). Once the two Fiat entities signed the appropriate contract, and showed it to the CNIL, the French data protection agency gave them its formal approval, which was marked by a “receipt” (récépisse) that allowed the transfer. Id.

II. How Trade Spurred Privacy

There was a simple and elegant solution to the privacy challenge for trade. If a country with privacy law was reluctant to see its citizens’ data go abroad to less well-regulated zones, then why not simply introduce privacy law to those domains? The birthplace of European privacy law is the German state of Hesse, which enacted the first data protection law in the world in 1970. It would not take long for policymakers to begin worrying about how the absence of data privacy laws or variation in such laws would frustrate trade. On June 14, 1972, the Council of Europe’s committee on the protection of privacy against electronic data banks issued its preliminary recommendations. The recommendations began with recitals noting that “the objective of the Council of Europe is closer union among its member States” and encouraged member states “to take measures designed to avoid new discrepancies between the legal systems of member States in this matter.” Accordingly, they set out basic principles of data protection. The recommendations noted “the possible drafting of an international agreement.” On September 26, 1973, the Council of Europe’s Committee of Ministers adopted the recommendations.

A. The International Privacy/Trade Formula

Concern about the interruption of trade due to regulatory gaps in privacy proved a key motivation for all of the international privacy instruments entered into in the 1980s and the 1990s. Let’s begin with the first of these instruments. In 1980, the Organization of Economic Co-operation and Development (OECD) adopted the Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data (“Guidelines”). The OECD expert group that wrote the Guidelines was chaired by the Australian Michael Kirby, who served as a justice of the High Court of Australia.

Insight into Justice Kirby’s own approach can be found by reviewing an article he wrote in 1980 in the Stanford Journal of International Law. Like Jan Freese before him, Justice Kirby anticipated the essential contours of the arguments that would follow over the next half century. He began by observing that some countries were adopting data privacy laws. However, he observed, “Protective legislation in one

31. STAFF OF S. COMM. ON GOV’T OPERATIONS, 93D CONG., PRIVACY AND PROTECTION OF PERSONAL INFORMATION IN EUROPE: PRIVACY DEVELOPMENTS IN EUROPE AND THEIR IMPLICATIONS FOR UNITED STATES POLICY 399–400 (Comm. Print 1975), https://hdl.handle.net/2027/uc1.a0003956273 [https://perma.cc/M68M-WV4U]. At this time, the term “data bank” was often used to refer to what we now call a “database.”
32. Id. at 400.
33. Id.
34. Council of Europe Committee of Ministers, Resolution 73 (22) On the Protection of the Privacy of Individuals vis-à-vis Electronic Data Banks in the Private Sector, COUNCIL OF EUROPE, https://rm.coe.int/1680502830 [https://perma.cc/RB8P-87DU].
country could be readily circumvented by storing data across the border beyond the jurisdictional control of privacy laws where they would be subject to easy retrieval via international telecommunications systems . . . .” 35 At the same time, he noted the possibility of “data protectionism.” That is, “[l]egislation, nominally for the purpose of data protection, could actually have such objectives as the protection of domestic . . . industries . . . .” 36 “In order to avoid unnecessary restrictions on transborder data flow, it will be imperative to agree upon international standards for privacy legislation.” 37 Justice Kirby concluded by arguing for achieving a “proper balance between flows of information and the legitimate protection of individual privacy . . . .” 38

The OECD Guidelines offered a solution to the problem Justice Kirby had so insightfully identified. The Guidelines were built on two cornerstones:

- First, a commitment to a set of fundamental data privacy protections in national law. 39
- Second, an agreement to permit flows of data to other countries, unless they didn’t protect data privacy in accordance with those fundamental privacy rules. 40

The first cornerstone would lay the foundation of globalizing privacy law. The second cornerstone would lay the foundation for trade. Thus, an international agreement to protect privacy simultaneously served multiple purposes, as Justice Kirby recognized. The first cornerstone sought to avoid the regulatory evasion sought by those who would move data overseas to less regulated jurisdictions. 31 As Justice Kirby noted, “Protective legislation in one country could be readily circumvented by storing data across the border beyond the jurisdictional control of privacy laws where they would be subject to easy retrieval via international telecommunications systems . . . .” 42 An international agreement would respond to this concern by ratcheting up the privacy standards in those overseas jurisdictions. There would be little need to establish barriers to data flows in order to ensure data protection because data would be safe if it traveled abroad. The second cornerstone sought to prevent countries from blocking data flows for reasons of protectionism. Justice Kirby observed that some worried about “‘data protectionism,’” and argued that “an international standard might reduce or discourage the adoption of national

