UNITED STATES OF AMERICA

Federal Trade Commission

Remarks of Commissioner Noah Joshua Phillips[1]

Antonin Scalia Law School's Program on Economic and Privacy Program: Is EU Privacy Regulation Being Exported to the US?
Washington, DC
December 3, 2019

Introduction

Thanks, James; and thanks to the Antonin Scalia Law School's Program on Economics and Privacy for having me. As privacy surges to the forefront of national and international dialogue, the rigorous study James and PEP more broadly foster on the issue is critical to advancing the national interest.

I'm particularly pleased to join the great roster you've gathered today: Lydia Parnes, Professor Liad Wagman, and Acting Assistant Secretary of Commerce Jim Sullivan.

As for me, all I'll note is that the views I express today are my own and do not reflect those of my fellow Commissioners or the Commission as a whole.

This briefing asks the question: "Is EU Privacy Regulation Being Exported to the US?".

The timeliness of this question cannot be gainsaid. Last week, Senate Commerce Committee Chairman Roger Wicker circulated a discussion draft of

[1] The remarks I give today are my own and do not necessarily reflect the views of the Federal Trade Commission or any of my fellow Commissioners.

national privacy legislation. That committee will hold a hearing on this and other proposals tomorrow. I welcome this development, and commend the Chairman and his staff for their leadership, hard work, and thoughtful approach to a complex area of policy.

The phrasing of our question today, whether EU Privacy *regulation* is being *exported*, speaks volumes.

When we talk about imports and exports, we tend naturally to think of commerce in goods. From the Spice Road to the Boston Tea Party to the closing of the Suez Canal through to today, nothing less than world history is driven by such commerce. (Of course, ideas too have been exported: religious ideas, political ideas, and so forth.)

Commerce today involves far more than goods. Today, increasingly, it involves services; and – critically for today's discussion – the data upon which those services are based. While it can present risks, the international flow of data is and will remain essential to U.S. economic development and leadership. And a substantial amount of that flow involves data about individuals, which is to say that it implicates privacy.

When we think of commerce, then, we think of goods; we think of services; we think of data, including about people; but do we think of *regulation*?

Most people, I suspect, would not. But they should. The rules we adopt for commerce among states matter, greatly. The Roman law of commerce dominated

Europe and beyond for well over a millennium[2] ; the Framers of our Constitution empowered Congress specifically to "regulate commerce with foreign nations, and among the several states…" – that's the Commerce Clause[3] – the list goes on.

Too often, the privacy debate preoccupies itself with discussion of the risks *of* trade in data. Today, I want to talk about the risks *to* such trade.

International Data Flows

What's at stake?

A 2016 Department of Commerce study, which looked at the ways to measure the value of cross-border data flows, conducted by the National Telecommunications and Information Administration (NTIA) and the Economics and Statistics Administration, catalogued three types of commercial data traffic:[4]

1) Transaction data exchanged among market participants, including direct purchases from sellers and sales with digital platforms acting as intermediaries, such as when a U.S. consumer sends payment and address information via eBay to purchase an item only available abroad.
2) Commercial data and services – such as design information or human resources data – transferred between and within business enterprises. Rio

[2] Arthur Nussbaum, *The Significance of Roman Law in the History of International Law*, 100 U. Pa. L. Rev. 678, 680 (1951).

[3] U.S. CONST. Art. I, § 8, cl. 2.

[4] U.S. DEP'T OF COMMERCE, MEASURING THE VALUE OF CROSS-BORDER DATA FLOWS (2016).

Tinto, for example, has developed "excellence centers" to monitor worldwide operations at its plants and mines, allowing it to identify and avoid delays.[5]

3) Digital services exchanged between businesses and end-users (often consumers), such as internet telephony, search, and social media. This category includes familiar services like WhatsApp and, whatever you think of it, TikTok, not to mention email.

As these few examples demonstrate, the international flow of data enables companies to 'go global' in ways not possible only a short time ago. Companies of all kinds can readily take advantage of a global talent pool and build worldwide teams, remotely analyze manufacturing activity and supply chains, and extend their reach to customers an ocean away with relatively little effort, among other things.

The companies that purvey goods and services benefit, of course, but so – critically – do consumers. We all see better *and* cheaper products and services, and now can access those that, not too long ago, would have remained out of reach.

