2020

Governing the Internet: The Extraterritorial Effects of the General Data Protection Regulation

Sasa Jovanovic
Bowdoin College

Governing the Internet: The Extraterritorial Effects of the General Data Protection Regulation

An Honors Paper for the Department of Government and Legal Studies

By Sasa Jovanovic

Bowdoin College, 2020

An abundance of thanks to my family, friends, and professors, near and far.

Све пише за писмене.

Table of Contents

Chapter 1: Introducing Frameworks for Internet Governance

Introduction

David Carroll graduated from Bowdoin College *cum laude* in 1997, with a degree in Art History and Religion. In typical liberal arts fashion, his honors thesis explored the impact of tourism on Balinese dance-drama, a niche interest that has little to do with Carroll's work today. Technology had yet to captivate the world. In 1997, fewer than 40 percent of US households owned a PC.[1] IBM's Deep Blue supercomputer beat reigning world chess champion Garry Kasparov in a game of chess.[2] DVDs had been around for a total of two years.[3] "Back when I was [at Bowdoin], we had just discovered the Internet on Unix workstations running pine email and the Mosaic browser to see the earliest websites."[4]

Twenty years later, Carroll is neither museum curator nor priest, but starring in the Netflix documentary *The Great Hack*. Technology is no longer an accessory to daily lives, but has integrated into daily lives—sometimes, with disastrous consequences. *The Great Hack* tells such a story, focusing on the practices of UK political consulting firm Cambridge Analytica, now infamous for harvesting the Facebook profiles of 87 million users to influence voter behavior in more than 200 elections around the world, including the 2016 United States presidential election.[5] One of these 87 million users was David Carroll. *The Great Hack* follows his legal battle to retrieve

---

[1] Statista, "Percentage of households with a computer at home in the United States from 1984 to 2010," Statista, last modified 2019, accessed November 21, 2019, https://www.statista.com/statistics/184685/percentage-of-households-with-computer-in-the-united-states-since-1984/.

[2] Bruce Weber, "Swift and Slashing, Computer Topples Kasparov," *New York Times* (New York City, New York, USA), May 12, 1997, accessed November 22, 2019, https://www.nytimes.com/1997/05/12/nyregion/swift-and-slashing-computer-topples-kasparov.html.

[3] The Editors of Encyclopedia Brittanica, ed., "DVD," Encyclopedia Brittanica, last modified September 21, 2018, accessed November 22, 2019, https://www.britannica.com/technology/DVD.

[4] David Caroll, "Bowdoin Student Interested in Data Privacy," e-mail message to author, August 14, 2019.

[5] *The Great Hack*, directed by Karim Amer Amer and Jehane Noujaim, Netflix, 2019.

his data from Cambridge Analytica by employing a patchwork of European data protection laws, tracking the development of the Cambridge Analytica scandal as it escalates to gain the attention of the US Federal Trade Commission (FTC), the UK Information Commissioner's Office (UK ICO), and the British High Court.[6]

The Cambridge Analytica Scandal is just one example of how the Internet is making the world a smaller place. Since the Internet allows data to be regularly exchanged over borders at an unprecedented volume and speed, the Internet has been touted as a global commons[7] allowing for the transnational exchange of information, goods, and culture.[8] Data flows, or the transfer of information between computer servers across country borders, are also highly lucrative; according to a UN report, between 4 and 15% of global GDP is attributed to the digital economy.[9] It is in the interest of all states to maintain open data flows for the purpose of economic prosperity, and there are network and bandwagon benefits associated with doing so. This means that if one country joins a network, it also benefits all the other parties also on the network because the value of the network overall increases.[10] Therefore, interstate cooperation has been widely considered the most appropriate means of handling transnational internet issues.[11]

---

[6] *The Great Hack*, directed by Karim Amer Amer and Jehane Noujaim, Netflix, 2019.
[7] Gerald Stang, "Global Commons:" (European Union Institute for Security Studies (EUISS), 2013), JSTOR, www.jstor.org/stable/resrep06840; Milton Mueller, John Mathiason, and Hans Klein, "The Internet and Global Governance: Principles and Norms for a New Regime," *Global Governance* 13, no. 2 (2007): 237–54.
[8] Mark Raymond, "Puncturing the Myth of the Internet as a Commons," *Georgetown Journal of International Affairs*, 2013, 53–64.
[9] "Digital Economy Report 2019: Value Creation and Capture Implications for Developing Countries" (New York, New York: United Nations Conference on Trade and Development, 2019), https://unctad.org/en/PublicationsLibrary/der2019_overview_en.pdf.
[10] Milton Mueller, *Will the Internet Fragment? Sovereignty, Globalization and Cyberspace*, Digital Futures (Cambridge, UK ; Malden, MA: Polity Press, 2017).
[11] Bertrand de La Chapelle, Paul Fehlinger, and GLOBAL COMMISSION ON INTERNET GOVERNANCE, "JURISDICTION ON THE INTERNET: FROM LEGAL ARMS RACE TO TRANSNATIONAL COOPERATION," A Universal Internet in a Bordered World (Centre for International Governance Innovation, 2016), JSTOR, www.jstor.org/stable/resrep05249.10; Scott J. Shackelford, *Governing New Frontiers in the Information Age: Toward Cyber Peace* (New York, NY: Cambridge University Press, 2019).