35. Michael D. Kirby, Transborder Data Flows and the “Basic Rules” of Data Privacy, 16 STAN. J. INT’L L. 27, 28 (1980). He argued that “unintended disparities in the law of friendly nations could create adverse effects on the free flow of data between countries.” Id. And he offered a solution: “The adoption at an international level of agreed principles might help to promote harmonization or standardization of laws.” Id.
36. Id.
37. Id. at 27.
38. Id. at 66.
40. See id. at art. 17.
42. Kirby, supra note 35, at 28.
legislation that imposes an artificial barrier on the free flow of information."  

Reflecting on the OECD Guidelines thirty years later, Justice Kirby noted, “One does not normally think of the Organisation for Economic Co-operation and Development (OECD) as a major player in the global elaboration of human rights.” Privacy is recognized as a human right in international law instruments. Given the EU’s focus on improving the economic lives of people, many might be surprised to see its role here in promoting a noneconomic human right. Justice Kirby explained the OECD’s intervention: “the important human right that was at stake was shown to have significant economic implications, deserving the attention of the OECD.”

Of course, the Guidelines were just that—guidelines, rather than enforceable hard law—but its privacy/trade formula would be replicated again and again, including in European law as we shall see. This formula would form the basic architecture of international privacy law beginning with the Council of Europe’s Convention 108. In 1981, the Council of Europe opened for signature its Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, the so-called “Convention 108.” The explanatory report for Convention 108 observed that some “data users might seek to avoid data protection controls by moving their operations, in whole or in part, to ‘data havens’, i.e. countries which have less strict data protection laws, or none at all.” At the same time, the report worried that “a license for export” of data would interfere with the “free international flow of information.” In other words, businesses could exploit a race to the bottom by supplying services from “data havens.” Governments would accordingly respond by requiring licenses for data export, a cumbersome solution that would interfere with the benefits of the flow of information across borders. Convention 108 offered a solution to the data haven/license to export dilemma. Countries would sign up to the Convention standards, thereby avoiding a race to the bottom, obviating any need for other countries to impose licenses for export. But Convention 108 was intended to harmonize laws within the member states of the Council of Europe and was not

43. Id.
46. OECD, supra note 44, at 8.
49. Id.
actively promoted as an international standard until 2008. To this day, it only counts nine member states outside the Council of Europe member states.

B. Creating a European Single Market

A closer examination of the European Union’s regional data protection law as well as the process of EU expansion shows the critical role of trade in promoting privacy. This connection can be seen in the growth of privacy law within the European Union itself, the requirement for countries joining the European Union in various phases of enlargement, and the determination that the legal protections in non-EU states are “adequate” for purposes of EU data protection law.

1. Expanding Privacy Within the EU

The EU recognized that a link between privacy and trade was essential to its goal of a single market across the EU. Both the Data Protection Directive and the GDPR thus declare that data protection cannot be used as a basis for interfering with trade, at least within the European Union. This linkage of privacy to trade embedded in European Union law is possible because the Directive and the GDPR establish EU-wide privacy law such that privacy rules travel with the data across the EU. Thus, linking the two does not render privacy subservient to trade—except to the extent that an individual member state or subnational jurisdiction cannot demand stricter privacy protections than provided in European Union law. Desire for trade with the European Union has also led many other states to establish or strengthen their data privacy law, often modeling it on the Data Protection Directive or, more recently,


53. In its very first article, the GDPR embraces the free movement of personal data no less than twice when declaring its objectives and makes clear that privacy cannot be used to block personal data flows within the EU:

1. This Regulation lays down rules relating to the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data.

3. The free movement of personal data within the Union shall be neither restricted nor prohibited for reasons connected with the protection of natural persons with regard to the processing of personal data.

Id. at 32 (emphasis added).
the GDPR. Indeed, Anu Bradford cites data protection as one of the most prominent examples of the Brussels Effect in action. Japan, for example, strengthened its privacy law in order to meet the European Union’s requirements for being recognized as adequate according to European data protection law.

We can see the privacy-trade link imprinted directly into the landmark directive on data protection in 1995, the progenitor of today’s GDPR. While we know that 1995 directive using its short form, the “Data Protection Directive,” its official title reads as follows: “Directive 95/46/EC . . . on the protection of individuals with regard to the processing of personal data and on the free movement of such data.” This title situates “the free movement of such data” as a twin goal alongside data protection itself. Furthermore, this trade facilitative goal is operationalized in the very first article of the Directive:

1. In accordance with this Directive, Member States shall protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data.
2. Member States shall neither restrict nor prohibit the free flow of personal data between Member States for reasons connected with the protection afforded under paragraph 1.