These developments are particularly useful to smaller businesses and new entrants (and by extension, their customers), who can achieve the reach and efficiencies previous limited to larger companies in a fraction of the time and at a fraction of the cost and risk.[6] In a 2016 study, almost two-thirds of worldwide

[5] James Manyika and Susan Lund, *Digital Protectionism and Barriers to International Data Flows*, The Bretton Woods Committee (Jun. 25, 2018), https://www.brettonwoods.org/article/digital-protectionism-and-barriers-to-international-data-flows.

[6] James Manyika et al., *Digital Globalization: The New Era of Global Flows, Executive Summary*, McKinsey & Company, at 7 (Mar. 2016), https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/digital-globalization-the-new-era-of-global-flows; *See also World Trade Report 2016*, World Trade Organization, at 46-50 (2016), https://www.wto.org/english/res_e/booksp_e/world_trade_report16_e.pdf.

startups surveyed had customers or users in other countries and close to half used foreign talent.[7]

Consider Etsy. 20 years ago, if you wanted to source custom craft work, you would have likely been limited to craftsmen in your local area or relying on importer middlemen. After a lot of effort, *maybe* you could find someone that would do great work at a good price. If you sold specialty crafts, reaching customers outside your region would have required a substantial investment in developing and marketing a worldwide e-commerce presence. Enter Etsy, and now we all are able to search globally among competing sellers, who in turn have a turnkey option to reach a global customer base. Indeed, over 30% of Etsy's volume comes from international transactions, including cross-border transactions.[8] That's a flowering of new connections between buyers and sellers, the expansion – and, as a matter of fact and logic both, the improvement – of the market itself.

Take another example: online education. Today, a prestigious university like MIT can offer online MicroMasters certificates in fields like supply chain management and data science without having to make risky investments in facilities or faculty.[9] And students from across the globe need only access to an internet connection to gain important new skills.

[7] Manyika, *supra* 5 at 8.

[8] Etsy, Inc., Quarterly Report (Form 10-Q) (Oct. 31, 2019).

[9] *See* MITx MicroMasters Programs, Mass. Inst. of Tech., https://micromasters.mit.edu/.

Though quantifying the value of digital trade is difficult, recent analysis cited by the Department of Commerce[10] bears out just how significant it is. Worldwide, according to a McKinsey Global Institute study, global data flows accounted for approximately $2.8 trillion in value in 2014, more than the trade in physical goods.[11] Other studies estimate that the impact of increased productivity and lower costs raised real U.S. GDP by $517 to $710 billion even back in 2011, or between 3.4 and 4.8 percent.[12] Practically, these data flows are allowing for the development of new businesses and the growth of existing firms; new and better jobs; innovative and improved products; and reduced costs for consumers. And all of this digital trade relies on international data flows, on information – about product specifications, employee information, customer data, etc. – going from country A to country B over the internet.

Risks, Both Foreign and Domestic

But risks to digital trade are growing. It has enemies, foreign and domestic.

First, data localization. An increasing number of countries require that data collected within the country be stored on servers located there. We have seen broad versions of these laws in Russia, China, and Indonesia for example.[13] Other countries, like South Korea and Germany, have sector-specific localization laws

[10] U.S. DEP'T OF COMMERCE supra 3.

[11] Manyika *supra* 5.

[12] U.S. INT'L TRADE COMM'N, 4485, DIGITAL TRADE IN THE U.S. AND GLOBAL ECONOMIES, PART 2 (Aug 2014).

[13] Cohen et al., *Data Localization Laws and their Impact on Privacy, Data Security, and the Global Economy*, Antitrust, at 107 (2017), https://www.americanbar.org/content/dam/aba/publishing/antitrust_magazine/anti-fall17.pdf.

applying to specific types of data, like health or financial information and telecom data.[14]

Under these regimes, companies are forced to make a choice whether to localize their data (and potentially their trade secrets), likely at a substantial cost, or abandon doing business in the country altogether. For smaller companies, there may not be a realistic choice – localization efforts may simply be cost prohibitive. Localization also limits competition, in particular for firms facing network effects of large incumbents and attempting to grow to scale.[15] The implications for consumers are higher prices, fewer services, or both.

Data localization requirements implicate more than trade, of course. Some of the countries imposing them also have far less concern for privacy than the U.S., which ought to concern civil libertarians.

