Privacy Peg, Trade Hole: Why We (Still) Shouldn't Put Data Privacy in Trade Law

Irion, K.; Kaminski, M.E.; Yakovleva, S.

Publication date
2023

Document Version
Final published version

The University of Chicago Law Review Online

POST

Privacy Peg, Trade Hole: Why We (Still) Shouldn't Put Data Privacy in Trade Law

Kristina Irion, Margot E. Kaminski & Svetlana Yakovleva [1]

* * *

A Response to Profs. Anupam Chander & Paul Schwartz's Privacy and/or Trade.

Introduction

Data privacy, it turns out, is still not bananas.

Some principles are not well suited for negotiation through the international trade regime. Or rather, the international trade regime has never been the right forum for negotiating or enforcing human rights. The World Trade Organization's (WTO's) current approach to data privacy law both instantiates and illustrates this: it brackets data privacy as something trade law cannot well address, while illustrating the ways in which trade law superimposes its prioritization of trade liberalization atop other public values.

Trade's core framing prioritizes economic over human rights values. That is the case even assuming that values beyond the neoliberal lend their support to a call for open borders. Trade law often bundles policy issues in multipart agreements, leading to compromises over public principles in the name of market access. Trade's institutions, both international and domestic, are ill-designed to channel input by civil society or enable oversight by the general public and arguably have led in the past to considerable industry capture. Beyond ensuring non-discriminatory treatment, trade law remains, in our view, the wrong place for both defining and enforcing rules on cross-border flows of personal data.

Thus, while we welcome with open arms the thoughtful attention Professors Anupam Chander and Paul Schwartz pay to the current transnational struggle over data flows and digital trade, we cannot join in their optimism that trade law is the right forum for arbitrating it. As Chander and Schwartz rightly note, the United States and the European Union retain fundamental differences in how each conceives of the balance

between the free flow of information and the protection of data privacy. What they largely disregard, however, is the central import of national security in these debates. While the European Union decries U.S. national security surveillance, the United States itself has recently invoked national security to block the international flow of data and protect its citizens. The national security elephant in the room will not be resolved through trade law.

It is not that we or other critics of data privacy in trade are antitrade conceptually. We are not opposed to the cross-border supply of goods and services and attendant data flows, and there is much good to be had from (non-race-to-the-bottom) trade between nations. However, to be pro-trade is not necessarily to be pro-trade *law*. Trade law is, fundamentally, not *constitutional* for cross-border data flows. Trade law lacks the normative orientation, legal underpinnings, institutions, and actors that are necessary for constructing just and sustainable data flows. Data protection law has for generations used its own mechanisms to govern personal data transfers across borders. And the United States has, for generations, been evading them. As the United States tries to subject data privacy instead to trade law institutions, it engages in a strategy known as regime shifting. Just as you would never negotiate a global treaty on free speech, or children's rights, to be enforced by the WTO, situating data privacy there would be a mistake. Data privacy, we contend, still does not belong in trade.

I. *Privacy and/or Trade*

In *Privacy and/or Trade*, Professors Chander and Schwartz make the case for revisiting Professor Joel Reidenberg's 1999 proposal for a global privacy treaty (the "Global Agreement on Privacy"), situated at and enforced by the World Trade Organization (WTO). Chander and Schwartz call for substantive international data privacy law negotiated by data privacy experts, adopted as part of WTO law and enforced through the WTO. Their proposal attempts to marry the virtues of harmonized international standards on data privacy with real enforcement through the WTO dispute resolution mechanism and trade sanctions: a treaty and a stick. What's not to like?

There is, indeed, much to love about this Article. It provides a deft and largely accurate entry into complex ongoing geopolitical battles in the trade and data privacy space. For many, the hurdles to joining in this discussion are high. *Privacy and/or Trade* is a must-read, written in clear and often witty language, by two leading experts in the fields of data privacy law and international trade law. Its conclusion, however, is wrong.

Chander and Schwartz lay out the problem as follows: international trade law, centrally concerned with cross-border trade of goods and services, has from the inception of the WTO recognized that data privacy protections are sand in the wheels of cross-border data flows. Data privacy laws regulate both the use of personal data and the conditions for personal data export, which can disrupt the flow of personal data to countries in which data privacy is not guaranteed. This in turn may stop the flow of IT-based services across borders.

The United States and the European Union (or, at the time of initial WTO negotiations, the European

Community) take markedly different approaches to data privacy law. As Schwartz has influentially remarked, in Europe there is a human rights backstop to comprehensive and harmonized data privacy law; in the United States, there is no human right to data privacy against commercial actors and also no general federal data privacy law (beyond spotty sectoral and consumer protection regulation). The United States is in the decided minority in its approach to data privacy law. In many countries, data privacy is an established human right. The majority of countries—the count stands at 157—have adopted data privacy legislation.