The very first article of the Directive thus prohibits EU states from applying data protection law in a manner that restricts the free flow of personal data. The European Union recognized that in order to create a single market, it would be necessary to permit data to flow across that market—to facilitate routine activities such as human resources management, customer management, fraud detection, and payments. The free flow of personal data across borders facilitates trade within the EU—permitting service providers to provide services across the EU, companies to gather data from customers elsewhere within the EU, and processing of that data by companies across the Union. The first article of the Directive thus disciplines data protection law, ensuring that it is not used to thwart trade within the Union. The Directive explains that this does not diminish privacy or other individual rights: “given the equivalent protection resulting from the approximation of national laws, the Member States will no longer be able to inhibit the free movement between them of personal data on grounds relating to protection of the rights and freedoms of individuals, and in particular the right to privacy. . . .”

56. Chander & Schwartz, supra note 54.
58. Id.
59. Id. at art. 1 (emphasis added).
60. Id. at recital 9.
The GDPR continues to embrace this framework connecting privacy and trade. As with the Data Protection Directive, the “free movement of such data” is literally in the official title of the GDPR. The full title reads: “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 (General Data Protection Regulation).”\(^{61}\) In its very first article, the GDPR embraces the free movement of personal data no less than twice when declaring its objectives. The first article declares that privacy cannot be used to block personal data flows within the EU:

1. This Regulation lays down rules relating to the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data . . .
2. The free movement of personal data within the Union shall be neither restricted nor prohibited for reasons connected with the protection of natural persons with regard to the processing of personal data.\(^{62}\)

And indeed, bringing privacy law to all corners of the European Union was a critical part of creating a single market in Europe. So far from a story of a unified Europe, with a strong legal commitment to privacy as a fundamental right arising out of a shared history, we instead see various European states adopting privacy laws at different speeds—many spurred by the desire to integrate their economies with the other economies of Europe and to benefit from the increased trade that offered. Many of the countries—including Portugal, Belgium, Spain, Italy, and Greece—only established national comprehensive data protection laws after the EU began negotiating toward what would become the Data Protection Directive.\(^{63}\)

---

62. Id. at art. 1 (emphasis added).
63. In fact, in January 2000, the European Commission took France, Luxembourg, the Netherlands, Germany, and Ireland to the European Court of Justice for failure to notify all the measures necessary to implement the Data Protection Directive. European Commission Press Release IP/00/10, Data Protection: Commission Takes Five Member States to Court (Jan. 11, 2000); Andrew Charlesworth, Information Privacy Law in the European Union: E Pluribus Unum or Ex Uno Plures?, 54 HASTINGS L.J. 931, 937 (2003).
Not only did EU membership spur the adoption of comprehensive data protection law, it also required member states to ensure that any existing law met the EU standard. This required active vigilance by the Commission. In 2000, the European Commission sued France, Luxembourg, the Netherlands, Germany, and Ireland for failing to notify all the measures necessary to implement the Data Protection Directive.65


65. See European Commission Press Release IP/00/10, supra note 63; Charlesworth, supra note 63.
2. Expanding Privacy to the EU’s New States

As the EU pushed eastward after 1995, bringing in new member states, the new member states, too, adopted comprehensive privacy laws in order to be able to trade freely with the rich markets of Western Europe. As we will see, data protection was a key requirement for accession to the free trade offered by the European Union. Thus, data protection law expanded, along with the European Union itself. I examine below more closely the trajectory of some of the states that joined the EU after 1995.66

Figure 2

THE EXPANSION OF NATIONAL PRIVACY LAW WITHIN EUROPE, 1996-

The first Polish comprehensive data privacy law was enacted in 1997 and, in a footnote to its title, explicitly declared that it would be subject to the EU’s Data Protection Directive, which had just been approved two years earlier.68 Poland would become an EU member state in 2004.69

Accession to the European Union was contingent on aligning the candidate state laws with the European Union law already in place, which is called the "acquis."70


69. See European Commission Press Release IP/00/10, supra note 63.

70. European Neighborhood Policy and Enlargement Negotiations (DG NEAR), EUR.
Part of that *acquis* was, of course, the data protection law of the Union. The European Commission’s 2004 progress report on Bulgaria’s progress toward EU accession shows this process in action. The report finds that further improvements must be made in Bulgaria’s data protection law to meet the EU’s standards.\(^1\) Specifically, the report concludes:

> The Law on data protection is not yet fully in line with the *acquis*, notably because its structure and the definitions and criteria it introduces are in many cases different from those of the *acquis*. Steps for further alignment should be taken. A Commission for personal data protection was set up in 2002 which meets the requirement of independence but needs greater capacity in terms of human resources, budget and premises.\(^2\)

But the overall assessment part of the report struck a somewhat different tone, at least with regard to the formal law:

> Bulgaria has largely completed its legislative alignment in the area of data protection, including the use of personal data by the police. However, practical difficulties in applying the new rules suggest that further amendments to the Law on Protection of Personal Data are needed to ensure proper implementation of the *acquis*. The Commission for Personal Data Protection (CPDP) cannot yet be considered as operational and needs to be strengthened. It currently employs 15 persons and lacks suitable premises, training and equipment. Further efforts are required in order to make it fully operational. Suitable premises should be allocated as a matter of priority. Bulgaria also needs to continue to strengthen the security unit in the Ministry of Interior.\(^3\)

Both of these passages show that not only was the European Union focused on the formal law in assessing readiness for accession, but also the capacity of Bulgarian institutions to enforce this law.

A similar 2004 report on Romania’s progress also suggested improvements in data protection law. The Commission concluded that Romanian data law “should be fully aligned with the *acquis* and efforts should increase to create the necessary administrative capacity, to strengthen enforcement and to raise the level of public awareness in this area.”\(^4\) Overall, the focus was on implementation, not the law itself:

---


\(^2\) Id. at 54.

\(^3\) Id. at 120.

As regards the protection of personal data, the major pieces of legislation are already in place. However, progress in implementing personal data protection rules has only been limited. There are grounds for concern regarding the enforcement of these rules: enforcement activities are far below levels in current Member States and additional posts have not been filled during the reporting period.  

In the overall assessment, however, the Commission seemed to find fault with the formal law, stating that, “In addition, the data protection legislation should be further aligned.”

The accession reports also suggest a significant shift in the European Union’s own thinking about the role of data protection within the regional integration system. The European Union’s accession reports long framed data protection within the chapter on the “Freedom to provide services”—demonstrating the trade imperative at play. More recently, however, data protection has been considered within the fundamental rights section of the report. For example, while the 2004 accession report for Romania considered data protection within “Chapter 3: Freedom to provide services,” the 2022 accession report for Bosnia and Herzegovina fixes the consideration of data protection firmly within “Chapter 23: Judiciary and fundamental rights.” A possible explanation is the influence of the Charter of Fundamental Rights of the European Union, which was declared in 2000 and came into force in 2009. Article 8 declared the protection of personal data a fundamental right as part of European Union law. The first accession report on Croatia in 2005 notes that “These [constitutional] principles [of the consolidated Treaty of European Union] were emphasised in the Charter of Fundamental Rights of the European Union that was proclaimed at the Nice European Council in December 2000.”

These examples show how membership in the European Union served to catalyze privacy law and enforcement across the candidate states. In order to benefit from the trade and other privileges of European Union membership, Bulgaria and Romania, for example, had to bring their data protection law in line with European Union standards.

75. **Id.** at 61.
76. **Id.** at 126.
77. I’m grateful to my research assistant Andy Yin for this nice insight.
78. Romania Report, supra note 74, at 59.
This same dynamic would prove true of European member state’s own data privacy law, regarded as among the strictest in the world.

3. Expanding Privacy Across the World

The framers of the Data Privacy Directive were not only concerned about the free movement of data within the European Union; they understood its importance between the European Union and the outside world as well. The Directive declares that “cross-border flows of personal data are necessary to the expansion of international trade.”\(^{83}\) It goes on to say that data protection should not stand in the way of such flows, at least to countries that have an adequate degree of data protection in place: “[T]he protection of individuals guaranteed in the Community by this Directive does not stand in the way of transfers of personal data to third countries which ensure an adequate level of protection.”\(^{84}\) For those countries that do not have such laws in place, the Directive provides alternative paths to safeguard the data: “[P]articular measures may be taken to compensate for the lack of protection in a third country in cases where the controller offers appropriate safeguards.” The European Union in fact innovates numerous paths for trusted transfers. The GDPR expanded on the set of mechanisms first offered in the Data Protection Directive, adding certifications and codes of conduct and formalizing binding corporate rules as a legal basis for international data transfers.\(^{85}\) “Data Free Flow with Trust” was thus an established European practice before it was named by Prime Minister Shinzo Abe.\(^{86}\)