Second, privacy laws that may not require localization, but do require that countries receiving data put in place a range of protections comparable to the protections of the country where the data was collected. Standing on its own, there is nothing wrong with this. The worry arises, however, when standards are applied unevenly, selectively, or based on inaccurate information.

Take Europe. In 1995, the EU adopted Directive 95, also known as the Data Protection Directive, to set up a common data privacy framework.[16] Under Directive 95, personal data could only be transferred outside of the EU if the European

---

[14] *Id.*

[15] Catherine Tucker, *Network Effects and Market Power: What Have We Learned in the Last Decade?*, Antitrust, at 72 (2018), http://sites.bu.edu/tpri/files/2018/07/tucker-network-effects-antitrust2018.pdf.

[16] Council Directive 95/46, 1995 O.J. (L281) 31-50 (EC).

Commission determined that the receiving country provided an adequate level of data protection.[17] Adequacy was to be determined by a range of factors, including the receiving country's data protection laws.[18] (The General Data Protection Regulation (GDPR), which maintains the Directive's transfer limitation and adequacy principles, supplanted Directive 95 in 2018.)[19]

Like the GDPR, while Directive 95 was European, its impact was global, including in the US. U.S. privacy law has long taken a different approach, instituting greater protections for higher-risk data – like financial or health data[20] – backed up by the Federal Trade Commission's unfairness and deception authority,[21] to ensure that consumers can make informed choices and are protected from harm. U.S. national security and criminal laws provide extensive privacy protection from the State. The Fourth Amendment to the U.S. Constitution establishes a baseline level of protection,[22] and federal and state statutes provide greater privacy protection even than the Constitution requires.[23]

Given these differences and the challenge of determining adequacy at a national level for the U.S., U.S. and EU officials instead negotiated the Safe Harbor

---

[17] *Id*., art. 25.

[18] *Id*.

[19] Council Directive 2016/679, art. 45 2016 O.J. (L119) 1-88 (EU).

[20] *See, e.g.* Fair Credit Reporting Act ("FCRA"), 15 U.S.C. § 1681 *et seq.* and Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), Pub. L. No. 104-191, 110 Stat. 1936 (codified in scattered sections of 42 U.S.C. and 29 U.S.C.).

[21] 15 U.S.C. § 45(a).

[22] U.S. CONST. amend. IV.

[23] *See, e.g.*, Electronic Communications Privacy Act of 1986 ("ECPA"), Pub. L. No. 99-508, 100 Stat. 1848 (codified as amended in scattered sections of 18 U.S.C.).

Privacy Principles,[24] under which a U.S. company could certify compliance with certain privacy protections and thus be eligible to receive data transferred from the EU.

That worked for a while. In 2015, however, in a case known as *Schrems*, the European Court of Justice (ECJ) struck down the Safe Harbor as insufficiently protective, primarily responding to concerns relating to the collection of law enforcement and national security information by the U.S. government, prompted by the leaks perpetrated by Edward Snowden.[25]

While the leaks provided sensational headlines, I admit that I find myself surprised by the perspective expressed by the ECJ and others about the U.S. We have more than 200 years of legal tradition, beginning with our natural rights tradition and the Fourth Amendment and made concrete through jurisprudence and statute,[26] establishing the privacy rights of individuals vis-a-vis the government. Our laws offer privacy protections from the State among the strongest – if not the strongest – in the world, including developed liberal democracies in Europe[27], and our intelligence gathering practices are second to none, by far, in transparency.[28] To argue for data embargoes predicated on what are, at core, relatively minor

[24] Comm'n Decision 2000/520, 2000 O.J. (L215) 7-47 (EC).

[25] Case C-362/14, Maximillian Schrems v. Data Protection Comm'r, 2015, https://curia.europa.eu/jcms/jcms/P_106311/en/.

[26] Carpenter v. U.S. 138 S. Ct. 2206, 2217 (2018).

[27] *See* Cameron Kerry, *Missed Connections: Talking With Europe About Data, Privacy, and Surveillance*, Brookings Institution, at 2, 16 (May 2014), https://www.brookings.edu/research/missedconnections-talking-with-europe-about-data-privacy-and-surveillance/.