Aware of this significant divergence between major international players, trade law negotiators elected to bracket data privacy law from international trade law in what Chander and Schwartz refer to as "the Privacy Bracket": GATS Art. XIV(c)(ii). The Privacy Bracket, while on its face an exception, essentially kicks the can down the road regarding whether or not substantive data privacy law violates trade law. As Chander and Schwartz describe it, the Bracket "neither establishes global minimum standards for privacy, nor provides an international process for creating such standards. It simply allows signatory nations to protect privacy so long as this action can be said to be 'necessary.'" But what exactly is "necessary?" The authors note, correctly, that the Privacy Bracket is a compromise that satisfies absolutely nobody. Despite zero privacy-related enforcement actions at the WTO, both the United States and the European Union have been battling over cross-border data privacy since.

Chander and Schwartz claim that we now face a reckoning. For too long, they assert, other countries have "muddled through" the mess created by the soft geopolitical warfare between the United States and the European Union over data privacy. While the European Union has been deliberately exporting comprehensive data privacy law through its adequacy mechanism, country-by-country, the United States has been negotiating a narrower understanding of cross-border data privacy protections into both international soft law (APEC) and its recent plurilateral and bilateral trade agreements (e.g., USMCA).

This is the point, by the way, at which nonexperts often tune out: the field is rife with acronyms and terminology, and a great strength of this Article is in not wallowing in them. Instead, Chander and Schwartz paint the core picture in broad strokes, easy for nonexperts to understand: the United States continues to value and advocate for trade over privacy; the European Union values and advocates for privacy over trade.

The result, they argue, has been an increasingly messy regulatory thicket of varying and inconsistent data privacy regimes. Companies that wish to operate across borders face high compliance costs, and this favors, Chander and Schwartz claim, large businesses over small businesses and the Global North over the Global South. They introduce into the debate the framing of trade law not just as neoliberal in nature, but as neo-Brandeisian. Trade, they argue, can serve to break up big businesses, opening dominant domestic companies to challenges by international innovators. We are skeptical that embracing a laissez-faire approach to cross-border data privacy will release Schumpeter's creative destruction. Data fuel massive economies of scale and scope which are at the core of digital market power—nowhere better illustrated than in the less regulated United States platform technologies market.

So, what is to be done? On the one hand, Chander and Schwartz note that we could continue to "muddle

through," allowing the European Union and the United States to find, or to force, like-minded partners onto their team through smaller regional and bilateral agreements. The thicket problem, however, would remain. Or we could negotiate an international treaty and come to a compromise. Given the transatlantic divergence on fundamental norms and institutions, one might think this to be a nonstarter. Chander and Schwartz claim, with admirable optimism, that this is not the case.

They point to the uneasy "escape valve" in trade-privacy law: the "Safe Harbor"/"Privacy Shield" that the United States and the European Union have repeatedly negotiated bilaterally—and that the Court of Justice of the European Union (CJEU) has already overturned twice. In that compromise model, companies (rather than a country) opt in to a set of data privacy principles and practices and certify themselves to be in compliance. A third-party might oversee certification (the APEC model); a local regulator then enforces, in theory, against noncompliance. The CJEU overturned this compromise because it found that the United States does not qualify for an adequacy decision on the basis of its national security surveillance practices. (More on this later.) But Chander and Schwartz take this model as the starting point for two possible suggestions.

First, they write, we could get out of the present mess by creating a Global Privacy Enforcement Treaty. This treaty would take the escape-valve compromise as its starting point and give it teeth. It would allow countries to go after each other at the WTO, through the dispute settlement process, for failing to enforce against companies that have certified to privacy principles and proceeded to ignore them. This would, in theory, force the United States to put more enforcement resources into the Federal Trade Commission (FTC) and spur more significant oversight over compliance with a revived Privacy Shield mechanism.

Second, they argue, "[i]t is now possible to develop a vision for a Global Agreement on Privacy (GAP)" housed at the WTO. Reviving Reidenberg's two-decades-old idea of a global privacy treaty housed in trade law, Chander and Schwartz call for a substantive data privacy treaty. The escape valves of privacy law, alongside new state data privacy laws in the United States, might evidence a growing global consensus over norms and principles in data privacy law.

Chander and Schwartz acknowledge the validity of concerns about negotiating such a treaty within the WTO, heading off some of our criticism at the pass. They call instead for a treaty negotiated between external data privacy experts, analogizing to the process by which the WTO adopted and enforced international standards on food safety. After these experts (they suggest the Global Privacy Assembly, a forum for privacy officials) negotiate the substance, the WTO's dispute settlement procedures and trade sanctions would provide the teeth.

Chander and Schwartz aim to overcome compartmentalization in the privacy and trade literature (an important goal and one we share). The authors are clearly committed to the benefits of digital globalization, including economic development, alongside the value of human rights. They highlight, importantly, the longstanding, complex, and troubling dynamic in international trade law between the Global North and the Global South. And they frequently acknowledge the known limitations of international trade law as both substance and regime.