The EU has, at times, pressed for privacy protections in its trade partners through its free trade agreements. As Mira Burri notes, “The EU has also pushed for more safeguards, requiring its partners to adopt appropriate measures to ensure the privacy protection while allowing the free movement of data, establishing a criterion of ‘equivalence.’”\(^{87}\) Take, for example, the 2002 EU-Chile FTA.\(^{88}\) The data protection provision, Article 30, can be found under title I, on “Economic Cooperation”:

84. Id.
85. Id. at recital 59; see Transferring Data from the EU: Privacy Shield and Data Transfers Under the GDPR, ALSTON & BIRD LLP 1, https://www.alston.com/files/docs/Roadmap-to-the-GDPR-International-Data-Transfers.pdf [https://perma.cc/H2K6-RJYS].
88. Agreement Establishing an Association Between the European Community and Its Member States and Chile, art. 30, Dec. 30, 2022, EUR. CMTY. [hereinafter EU-Chile Association Agreement].
Article 30 Data protection
1. The Parties agree to cooperate on the protection of personal data in order to improve the level of protection and avoid obstacles to trade that requires transfers of personal data.  

This provision commits the parties to cooperate on the protection of personal data, in part, to “avoid obstacles to trade that requires transfers of personal data.” A later article, also titled “Data Protection” but under Part 5, on “Final Provisions,” requires each party to provide “a high level of protection to the processing of personal and other data, compatible with the highest international standards.” Finally, the agreement repeats the General Agreement on Trade in Services (GATS) exceptions verbatim, including their nondiscrimination and other conditions.

Thus, we see the European Union using the promise of increased trade—within the Union and beyond—to promote privacy law. Indeed, it is this hope that propels European Union law to become the de facto legal standard for data protection across much of the world.

III. U.S. EXCEPTIONALISM

One critical participant in global trade, the United States, proved a holdout with respect to a comprehensive national privacy law regulating the private sector. But yet it managed to participate in international trade nonetheless. How did the U.S. manage to ensure trade for its enterprises without adopting a broad privacy law?

It is important to recognize that the U.S. failure to enact comprehensive private sector privacy law was not for lack of effort, as the following history demonstrates. In 1975, a U.S. Senate committee led by Senator Sam Ervin, Jr. visited Europe to study the development of privacy protections there, with a focus on implications for the United States. Its report explained the emerging laws in certain European states, with Senator Ervin crediting “a dynamic effort in Europe . . . to master the challenge of automation technology.” The report noted the possible barrier to trade raised by data protection law. Among the witnesses they met was Jan Freese, then head of the Swedish Data Inspection Board and a data protection pioneer. Even in 1975, Freese sounded a worry about the trade implications of “data protectionism,” observing that “[d]ata protectionism may be a growing theme.” He explained that this would “curtail now unrestricted transborder flows of personal information.” He observed that the Swedish Data Act “authorizes the Board to impose controls over exportation of personal data.”

---

89. Id.
90. Id.
91. Id. at art. 202.
92. Id. at art. 135.
93. Bradford, supra note 55, at 168 (“The EU’s requirement for ‘adequacy’ as a condition for international data transfers has given additional impetus for foreign governments to emulate the GDPR.”). Paul Schwartz argues that “the world follow’s the EU’s lead in this area” because the EU exercised the negotiating leverage offered by adequacy in a flexible manner. Paul M. Schwartz, Global Data Privacy: The EU Way, 94 N.Y.U. L. REV. 771, 773 (2019).
95. Id. at 22.
of personal data, especially prevalent in commercial organizations, and this is becoming more necessary in the absence of multi-national agreements to maintain coming high standards of information integrity. Freese, here, outlined both the problem—restrictions on information flows due to a lack of data protections elsewhere—and the solution—an international treaty upholding data protection standards.

Some within the U.S. Congress, including Senator Ervin, sought to embrace a key component of the emerging European approach to privacy—a data privacy regulator. Such a regulator was proposed as early as 1974. That year, Senator Ervin proposed a bill that would have created a Federal Privacy Board to govern federal and state agencies, as well as “other organizations,” with limits on the collection, maintenance, and dissemination of personal information. Strikingly, the bill also proposed a kind of proto-adequacy regime, permitting personal information to be transferred outside the United States only with “specific authorization from the data subject” or “pursuant to a treaty or executive agreement in force guaranteeing that any foreign government or organization receiving personal information will comply with the applicable provisions of this Act with respect to such information.” The final text of what would become the Privacy Act of 1974, however, limited itself to government collection and handling of personal information and had no limitations on cross-border data transfer.