[28]Letter from Robert Litt, General Counsel, Office of the Director of Nat'l Intelligence, to Justin Antonipillai, Counselor, U.S. Dep't. of Commerce, and Ted Dean, Deputy Assistant Secretary, International Trade Administration, U.S. Dep't of Commerce (Feb. 22, 2016), https://www.privacyshield.gov/servlet/servlet.FileDownload?file=015t00000004q1F.

differences in approaches to national security, and among countries that all embrace civil liberties, is puzzling to me, and may advance neither privacy nor national security, much less international commerce.

One of the most perplexing things about the *Schrems* case is that no similar actions have been filed relating to data transfers to, say, China and Russia, regimes that approach civil liberties differently, shall we say, from the West. As the European Parliamentary Research Service noted in 2016, "transfers to other big [non-U.S.] market players, such as China, have tended to be neglected, despite the increasing use of Chinese products (e.g. software and devices) and services (e.g. social networks and e-commerce websites) entailing a very large volume of data exchanges."[29]

Be that as it may, in response to the ECJ's ruling, EU and U.S. officials negotiated a new agreement, known as the Privacy Shield.[30] Privacy Shield includes new data-minimization and data transfer rules and restrictions, enhanced dispute resolution processes, and additional reporting and continuing compliance obligations for participating companies. The U.S. government also provided assurances in Presidential Policy Directive 28 and via written communications with EU officials that intelligence gathering activities would respect privacy interests and be subject to clear limitations and safeguards, such as limitations on bulk data

[29] *Personal Data Transfers to China*, European Parliamentary Research Service (Jun. 20, 2016), http://www.europarl.europa.eu/RegData/etudes/ATAG/2016/583836/EPRS_ATA(2016)583836_EN.pdf.

[30] Privacy Shield Framework, 81 Fed. Reg. 51041 (Aug. 2, 2016).

collection.[31] Like the Safe Harbor before it, the Privacy Shield was to be supported by robust FTC enforcement – and so it has been: we have brought over 20 cases (including four being announced today) for non-compliance since 2016.[32]

Maintaining this framework is important, especially for smaller companies, which may not be able to take advantage of the alternative legal bases for using or transferring EU data. Large entities can more easily establish subsidiary processing locations within the EU. They have the legal and financial infrastructure to adopt binding corporate rules, or standard contractual clauses.[33] Those to, by the by, are at risk. What is known as the *Schrems II* case challenges the use of standard contractual clauses, and could extend to Privacy Shield.[34]

Finally, today we are seeing a reflexive hostility toward the use and sharing of data domestically. It seems every time a company announces an innovation involving data, public officials and the media assume the worst, parading horribles even before taking any time to understand the practice. While some of these reactions may be understandable in light of some bad data practices that have come

---

[31] The White House, Pres. Policy Directive 28: Signals Intel. Activities (PPD-28) (Jan. 17, 2014), https://obamawhitehouse.archives.gov/the-press-office/2014/01/17/presidential-policy-directive-signals-intelligence-activities.

[32] Press Release, *FTC Announces Settlements with Four Companies Related to Allegations they Deceived Consumers over Participation in the EU-U.S. Privacy Shield*, Federal Trade Commission (Dec. 3, 2019), https://www.ftc.gov/news-events/press-releases/2019/12/ftc-announces-settlements-four-companies-related-allegations-they.

[33] A 2013 study indicated that revoking Safe Harbor could reduce U.S. services exports to the EU by 0.2 to 0.5 percent, and that the burden would fall disproportionally on smaller businesses who cannot open subsidiaries or use other legal mechanisms to transfer data. European Centre for International Political Economy, *The Economic Importance of Getting Data Protection Right: Protecting Privacy, Transmitting Data, Moving Commerce*, U.S. Chamber of Commerce (2013), https://www.uschamber.com/sites/default/files/documents/files/020508_EconomicImportance_Final_Revised_lr.pdf

[34] Case C-311/18, Data Protection Comm'r v. Facebook Ireland Ltd., Maximillian Schrems, 2019, https://curia.europa.eu/jcms/jcms/P_106311/en/.

to light, we should not succumb to the temptation to view data collection, use, and sharing as inherently or irredeemably flawed.

And this brings us back to the question of this program: Is EU Privacy Regulation Being Exported to the US?

Based on our conversation, I hope not, but I fear it might be.

Specifically, I am concerned about how these reactions will translate into legislation and whether we have learned the right lessons from what is going on overseas.