Where we fundamentally diverge is that Chander and Schwartz emerge optimistic about trade institutions and a trade law regime that, we argue, is by its very nature antithetical (or at least antagonistic) to data privacy law. Writing a treaty elsewhere does not solve the problem. As in most areas of law, interpretation and application are the key to trade law in practice. If we embed international privacy law principles in institutions substantively unaccustomed to the nuances and norms of personal data protection and instead accustomed to prioritizing free flows of services, the results will, we fear, predictably deprioritize data privacy, as has happened to other public values we discuss further below. Moreover, the WTO dispute settlement system is rarely deployed by countries in matters other than removing barriers to trade. This could render a data privacy agreement inside the WTO system symbolic. In other words, it is unlikely that parties to such a WTO treaty would enforce data privacy commitments through the WTO dispute resolution mechanism.

It is not that solving the puzzle of free-flow-versus-human-rights-protection is not doable. This is, as Chander and Schwartz rightly note, the same puzzle that EU data protection law itself aims to solve. The trouble is that international trade as a regime is fundamentally the wrong forum for striking a balance. Instead of regulators backed by not one but two human rights courts, you would get a series of panelists chosen by the parties to a trade dispute, typically socialized as trade lawyers. Trade's priorities, in other words, are baked into the dispute settlement process. Put data privacy enforcement in the trade system, and you will get pro-trade outputs. Privacy peg, trade hole.

In the next Part, we go into this argument in greater detail. We then turn to highlighting other important ways in which our premises differ from Chander and Schwartz's: the ongoing and unresolved core problem of mass national security surveillance; rising "data protectionism" by the United States under a national security label; and our differing take on the North-South digital divide.

II. Why Trade Is the Wrong Venue

We firmly believe trade is the wrong venue for the protection of data privacy, with the wrong set of both institutions and actors. Trade as a venue typically reflects the reality of geopolitics, with countries historically using trade as both a lever and a forum for outmaneuvering. Power is central to, and exploits, trade law. Trade's institutions, both international and domestic, are organized in ways that tend to channel private power and avoid broader accountability. And trade's norms and institutions lack tethering in human rights. The fact that the United States has recently tried to regime-shift data privacy into trade law is not evidence of trade's suitability as a forum, but rather, of its susceptibility to geopolitical power plays.

A. Realist Theory Plays Out in Trade: The Geopolitics of Countries and of Interest Groups

The idealized view of trade law is that it reduces barriers and protectionism, optimizing each country's comparative advantage and creating a rising tide for all. The realist view of trade law is that it is often a forum in which geopolitical forces rule the day. Besides, international trade policy is not made in a single

forum but many fora with different opportunity structures—such as the WTO, bilateral and plurilateral trade agreements, the OECD, the G7 and G20—that can be used to advance particular trade interests.

Historically, international trade law has served the geopolitical interests of powerful nations, such as the United States. Take for example Brazil's successful challenge to U.S. cotton subsidies. U.S. policy was found at the WTO to flout international trade rules by subsidizing cotton, thus depressing world prices and impacting the ability of developing countries to competitively export cotton. Rather than coming into compliance, the United States agreed to pay Brazil hundreds of millions of dollars to continue its cotton subsidies—thereby continuing to harm other cotton exporters, including developing countries in the Global South.

This story of the role of geopolitics in trade is not an outlier. Take as another example the recent history of intellectual property (IP) law in trade. The insertion of IP law into trade law is one of regime shifting par excellence. Dissatisfied with the results in one international forum—the UN, specifically, the World Intellectual Property Organization (WIPO)—the United States shifted not just forums but regimes, from the UN regime, rife with human rights commitments, to trade law. The story of data privacy in trade, we worry, is just another example of this well-rehearsed move.

The United States, driven in large part by domestic business interest groups, had been negotiating for a heightened level of international IP protection at WIPO. Developing countries banded together to push back against this agenda, noting the harmful effects of more stringent patent policies on access to medicines and on global public health. Stymied at WIPO, U.S. negotiators regime-shifted over to the WTO. This shift resulted in the negotiation of the TRIPS agreement (the Agreement on Trade-Related Aspects of Intellectual Property Rights) at the WTO—and outcry, again, from developing countries and a host of allies that a heightened level of IP protection enforced through trade sanctions would have a significant negative impact on public health, economic inputs, cultural hegemony, and more. TRIPS remains controversial. It maximizes the economic interests of intellectual property owners but ignores the moral rights of creators (espoused in EU law) and affects sustainable development in the Global South.

The story of IP in trade law, however, did not end there. Developing countries were arguably able to catch up to the largely U.S.-driven agenda around IP at the WTO, famously inserting a public health exception into TRIPS. What did the United States do? It forum-shifted again, this time to a series of bilateral and plurilateral trade agreements through which it could continue to ratchet up global IP protection, avoiding expected obstruction from developing countries at global fora. Chander himself has written about the pathologies of bilateral trade negotiations, noting the irony that in exporting measures from U.S. copyright law through trade, the United States used free trade law to "foist upon our trading partners rules that corporations may exploit to gain monopolies."

Ironically, forum shifting contentious issues into trade law has resulted in the recent weakening of global trade law. The WTO as a forum has been significantly weakened in recent years, again as a result of geopolitical forces. The WTO has been thrown into disarray by the United States's refusal to appoint new judges to the WTO's Appellate Body, thereby damaging its Dispute Resolution Mechanism. The United

States blames the WTO Appellate Body for not functioning according to its mandate while rejecting the authority of its verdicts as illegitimate under U.S. law.