Again, in 1977, Ed Koch, then a Democratic Congressman from New York, and Barry Goldwater, then an Arizona Republican Congressman, sponsored a bill to establish a Federal Privacy Board to promulgate model privacy protection procedures for public and private entities. That same year, Representative Silvio Conte, a Republican from Massachusetts, proposed the Comprehensive Right to Privacy Act, which would go further and impose a robust set of obligations for both public and private sector organizations that maintained a personal information system. The bill would have offered a private right of action and permitted states to establish privacy laws only if they were stricter than the federal standard. Bills to establish a federal privacy commission would continue to be introduced throughout the 1980s and 1990s but would fail to advance.

96. Id.
99. Federal Information and Privacy Board Act, H.R. 9986, 95th Cong. (1977). Koch and Goldwater had both served on the Privacy Protection Study Commission, which had recommended such a board.
recommended a national Privacy Protection Board in his National Performance Review in 1993.\textsuperscript{102}

Why did these efforts to establish a substantial federal privacy supervision system in the United States fail? One reality is that they failed to win widespread business support. Many U.S. businesses watched with “trepidation” as the Data Protection Directive wound its way through the European Union’s policy process, as Priscilla Regan describes.\textsuperscript{103} Some American businesses did support the establishment of a data privacy commission at home but failed to carry the day. Ultimately, most American businesses chose “to lobby abroad rather than to lobby for change in legislation at home.”\textsuperscript{104}

Instead of enacting a broad privacy law, the United States found itself negotiating with the European Union for an adequacy decision, again and again, now employing private commitments backed by public enforcement as the data protection mechanism. The first such decision followed the Safe Harbor adopted in 2000; the second, after the Privacy Shield adopted in 2016; and the third, after the EU-U.S. Data Privacy Framework. As Paul Schwartz notes, the European Union was keen to continue trade with the United States, giving the United States leverage in these negotiations: “In light of the EU’s goal of promoting successful external trade for its single market bloc of member states, the United States represents its most valuable economic relationship.”\textsuperscript{105}

The end result was this: U.S. businesses and politicians would leverage U.S. negotiating power for access to foreign markets, rather than seeking to offer assurance to foreigners that their data would be well-protected in the United States through robust private sector privacy laws.

IV. EU EXCEPTIONALISM

Recently, the European Union has introduced into its trade agreements a prohibition on trade law challenges to any measures based on data protection. Thus, EU member states can violate their trade law obligations to the foreign trade partner if the EU member states assert that the violation is based on data protection. This goes beyond the escape valve built into the GATS framework—which states that countries can violate their trade law commitments, but only when justified and non-discriminatory. (As Paul Schwartz and I show, that GATS framework was in fact the invention of the European Union.\textsuperscript{106}) The European Union’s goal is to place the data protection regime above the trade regime—and to insulate any decisions ostensibly

Simon introduced the Privacy Protection Act of 1993, which would have established a five-person Privacy Protection Commission, with no more than fifty employees. Privacy Protection p9 Reporting Reform Act of 1994, S. 783, 103d Cong. (1993); 140 CONG. REC. 9176–77 (May 4, 1994).


104. Id.

105. Schwartz, supra note 105, 804–05.

106. See Chander & Schwartz, supra note 1, at 69.
based on data protection from review in the trade law regime. Within the European Union, as we have seen, the prohibition runs precisely the other way—a prohibition of the use of data protection to interfere with trade within the European Union.

The mechanism for this insulation is what is known as the “horizontal provisions” to be included in any future EU trade agreement. The provisions are to be found in model clauses for trade agreements published by the European Commission in 2018. They bar data localization obligations by any country. However, according to the European Data Protection Supervisor, they also “ensur[e] that trade agreements cannot be used to challenge the high level of protection guaranteed by the Charter of Fundamental Rights of the EU and the EU legislation on the protection of personal data.” Article B(2) in these horizontal provisions states:

Each Party may adopt and maintain the safeguards it deems appropriate to ensure the protection of personal data and privacy, including through the adoption and application of rules for the cross-border transfer of personal data. Nothing in this agreement shall affect the protection of personal data and privacy afforded by the Parties’ respective safeguards.