Concerns about privacy and data protection pose a threat to maintaining the openness of these flows. In response to scandals like Cambridge Analytica, states have adopted data protection laws that afford them the power to dictate the conditions under which data can be transferred to other jurisdictions, even halting the transfer altogether under extreme circumstances.[12] While data protection laws are motivated in part by the advent of the Internet, states that are more likely to adopt data protection laws are also those that tend to give privacy the status of a human right, and have an extensive legal history associated with that right.[13] Therefore, states justify the regulation or suspension of data flows by suggesting that it puts the rights of their citizens at risk.[14]

However, there are also special characteristics of data that make it difficult to regulate like any other good. While the trade of goods may be regulated at the border by quotas or sanctions, data can occupy many places at once, many jurisdictions at the same time, unlike most other goods.[15] Data is also non-rival, which means that consumption by one entity does not prevent simultaneous consumption by another.[16] Nor is it divisible, which means that data is irreducible in its intrinsic value. This paper will use the phrase "the nature of data" to succinctly refer to these characteristics. The nature of data encourages states to employ extraterritoriality as a legal instrument to expand its regulatory reach. The consequences are that such laws may lead to regulatory spill-over into other jurisdictions, whether it be de facto changing corporate and

[12] Mueller, *Will the Internet Fragment?*
[13] Daniel J. Solove, "Conceptualizing Privacy," *Calif. L. Rev.. California Law Review*, no. IR (n.d.), http://lawcat.berkeley.edu/record/1118238. Alan F. Westin, "Science, Privacy, and Freedom: Issues and Proposals for the 1970's. Part I--The Current Impact of Surveillance on Privacy," *Columbia Law Review* 66, no. 6 (1966): 1003–50, https://doi.org/10.2307/1120997.
[14] Mueller, *Will the Internet Fragment?*
[15] Organisation for Economic Co-operation and Development, *Regulatory Co-Operation for an Interdependent World* (Paris: OECD Pub., 1994), https://doi.org/10.1787/9789264062436-en.
[16] Yan Carrière-Swallow and Vikram Haksar, "The Economics and Implications of Data: An Integrated Perspective" (International Monetary Fund, September 2019), file:///Users/sasajovanovic/Downloads/TEIDEA.pdf.

individual behaviors, or de jure influencing the decision-making of institutions.[17] This paper will refer to these collective consequences as the "extraterritorial effects" of such legislation.

This paper will use the EU-US relationship to empirically analyze the extent to which of two frameworks, presented in this chapter, better explains the development of data protection regulation between two major powers. In 2016, the EU adopted the General Data Protection Regulation (GDPR),[18] a data protection law which has since acquired the title of the strongest data protection law in the world.[19] The passing of the GDPR was hugely consequential towards the maintenance of open data flows because the law bestows the EU the power to determine the "adequacy" of third countries to grant EU citizens with data protection once their data is exported out of the EU.[20] While individual companies are provided the ability to conduct data transfers under certain EU conditions, this segments domestic markets into those companies that can afford to be GDPR compliant against those that cannot, since access to the EU market is economically advantageous. In order for the entire data flow to be GDPR compliant, the third country needs to either adopt data protection laws of their own that amount to adequacy per the EU's determination, or it needs to engage in bilateral negotiations. The US opted for the later.[21]

Therefore, regulation of data flows presents a serious governance challenge. While it would be beneficial to all states to maintain open data flows, it likewise difficult to diminish the sovereign right of a state to attempt to control a data flow if it is in the interest of their citizens. In light of

[17] Anu Bradford, *The Brussels Effect: How the European Union Rules the World* (New York: Oxford University Press, 2020).
[18] Commission Regulation 16/679, 2016 O.J. (L 119) p 1-88.
[19] Adam Satariano, "G.D.P.R., a New Privacy Law, Makes Europe World's Leading Tech Watchdog," *The New York Times*, May 24, 2018, sec. Technology, https://www.nytimes.com/2018/05/24/technology/europe-gdpr-privacy.html.
[20] Commission Regulation 16/679, 2016 O.J. (L 119) p 1-88.
[21] Henry Farrell and Abraham Newman, *Of Privacy and Power: The Transatlantic Struggle over Freedom and Security*, 2019, https://doi.org/10.1515/9780691189956.