The role of the WTO has also been diluted by a myriad of bilateral and mega-regional trade agreements (e.g., CPTPP and USMCA). In an effort to isolate China, the United States has shifted from broader plurilateral fora to those assembling like-minded countries, such as the G7 and the OECD. In view of these geopolitical maneuvers, our hopes for a Global Agreement on Privacy are not high. Other scholars (Professors Susan Ariel Aaronson and Patrick Leblond) who once suggested the WTO would be the right forum have since suggested shifting governance of cross-border data flows from the WTO to a standard-setting body similar to the Basel Committee on Banking Supervision.

The story of IP in trade is, at its core, geopolitical. A large and powerful country, the United States, harnessed the trade regime towards the ends of supporting specific domestic interest groups. What the United States is now doing in trade with respect to data privacy, we argue, is part-and-parcel of the same narrative. But first, to understand why trade law is so susceptible to serving as a forum for geopolitical power plays, we turn to a short overview of trade law's institutions and actors.

B. Trade's Institutions and Actors

Trade negotiations are not your typical lawmaking. This, we argue, affects the orientation and knowledge base of trade's institutions and actors. Even if one were to negotiate a Global Agreement on Privacy outside of trade, as Chander and Schwartz suggest, putting enforcement within the trade regime would skew its substance. To understand how such an Agreement would likely be enforced from within trade law, one has to understand trade law's typical actors and institutions.

Trade negotiations between countries take place behind closed doors, evade public scrutiny, and exclude civil society participation. Large tech companies and industry associations, meanwhile, intensively lobby their governments and enjoy privileged access to trade negotiators. This corporate lobbying has fallen on fertile ground with policymakers whose mission it is to maximize trade and commerce across borders. The very design of trade law's institutions, both global and domestic, incentivizes and channels this lobbying, while excluding civil society and the general public. That is, trade's neoliberal inclinations are not just a matter of principles but of institutional design.

As opposed to removing tariffs and quotas, today's Free Trade Agreements (FTAs) seek deep integration of participating countries' economies—but in specific ways. Today's FTAs are, per Professor Dani Rodrik, shaped largely by rent-seeking, self-interested behavior on the export side. Researchers who studied the lobbying of big internet companies note a particularly intensive transfer of ideas and personnel in digital trade that became government policy in the United States. The revolving door between industry and government in this space is long decried and very real. For example, Robert Holleyman spent twenty-three years as the President and Chief Executive of the Business Software Alliance (BSA) before he was appointed Deputy to the United States Trade Representative (USTR) from 2014 to 2017.

C. Bias Towards Trade Liberalization and the Lack of Human Rights

Even if the envisaged Global Agreement on Privacy were to be negotiated by external privacy experts, placing its enforcement within trade law institutions would significantly skew its substance. Any Global Agreement on Privacy is unlikely to be very detailed, if it is to be accepted by all members of the WTO (or at least all 87 parties to the Joint Statement Initiative on E-Commerce). Such an Agreement is far more likely, in the name of compromise, to include broad standards rather than strict rules. Interpretation of what those principles mean in practice will then fall in the hands of trade adjudicators, leaving them significant discretion over the Agreement's meaning.

As Chander and Schwartz observe, the international framework for data privacy remains incoherent and highly fragmented. It is unclear that a high-level consensus Global Agreement on Privacy would manage to meaningfully overcome existing substantive disagreements. If agreement is to be reached at all, it will be at the level of high-level principles.

If existing WTO cases are any indication, interpretation of vague principles by trade adjudicators is likely to emphasize economic rationality. It will treat data privacy as an *instrument* to promote trade, rather than as a human right and a societal value. There is a solid body of empirical research on the WTO's Dispute Settlement Mechanism that attests to the continued dominance of developed countries, its bias toward trade liberalization, and its inability to give due recognition to noneconomic objectives. Although there are recent signs of increased openness to nontrade norms and values at the WTO (in particular, public health in the WTO tobacco plain packaging cases), it is uncertain whether and to what extent this tendency will continue.

Trade law has long been decried for ignoring, or at least failing to internalize, human rights law (although there are those who disagree). Professor Philip Alston, for example, has warned of the merger and acquisition of human rights by international trade law, arguing that this would not lead to better recognition of noneconomic objectives but rather to a co-opting of human rights principles within trade. Even the G20 countries that adopted a mandate to achieve "Data Free Flow With Trust" (DFFT) were advised that "trade disciplines are not the primary means of building trust."

International trade agreements are, by definition, economic laws. 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.

Adding more human rights considerations to trade law does not necessarily meaningfully influence the interpretation and application of trade law. Newer trade agreements already hold a great deal of aspirational language about sustainability, labor rights, consumer protection, and also data privacy, to name but a few. This praiseworthy substance, however, typically does not manifest as binding commitments. Because of its aspirational rather than binding nature, it rarely actually reassures parties that if they regulate in these areas, they will fall under the general exceptions in trade.