By giving each party the right to maintain the personal data transfer rules “it deems appropriate,” the horizontal provisions seem to reduce opportunities to challenge measures interfering with trade that a party declares to advance data protection.

V. Of Privacy and Bananas

The prior discussion helps demonstrate the long and deep association between privacy and trade. But should there be an official, justiciable link? Specifically, should trade law have anything to say about assertions of privacy that conflict with trade?

Some argue that privacy cannot be considered within trade law because that would subject a human right to an economic regime. Privacy is a superior value to trade, and therefore should not be considered within a trade framework, this argument goes. “This is not bananas we are talking about,” as the great European privacy scholar Spiros Simitis famously declared.

And indeed, the flow of personal data across borders is different than the flow of bananas across oceans. As Svetlana Yakovleva and Kristina Irion observe, “Personal

---


data is peculiar in the way it combines the dignity of a human being with economic properties valuable for commercial activity."  


111. The relevant WTO agreement on food safety encourages states to adopt international standards for food safety, where available, and permits nations to adopt stricter standards as long as they are scientifically justified. Agreement on the Application of Sanitary and Phytosanitary Measures, art. 3.1, 5, April 15, 1994, 1867 U.N.T.S. 493 [hereinafter SPS Agreement].

112. The call for a New International Economic Order was designed to respond to precisely this concern.

would be denied [critical] opportunities . . . .”

Fourth, bananas have in fact been subject to WTO dispute settlement, suggesting how the system would in fact deal with privacy claims. Even as Simitis made the remark denying privacy’s susceptibility to being subject to rules made for bananas, the WTO was considering claims by Latin American nations that the EU’s banana import regime improperly discriminated between countries based on colonial ties—a dispute that would finally be settled in 2009 with the EU’s reform of its banana import system. In that case, Latin American countries complained that the EU violated its trade commitments by favoring its former colonies, an explicitly discriminatory regime that the EU had not negotiated to protect when the WTO was created. This suggests a critical role for trade law—repudiating the use of domestic law to effectively discriminate against certain countries while favoring other countries when not justified by legitimate goals such as food safety or data privacy. Some scholars have noted the possibility that current EU data privacy practices, especially with respect to adequacy findings, might not fare well in a discrimination complaint brought under GATS. Irion, Yakovleva, and Bartl argue, “Demonstrating the required ‘consistency of enforcement’ could be a challenge for the EU, in particular with a view to administering and adopting adequacy decisions by the Commission.” Mira Burri observes, “[I]t can well be maintained that there are less trade restrictive measures that are reasonably available for achieving the EU’s desired level of data protection.” Rolf Weber and Dominic Staiger have noted that “the inconsistent application of third country transfer provisions may violate the chapeau, for example, when a third country is denied the same framework as is present under the Privacy Shield.” As Paul Schwartz and I note, “For example, this test would require that a GATS signatory did not single out one state for tougher application of extraterritorial provisions found in its data privacy law. Thus, the privacy exception is limited by a requirement that it not be disguised protectionism or favoritism.”

There are yet additional reasons to link privacy and trade that go beyond the bananas comparison.

Fifth, as shown in Part II above, linking privacy and trade is precisely what the European Union did in establishing the European Union itself as a single market.

Sixth, privacy is increasingly negotiated alongside trade, even by the European Union. As Paul Schwartz and I have observed, “The EU-Japan adequacy agreement was negotiated in tandem with negotiations for the EU-Japan Economic Partnership

114. Chander & Schwartz, supra note 1, at 108.
118. ROLF H. WEBER & DOMINIC STAIGER, TRANS ATLANTIC DATA PROTECTION IN PRACTICE 59 (2017).
119. Chander & Schwartz, supra note 1, at 59.
120. See supra Section II.B.
Agreement. The Commission adopted the adequacy decision on January 23, 2019, and the Economic Partnership Agreement on February 1, 2019, in a one-two demonstration of syncing up the two matters.\footnote{121} Data flows are a necessary component of opening up trade. Indeed, the European Union recognizes this implicitly: when announcing the Japanese mutual adequacy arrangement, the Commission heralded the economic benefits, including “privileged access [for European companies] to the 127 million Japanese consumers.”\footnote{122}

Seventh, privacy can support trade. The more we trust that the trade will benefit us, the more likely we are to engage in it. Data privacy thus helps ensure that personal data can be shared across borders. This is a central goal of EU data protection law, which seeks to ensure that data can be sent abroad safely, both within the Union and beyond it.