this reality, two frameworks can pointedly describe the dichotomy of outcomes which may emerge as a result of this dilemma. Complex interdependence is a framework which emphasizes bilateral cooperation as a resolution to instances when states are linked by common goals and mutual reliance, like a data flow for instance, and has been widely regarded by scholars as a valuable perspective when thinking about Internet governance.[22] On the other hand, the Cyber Westphalian System (CWS) [23] is a framework which emphasizes bilateral competition, as states use strategies to pursue their own interests and reassert their dominance over a transnational platform. When the success of bilateral cooperation hinges on joint collaboration, state authority is in danger of waning in an interdependent environment, and so CWS offers a way to comprehend states which either do not want to cooperate, or are responsive to competing priorities which complicates inter-state cooperation.[24]

The Privacy Shield in 2016 emerged as a bilateral solution to afford the US adequacy under the GDPR, providing US companies with access to the EU market under joint oversight of US and EU institutions.[25] However, whether or not this agreement will succeed in the long run is subject to speculation.[26] This is not the first time that the two states have attempted to resolve issues concerning the EU-US data flow. The US has previously used bilateral agreements as a way to

---

[22] Kenneth S. Rogerson, "INFORMATION INTERDEPENDENCE: Keohane and Nye's Complex Interdependence in the Information Age," *Information, Communication & Society* 3, no. 3 (January 2000): 415–36, https://doi.org/10.1080/13691180051033379.

[23] While Demchak uses CPS as a shorthand for the term, Cyber-Westphalian System, this paper will employ CWS as a shorthand for clarity reasons. Chris Demchak and U.S. Naval War College, "Three Futures for a Post-Western Cybered World," *Military Cyber Affairs* 3, no. 1 (June 2018), https://doi.org/10.5038/2378-0789.3.1.1044.

[24] Samantha Bradshaw et al., "THE EMERGENCE OF CONTENTION IN GLOBAL INTERNET GOVERNANCE," Who Runs the Internet? (Centre for International Governance Innovation, 2017), JSTOR, www.jstor.org/stable/resrep05243.8.

[25] "EU Commission and United States Agree on New Framework for Transatlantic Data Flows: EU-US Privacy Shield," Text, European Commission - European Commission, accessed April 4, 2020, https://ec.europa.eu/commission/presscorner/detail/en/IP_16_216.

[26] Mark Scott, "U.S. and Europe in 'Safe Harbor' Data Deal, but Legal Fight May Await," *The New York Times*, February 2, 2016, sec. Technology, https://www.nytimes.com/2016/02/03/technology/us-europe-safe-harbor-data-deal.html.

shield itself from forced adoption of data protection laws.[27] Therefore, the EU-US relationship presents an intriguing case. On the one hand, regulatory cooperation is an expected outcome because both states are equally dependent on maintaining open flows. Furthermore, since their domestic markets are of a similar size, neither actor is able to economically coerce the other to accede to their own preferences.[28] On the other hand, regulatory competition is an expected outcome since the EU and the US have significantly different legal approaches to data protection.[29] Unlike the EU, the US does not extend a right to data protection to its citizens, and the American preference for laissez-faire economic growth considers data protection a barrier to the liberalization of trade.[30] Therefore, the extraterritorial effects of the GDPR runs into conflict with the US being able to pursue these interests, making the US reticent to cooperate with the EU in bilateral coordination.

The purpose of this paper is to provide answers to the following questions: How do differences in the institutional and legal histories in the EU and US conceptions of data protection shape regulatory competition and cooperation? Why and how does the GDPR exert its influence beyond the EU jurisdiction, and is its dominance likely to continue?

This chapter will introduce two theoretical approaches that illustrate the conditions when states are likely to compete or cooperate over complex policy questions like data protection. The second section will present the complex interdependence literature, as well as the conditions under

---

[27] Henry Farrell, "Constructing the International Foundations of E-Commerce—The EU-U.S. Safe Harbor Arrangement," *International Organization* 57, no. 2 (2003): 277–306, https://doi.org/10.1017/S0020818303572022.
[28] Ernest J. Wilson, "Hard Power, Soft Power, Smart Power," *The Annals of the American Academy of Political and Social Science* 616 (2008): 110–24.
[29] Fernando Mendez and Mario Mendez, "Comparing Privacy Regimes: Federal Theory and the Politics of Privacy Regulation in the European Union and the United States," *Publius* 40, no. 4 (2010): 617–45; Franz-Stefan Gady, "EU/U.S. Approaches to Data Privacy and the 'Brussels Effect': A Comparative Analysis," *Georgetown Journal of International Affairs*, 2014, 12–23.
[30] Joshua P. Meltzer, "Cross-Border Data Flows, the Internet and What It Means for U.S. and EU Trade and Investment," *Brookings* (blog), October 21, 2014, https://www.brookings.edu/blog/up-front/2014/10/21/cross-border-data-flows-the-internet-and-what-it-means-for-u-s-and-eu-trade-and-investment/.

which regulatory cooperation is likely to occur. The third section in this chapter will present the CWS literature, and the conditions under which regulatory competition is likely to occur. The fourth section will suggest that there is also a third, inter-state equilibrium which can explain situations when states are able to benefit from certain competitive advantages of their regulation, also known as soft power,[31] under conditions of regulatory cooperation. I will argue that the EU has cultivated soft power through its institutional and legal history, which in turn provides it with a competitive advantage to obtain favorable outcomes in regulatory cooperation with the US.