D. Data Privacy, Thus Far, in Trade

We argue that the move to place data privacy into trade law represents a deliberate regime shift by the United States away from data protection. Trade law's institutions are well suited to carry the torch of free data flows, while shutting out epistemic communities in data privacy.

The most commonly used template for the digital trade chapter in recent Free Trade Agreements is a U.S. template known as The Digital Dozen. It contains a rule not to restrict the cross-border transfer of information, including personal data, by electronic means where this is part of a business activity. Aside from the United States, Australia, Japan, New Zealand, Singapore, and the United Kingdom (except for in its FTA with the EU) now routinely plug the same hard rule on free data flows into their bilateral or multilateral FTAs on digital trade.

This is how countries' data privacy laws, which tend to condition cross-border flows of personal data on adequate protection of data privacy, have become willfully entangled with trade law. Note another core aspect of this strategic move: 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. Starting from the premise that rules on cross-border flows of personal data should be minimally trade restrictive would favor those versions or aspects of data privacy law which are most trade friendly, as opposed to guaranteeing effective protection of individuals' data.

Placing binding provisions on cross-border data flows into FTAs restricts the policy autonomy of signatory states to unilaterally regulate these issues in their domestic law. That is, contracting states will likely have to justify data privacy laws as potentially trade law–violating measures through trade law's mechanism (i.e., the "Privacy Bracket" mentioned above).

The worry that data privacy laws will be successfully challenged as trade law violating is real. A recent report of the Waitangi Tribunal, which is tasked with protecting Maori people's interests in New Zealand, speaks to this concern. The Tribunal was called to decide whether New Zealand's government had protected Maori people's interests in data sovereignty and data governance when it entered the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP). The Tribunal's Report found that "reliance on the [trade] exceptions and exclusions . . . falls short of the [government's] duty of active protection." Put differently, reliance on the general exceptions in a trade agreement does not afford legal certainty that enables data sovereignty and data governance.

Data privacy has thus been framed in recent bilateral trade agreements as potentially protectionist without meaningful substantive guidance as to what constitutes acceptable regulation. To be clear, we are not advocating that substantive data privacy law belongs in trade law. Rather, dragging data privacy into trade as potentially protectionist with no meaningful guidance as to the scope of any exceptions, beyond the Bracket itself, creates a chilling effect. Coupled with trade's enforcement mechanisms, this move chills or will even restrict the ability of countries to regulate data privacy. This is an important point that Chander and Schwartz neglect—and one that in fact affects the United States as much as any other country. While

Chander and Schwartz note the recent development of state data privacy laws (in California, Colorado, and Connecticut, to name just a few), they point to these developments only to note the growing global consensus around data privacy principles. What they fail to address is that such new state data privacy laws—or if it comes to pass, a new federal data privacy law—could subject the United States to sanctions under its own free trade agreements.

E. Data Flows Are Already Constituted in Human Rights Frameworks

For decades, the balance between free cross-border flows of personal data and competing policy objectives, such as economic freedoms and freedom of speech, has been established not within trade law, but within human rights–driven legal frameworks.

The most firmly established regional framework constituting cross-border flows of personal data is the European Union's General Data Protection Regulation, which succeeded the 1995 Data Protection Directive. The rationale behind the creation of harmonized European data protection rules back in 1995 was, as Chander and Schwartz do note, an economic one: the creation of a single market for personal data and removing barriers to the free flow of personal data between member states. This has been achieved under the condition of a high level of personal data protection throughout the European Union, guaranteed by independent data protection authorities in the Member States. The European Union's highest court, the CJEU, ensures the uniform application and interpretation of personal data protection rules as part of EU law. The CJEU has assumed, over time, the role of a guarantor of fundamental rights, including the two fundamental rights to the protection of private life and personal data enshrined in the Charter of Fundamental Rights of the European Union.

Another influential international framework is the Council of Europe Convention 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data, modernized in 2018 as Convention 108+. The Convention views data flows through the prism of human rights, which are the catalyst contributing to the free flow of information between people. In other words, in stark contrast to trade law, the free flow of personal data is *conditioned* by the adherence to a certain high level of data protection rules and principles. The Convention is not limited to the members of the Council of Europe (a regional human rights organization within which it was initially adopted) but has already been joined by other countries, such as Argentina, Burkina Faso, Cabo Verde, Mauritius, Mexico, Morocco, Senegal, Tunisia, and Uruguay. Therefore, it has realistic prospects of becoming a global model for striking a balance between cross-border data flows and data privacy.

F. Race to the Bottom, Not the Top

It is true that there is significant consensus over the core principles of data privacy, which arise even within the more limited U.S. sectoral data privacy regimes. However, the regional standards established at the OECD and APEC and cited by Chander and Schwartz as evidence of norms convergence establish a consensus as to a data privacy floor, not a ceiling. Countries and regions remain able to establish a higher

level of data protection worthy of a human right. Trade law, on the contrary, sets the *maximum level* of protection, beyond which further protections are viewed as protectionism. The danger, and for some countries the allure, of placing data privacy into trade is that it will kick off a race to the bottom.