Eighth and finally, data privacy can be enhanced by trade. Just as keeping money in the bank is generally safer than keeping money under the mattress, storing data in world class systems is often safer than keeping that data on one’s bedroom computer.\footnote{123}

In a response to Paul Schwartz’s and my paper, Privacy and/or Trade, the scholars Kristina Irion, Margot Kaminski, and Svetlana Yakovleva argue that trade and privacy should not be part of the same regime. They argue that the “trade law regime . . . is by its very nature antithetical (or at least antagonistic) to data privacy law.”\footnote{124} Any effort to combine regimes “will treat data privacy as an instrument to promote trade, rather than as a human right and a societal value.”\footnote{125} Their basic worry is that privacy will suffer if connected to trade.

These scholars raise important points, and their paper is well argued, but I believe it is not ultimately persuasive. Trade disciplines are not designed to undermine consumer protection, but to target protectionism. One would not say that trade law, which, among other things governs trade in food and goods, is antithetical to safe food or safe goods. Each state has a right to insist on food safety, even within a free trade regime. Irion, Kaminski, and Yakovleva also write that “the FTAs are not themselves charged with the heavy lifting of constituting data privacy. Instead, they simply label data privacy laws as barriers to digital trade and digital protectionism.”\footnote{126} But no trade agreement treats privacy laws as inherent barriers to trade or inevitably protectionist. The U.S.-led renegotiated NAFTA text (now the United States-Mexico-Canada Agreement) even requires each country to protect privacy: “each Party shall adopt or maintain a legal framework that provides for the protection of the personal information of the users of digital trade.”\footnote{127} Irion,

\footnote{121. Id. at 92–93.}
\footnote{122. Id. at 93 (quoting Press Release, the European Union and Japan Agreed to Create the World’s Largest Area of Safe Data Flows, EUR. COMM’N (July 17, 2018)).}
\footnote{123. Anupam Chander & Uyên P. Lê, Data Nationalism, 64 EMORY L.J. 677 (2015).}
\footnote{125. Id.}
\footnote{126. Id.}
\footnote{127. United States-Mexico-Canada art. 19.8, July 1, 2020, Off. U.S. Trade Representative
Kaminski, and Yakovleva argue, “The framing of data flows in economic terms puts other values implicated by data flows in a subordinated position, wherein these other values have to be balanced against the primary goal of trade liberalization.”\textsuperscript{128} As I have argued above, a privacy-trade regime need not subordinate privacy. Irion, Kaminski, and Yakovleva also suggest that trade agreements seek to “strike the balance between liberalizing data flows and human rights.”\textsuperscript{129} This treats data flows as fundamentally at odds with human rights, but it is not clear why that need be so. It is possible to permit data flows while respecting human rights—which is precisely one of the theoretical goals of the European data protection regime. In regard to personal data, “[t]he free movement of such data” is literally in the title of the original European international data protection regime, as indicated earlier.\textsuperscript{130}

Of course, whether including privacy in trade law enhances privacy depends on the details of the linkage. If the linkage requires that a country accept a lower level of privacy than it would otherwise require, that would undermine privacy. For bananas, food safety rules can be based on objective science, though the level of acceptable risk itself is not a question that science can answer. For privacy, there may be objective standards for achieving certain goals,\textsuperscript{131} but the goals themselves are not ascertainable through objective methods alone.

\textbf{CONCLUSION}

Let’s return to the TikTok bans and the various European bans, from Google to Apple to Microsoft.\textsuperscript{132} They help shed light on different approaches to the two privacy-trade cornerstones described above. The U.S. formula toward privacy and trade has adopted only one of the two cornerstones—a commitment to the free flow of data, but not a binding commitment to a robust set of privacy protections. The U.S. formula thus far has not been enough. It simply seeks to remove the protections against data flows, without ensuring that privacy will be sufficiently protected. The TikTok bans, however, represent a retreat from that free flow of data. It thus provides neither the trade benefits of free flow of data—at least with respect to the world’s second largest economy—nor comprehensive privacy protections vis-à-vis the private sector. By contrast, the EU formula toward privacy and trade includes strong privacy protections but has only a weak commitment to the free flow of data.

Despite these recent controversies, history shows that trade and privacy have reinforced each other, and can continue to do so.

\textsuperscript{128} Irion et al., \textit{supra} note 124.
\textsuperscript{129} \textit{Id.}
\textsuperscript{130} See Data Protection Directive, \textit{supra} note 57 and accompanying text.
\textsuperscript{132} See \textit{supra} notes 2–13 and accompany text.