First, as should be clear from our earlier discussion, a law that burdens international data flows is bound to have a negative economic impact, particularly on smaller, innovative companies. American companies and consumers benefit from greater global data sharing. The Wall Street Journal recently reported a decline in American leadership in the services sector.[35] A lessening in the trade of data will exacerbate that trend. Nor is there any guarantee – given the types of concerns previously expressed by European courts – that the U.S. would achieve an adequacy determination as a result; a federal consumer privacy law, while merited in its own right, would not address European concerns about our national security processes. We must take care not become data isolationists, even as others go down that path. In fact, we must do the opposite, promoting mechanisms to ensure and enhance our ability to share data across borders.

[35] Paul Kiernan, *U.S. Dominance in Global Services Weakens*, The Wall Street Journal (Dec. 3, 2019), https://www.wsj.com/articles/u-s-dominance-in-global-services-economy-weakens-11575283275

Second, the lessons from Privacy Shield and data localization laws should be a cautionary tale. Legitimate as many privacy concerns are, we should recognize the substantial and tangible trade-offs privacy protection imposes on competition, growth, and innovation, and look carefully at research on the impact of regimes like the GDPR, something I expect Dr. Wagman will expand upon in a few moments.[36]

To take a minute on an American law, the FTC's aggressive enforcement of Children's Online Privacy Protection Act (COPPA)[37] has rankled content creators on YouTube.[38] We need to hear out their concerns. Catherine Tucker observes that innovation by American firms of kid-facing technology may have been chilled; while development in countries less concerned with children's privacy speeds up to fill the void.[39] Net result: *less* privacy protective technologies, and at the cost of American innovation. To be clear: that doesn't mean COPPA is bad or unwarranted – but we need to recognize the trade-offs.

Data sharing is endemic in the economy, supporting a multitude of business models that provide innovative products and services at low cost to consumers. If legislation is overly burdensome, if it means that firms do not have mechanisms through which they can use data to provide and develop products and services, then we risk undermining the growth and success of U.S. businesses; not to mention

---

[36] Jian Jia, Ginger Zhe Jin & Liad Wagman, *The Short-Run Effects of GDPR on Technology Venture Investment*, Nat'l Bur. Of Econ. Research (Nov. 8, 2019), http://dx.doi.org/10.2139/ssrn.3278912.

[37] Children's Online Privacy Protection Act ("COPPA"), 15 U.S.C. § 6501 et seq. and 16 C.F.R. § 312.

[38] Petition, *SAVE Family-Friendly Content on YouTube* (2019), https://www.change.org/p/youtubers-and-viewers-unite-against-ftc-regulation.

[39] Alex Marthews & Catherine Tucker, *Privacy Policy and Competition*, Brookings Institution, at 16 (2019), https://www.brookings.edu/wp-content/uploads/2019/12/ES-12.04.19-Marthews-Tucker.pdf.

options available to consumers. All of this is to say that in data privacy, as in life, there is no such thing as a free lunch; and we must be account for the collateral impacts of even the most well-intentioned rules.

Finally, we cannot just cut and paste a set of rules from one legal business culture into another and expect it to work as intended. For example, though the GDPR has a private right of action,[40] Europe does not have the robust plaintiff's bar that we have in the U.S., meaning that the GDPR is enforced and shaped by state actors. Should a similar private right of action be created in the U.S., as some are demanding, the impact would end up being the opposite, with private entities shaping the law through costly and inefficient litigation, government merely along for the ride in many cases, and laws completely impossible to change.

I'll conclude with one additional observation about data flows and the exportation of the GDPR.

The EU is attempting to export GDPR both by persuasion and by using adequacy determinations as an incentive. I understand their commitment to promoting rights they view as fundamental, and their pride in doing so. But the GDPR is a European project based on European traditions, society, economics, and laws; and less likely to have U.S. interests (economic and otherwise) top of mind. Other countries will approach things differently. Of course, there will always be countries that do not share our values and with which we will rightly be hesitant about sharing data. What we should not pursue, however, and should not want, is a

[40] Council Directive 2016/679, 2016 O.J. (L119) 1-88 (EU).

balkanized world of data among our friends. We should avoid creating unnecessary barriers between countries that each take seriously and respect privacy, albeit in somewhat different ways and with somewhat different points of emphasis. Rather than setting us at odds, the mutual goal of respecting privacy should be pulling us together.

There's much more to discuss about this topic, but I'm eager to hear what our great panelists have to say, so I'll end there.