There is indeed significant consensus over core data privacy principles. Beyond the human rights frameworks discussed above, international standards for data protection were developed by the OECD in 1980 and later revised in 2013. The APEC Privacy Framework followed suit in 2005, complemented by the Cross-Border Privacy Rules (CBPR) (a government-backed data privacy certification aimed to facilitate cross-border data flows) in 2011, and updated in 2015. Even with this significant consensus, some core principles of the data protection toolkit remain contested. For example, many U.S. data privacy laws leave out data minimization, which is recognized as one of the important principles of data privacy in both the GDPR and Convention 108+.

The nonbinding frameworks of OECD and APEC primarily aim to ensure that protection of personal data is not used for protectionist purposes. Both the OECD and the APEC, however, set *minimum* standards. As Professor Graham Greenleaf has rightly observed, they establish a "rock-bottom" and "second-rate" baseline (not the ceiling) of many data privacy laws around the world.

Plugging a Global Agreement on Privacy into the trade law system may lead to a regulatory chill, as countries would tend to refrain from adopting regulations that are potentially noncompliant with trade rules. This is true even within the United States, as discussed above. Unfortunately, those frameworks currently referred to in trade agreements as examples of international standards striking the *right* balance between data flows and data privacy are the weakest ones (e.g., Article 19.8 of the USMCA and Article 17 of the Singapore-Australia Digital Economy Agreement (SADEA)). This means that deviation from these standards by setting higher data protection standards (such as those provided for in Convention 108+, to which Mexico—a signatory of one of the newer U.S trade agreements that attempts to characterize data privacy as protectionism—is party), from now on, may lead to a violation of those trade agreements. Liberalizing the cross-border flow of personal data to conditions that meet only the floor of data protection standards will undo what has been achieved in some regions and countries.

In sum, the last 40 years of regional and global data privacy policymaking reflect ongoing attempts to strike the balance between liberalizing data flows and human rights. In light of deep-seated disagreements on how that balance should be struck at a global level, the coexistence of several regional frameworks, affording different levels of data privacy protection, provides the space for contestation characteristic of legal pluralism and offers the potential for future adaptation.

The trade law regime is the wrong venue for regulating cross-border data flows. The balance between economic interests and data privacy protection has long been more appropriately struck within a human rights framework in existing regional agreements. Those regional agreements, however, are unlikely to ever garner buy-in from the United States. Hence, legal pluralism, including its advantages and drawbacks, continues.

III. Different Premises: Our (Fundamental) Normative Disagreements

We close this Essay by turning from our critique of trade law to three fundamental premises on which we apparently disagree with Chander and Schwartz. We view these premises as crucial for a full discussion of whether a Global Agreement on Privacy is even possible.

First, we argue that mass national security surveillance is a core, or even the core, element of the U.S.-EU conflict over data privacy. It is not possible to resolve the data privacy conflict within trade because trade law does not address national security policy. Indeed, if anything, trade law heavily brackets national security, as we discuss below.

Second, we point out that while there are certainly elements of truth to characterizing the United States as promoting trade over privacy, that caricature fails to acknowledge that the United States has in fact taken an increasingly protectionist approach to international data flows in recent years. Rather than carving out exceptions for data privacy, the United States has been establishing a "national security bracket" to trade law. Sovereignty over national security policy, rather than the unmitigated free flow of data, is increasingly the name of the U.S. game.

Third, we close by addressing our disagreements with Chander and Schwartz over the role of the regulation of data privacy in the North-South divide. We are hesitant, for numerous reasons, to join in their characterization that liberalizing global flows of personal data by reducing data privacy protections will result in economic and thus social benefit for the Global South. The picture, in reality, is far more complex.

A. The Central Import of Bulk National Security Surveillance

Chander and Schwartz discuss the role of U.S. bulk national security surveillance in transatlantic privacy conflicts only in passing. We believe a discussion of national security surveillance is crucial for understanding and attempting to resolve the conflict at hand. There is a national security elephant in the room.

Nearly ten years ago, Edward Snowden leaked documents revealing the extensive nature of U.S. national security surveillance. The Snowden leaks indicated the scope and indiscriminate nature of U.S. national security surveillance, the extent of cooperation by the private sector, and the impact in particular on EU persons. Arguably, they helped inspire the GDPR. In two judgments, *Schrems v. Data Protection Commissioner* (*Schrems I*) (2015) and *Data Protection Commissioner v. Facebook Ireland Limited & Schrems* (*Schrems II*) (2020), the CJEU in effect found that EU persons' data could not be exported to a country conducting such indiscriminate mass surveillance and invalidated the privacy compromise reached by the

U.S. and EU as being in violation of the Charter of Fundamental Rights of the European Union.

It is an error to focus only on the economic aspects of data flows while ignoring the human rights issues raised by unfettered bulk surveillance and signal intelligence by countries. Any Global Agreement on Privacy that fails to address countries' national security surveillance is bound to produce an imperfect level of transnational protection for data privacy. That is, the same concerns over national security surveillance that led the CJEU to twice invalidate the EU-U.S. privacy compromise are unlikely to be addressed by a Global Agreement on Privacy housed in global trade law.

The EU has been accused of being hypocritical in its response to U.S. national security surveillance. We do not believe these accusations are a reason to ignore the elephant in the room. It is true that countries on both sides of the Atlantic need to better apply human rights to national security surveillance powers. However, there is less hypocrisy than might appear at first glance. In its subsequent case law, the CJEU applied consistent standards when assessing the law enforcement and national security powers of EU member states and third countries alike when considering the necessity and proportionality of national surveillance authorities. EU instruments authorizing communications data retention as well as communications surveillance and data retention measures of member states (in particular France, Sweden, and the United Kingdom) have also been held by the CJEU to the same human rights standards.

Rather than characterizing transnational restrictions on data flows as protectionist in the trade law sense, one can understand them to be a powerful lever in ratcheting up human rights. Restrictions on data flows have served as a mechanism to incentivize countries to adopt higher safeguards against state-sponsored surveillance. This is exactly what happened when the CJEU twice slashed the status of the United States as ineligible to receive personal data from the EU without limitations. In 2022, President Joe Biden issued an executive order enhancing the protection of non-U.S. persons in the context of U.S. government surveillance activities. This would not have been adopted were it not for the development, yet again, of a new EU-U.S. framework for free cross border data flows. Affording individuals who are not U.S. citizens elementary protections against unfettered surveillance is an important mechanism to realize the universal human right to privacy in the digital era.

The national security elephant has not gone ignored by regional actors. For example, on December 14, 2022, the OECD adopted a Declaration on Government Access to Personal Data held by Private Sector Entities. This intergovernmental agreement sets forth a number of nonbinding principles and safeguards on government access to private sector data shared by "rule-of-law democratic systems." (China is not a member of the OECD.) However, the OECD does not have a human rights mandate, and its nonbinding guidance is mostly about minimum safeguards (again the floor, not the ceiling) and is limited to the membership of the OECD.

B. The United States is No Longer That Liberal on Data Flows

A second central premise on which we disagree with Chander and Schwartz is the caricature of the United

States as the torchbearer of free data flows. The characterization of the United States as standing for trade over privacy may still be true—but it turns out that in the realm of data flows, the United States does give other issues priority over trade.

For quite some time, it is true, the United States aimed to preserve the open internet and freedom from censorship. These laudable goals were clearly also economically self-serving. Professors Chander and Haochen Sun have argued that due to its unique position in digital services, the United States historically enjoyed data sovereignty by default: "The fact that the largest internet companies are based in the United States also means that data about Americans is typically stored in the United States." This explains the U.S. administration's preference for free data flows, which naturally gives it a strategic position over other countries' data about individuals.

Today, it is no longer a ground truth that the United States is unreservedly in favor of unrestricted cross-border data flows. Rather than invoking data privacy, the United States increasingly invokes national security as a reason to block transnational flows.

For example, in 2019, the Committee on Foreign Investment in the United States (CFIUS) ordered Chinese gaming company Kunlun to divest from the dating app Grindr due to concerns about the safety of Americans' personal data. CFIUS prohibited Kunlun from accessing Grindr's personal data and transferring it to China. This marked the beginning of a major policy shift. The role of CFIUS in controlling the outflow of personal data from the United States has steadily increased, prompting some to call it "the privacy regulator."

The U.S. government has also raised multiple national security concerns related to the operation of the popular Chinese-owned TikTok app. In 2019, CFIUS investigated TikTok about whether its owner, Chinese internet giant ByteDance, would be required to sell the app to address the national security risks related to the flow of U.S. personal data to China and Chinese government access to this data. Then-President Donald Trump threatened to ban TikTok from the app stores if ByteDance did not sell the app. President Biden reversed the ban but introduced a broader review of foreign software applications and set forth general criteria to evaluate national security risks posed by applications collecting personal data from the U.S. population. Ironically for a country so against data localization in data privacy regimes, the U.S. government will likely condition TikTok's ability to continue operating in the United States on the localization of Americans' personal data in the United States.

Despite practical similarities, there is a significant difference between the U.S.'s concern over the export of personal data through the lens of national security and the EU's concern over the export of personal data through the lens of human rights. The key emphasis through the U.S. lens is on the flow of personal data related to certain populations, such as the military, and large collections of data (for example, in the Foreign Investment Risk Review Modernization Act (FIRRMA), which took effect in 2020), rather than on the personal data of individuals. It is, therefore, not *individual* interests (or individual rights) but the *collective* interest in national security that the U.S. government understands to be at stake.

The shift of the United States, however, from free-data-flow champion to selectively personal data (dare we say) protectionist looks to be permanent. National security–motivated barriers to free data flows are likely to continue to rise as pervasive online monitoring and the mass accumulation of data increasingly leads to security and geopolitical risks. New legislative initiatives are underway. In September 2022, President Biden issued a new executive order to introduce more safeguards against China's ability to access Americans' personal data. What is more, two bipartisan bills aiming to restrict data export to and ban social media platforms from China and other high-risk countries have been proposed in 2022, marking a clear shift in U.S. lawmakers' policy agenda on cross-border data flows.

In line with this protectionist shift, recent U.S.-led FTAs include a "National Security Bracket" that also applies to data flows. In its recent FTAs, such as the USMCA and U.S.-Japan Digital Trade Agreement, the United States has secured almost unlimited autonomy to derogate from any obligation, including the free data flow provision, under a broadened national security exception (e.g., Art. 32.2(1)(b) of the USMCA and Art 4(b) of the U.S.-Japan Digital Trade Agreement). The National Security Bracket justifies measures to address national security threats, which are increasingly entangled with U.S. economic interests.

The National Security Bracket demonstrates a significant departure from the WTO national security exception, which can be invoked only in limited circumstances, all related to war and fissionable or fusionable materials. (See GATS Article XIV). In contrast, the new U.S.-style National Security Bracket can be invoked to justify *any* "essential security" interests, as defined by the United States itself. The Bracket thus serves as carte blanche for the United States to justify its restrictions on cross-border data flows.

C. The North-South Digital Divide

The third premise on which it appears we disagree with Chander and Schwartz is the notion that the free flow of personal data will confer unmitigated benefits on the global South. Recall that they argue from a neo-Brandeisian perspective that freeing personal data flows will lead to an increase in global competition for services. In fact, regulating data flows through trade agreements may further broaden the digital divide between the global North and the global South.

Some countries, such as India and South Africa, question whether developing countries actually enjoy the benefits of the digital economy, pointing at profound challenges they face in this area. Those challenges include an infrastructural and technological divide, a skills divide, and the market power of global digital platforms. Both India and South Africa did not join the WTO Joint Statement Initiative on E-Commerce, which includes a provision on cross border data flows. India chose to opt out from the negotiations of the Regional Comprehensive Economic Partnership (RCEP) in part because of its unwillingness to make any trade law commitments on cross-border data flows.

These concerns are not unfounded. The United Nations Conference on Trade and Development (UNCTAD) predicts that not every nation will benefit from free data flows equally. The value of data increases as it transforms from "raw data" to "digital intelligence" by undergoing data monetization. In practice, according to UNCTAD, cross-border exchanges of data are unequal and strongly defined by

South-to-North flows. The free flow of personal data does not guarantee the free flow of skills or other relevant resources. For example, researchers from the global South could not get visas to attend an AI conference in Canada. The monetization of data requires skills, capital, and infrastructure, which puts a few global digital platforms concentrated in a limited number of countries (mostly the United States and China) in a privileged position to produce and capture value from data. As a result, UNCTAD warns that developing countries may become "mere providers of raw data to global digital platforms, while having to pay for the digital intelligence obtained from their data."

The data-driven economy and the rise of artificial intelligence pose interrelated social challenges beyond data privacy that further implicate the South-North divide. These challenges include: social inequality and the rise of "winner-take-all" companies; social control through public and private surveillance; social polarization and risks to democracy; premature deindustrialization implicating development; national security (as discussed above); and geopolitical conflict. Other societal interests also factor in, such as industrial policy, the protection of indigenous communities (as illustrated by the Waitangi Report mentioned above), and distributive justice. By placing the governance of data flows into trade law, these multidimensional issues are channeled into a silo. Trade law and institutions would take over what used to be the domain of multi-stakeholder internet governance, which is by default inclusive to developing countries, civil society, and human rights discourses.

Our understanding of the data economy is still in its relative infancy. Assumptions about the benevolent effects of cross-border data flows for economic development run counter to the observable tendencies of digital platforms towards concentration and conglomeration. Overcoming the North-South digital divide is an important imperative. But it is not clear that attacking so-called privacy protectionism will in fact in the end benefit countries of the Global South.

IV. Conclusion

Efforts to place data privacy into international trade law would result in an unconstructive relationship. Instead, we argue for a division of labor between international trade law and data protection (that is, data privacy) frameworks, with clear boundaries around what international trade law should and shouldn't do. Given normative conflicts and increasing tension internationally between, for example, the United States, China, and Russia, regional mutual interest arrangements might be the most practicable way to continue to muddle forward.

Ultimately, data privacy underpins other fundamental and democratic rights and societal values. Tilting the balance towards free data flow can have consequences beyond compromising individuals' data privacy, inflicting collateral damage on the fabric of our democratic societies. Placing data privacy in trade law will, we are afraid, tilt that balance. International trade law must not be permitted to foreclose experimentation with regulation of the rapidly evolving data-driven economy.

* * *

Kristina Irion is Associate Professor at the Institute for Information Law (IViR) at the University of Amsterdam. Margot E. Kaminski is Associate Professor of Law at Colorado Law School and Director of the Privacy Initiative at Silicon Flatirons. Svetlana Yakovleva is a Postdoctoral Researcher at the Institute for Information Law (IViR), University of Amsterdam, Adjunct Professor of Law at Benjamin N. Cardozo School of Law, and Senior Legal Adviser at De Brauw Blackstone Westbroek (Amsterdam).

Authors are listed in alphabetical order and contributed equally.

Authors

 Kristina Irion

 Margot E. Kaminski

 Svetlana Yakovleva

March 27, 2023 / international law, privacy law, trade law

Leave a Reply

Enter your comment here...