Friends with Benefits: The Complex Interdependence of Shared Data Flows

Keohane and Nye first made use of the term 'complex interdependence' in 1977 to describe how increased interconnectedness among states encourage politics of interdependence. This "allows for events and situations in one area, depend on, or are influenced by, those in another, and most importantly this relationship can be reciprocal."[32] Keohane later notes that reciprocity is not a common feature in most of international relations because of the ability of more powerful actors to coerce, dominate, or exploit lesser actors. Reciprocity is defined as "exchanges of roughly equivalent values in which the actions of each party are contingent on the prior actions of the other in such a way that good is returned for good and bad for bad."[33]

Reciprocity is present in the case of EU-US relations because the actors have roughly equivalent economic size and political importance in the international community.[34] Further, they are similarly reliant on mutual cooperation; the fact that both the EU and the US have repeatedly

[31] Joseph S. Nye, "Soft Power," *Foreign Policy*, no. 80 (1990): 153–71, https://doi.org/10.2307/1148580.
[32] Rogerson, "INFORMATION INTERDEPENDENCE," 416.
[33] Robert O. Keohane, "Reciprocity in International Relations," *International Organization* 40, no. 1 (1986): 8.
[34] Daniel S. Hamilton et al., "Forging a Strategic U.S.-EU Partnership," Shoulder to Shoulder: (Atlantic Council, 2009), JSTOR, www.jstor.org/stable/resrep03552.6.

made efforts to maintain data protection agreements indicative of this reliance. At the same time, because reciprocity is uncommon, the EU-US relationship is not representative of all inter-state relations since each actor may otherwise adopt coercive tactics in relations with less powerful states, meaning that the same degree of bilateral negotiation may not arise as in this case.[35] However, precisely because of this fact, it is important to take note of the outcomes from clashes between the EU and the US since the result of these negotiations may influence other intergovernmental agreements that involve one of these states.

Complex interdependence has primarily been employed to explain state behavior under conditions of globalization, but there is a theoretical overlap in thinking about globalized trade and data flows, since both are means of connection through exchange between two entities.[36] In this way, they are transnational.[37] At the same time, while the trade of goods may be regulated by quotas or sanctions, these same methods cannot be applied to the internet because of the nature of data. If anything, the Internet is more transnational as a result of these features, making it all the more difficult to govern, and pushing for states to adopt laws which employ extraterritoriality like the GDPR.[38] Complex interdependence calls attention to the importance of cooperation as a means of achieving common goals of states, in this case being the preservation of the EU-US data flow.[39] For these reasons, complex interdependence has been highly influential amongst scholars when thinking about internet governance.

---

[35] Keohane and Nye discuss power asymmetries among actors can induce behavior to align with the priorities of the more powerful state. Robert O. Keohane and Joseph S. Nye, *Power and Interdependence*, 2nd ed, Scott, Foresman/Little, Brown Series in Political Science (Glenview, Ill: Scott, Foresman, 1989).
[36] Rogerson, "INFORMATION INTERDEPENDENCE."
[37] de La Chapelle, Fehlinger, and GLOBAL COMMISSION ON INTERNET GOVERNANCE, "JURISDICTION ON THE INTERNET: FROM LEGAL ARMS RACE TO TRANSNATIONAL COOPERATION."
[38] Sean Watts and Theodore Richard, "BASELINE TERRITORIAL SOVEREIGNTY AND CYBERSPACE.," *Lewis & Clark Law Review* 22, no. 3 (September 2018): 771–840; JOANNE SCOTT, "Extraterritoriality and Territorial Extension in EU Law," *The American Journal of Comparative Law* 62, no. 1 (2014): 87–125.
[39] G. Gunasekara, "The 'Final' Privacy Frontier? Regulating Trans-Border Data Flows," *International Journal of Law and Information Technology* 17, no. 2 (June 1, 2009): 147–79, https://doi.org/10.1093/ijlit/eam004.

Complex interdependence highlights multiple channels of communications between two jurisdictions, not limited to interstate relations, which may erode the exclusive authority of the state to govern its domestic affairs.[40] For instance, multinational corporations must be responsive to many populations at once,[41] but are also able to influence political agendas in multiple jurisdictions through lobbying or shaping consumer expectations to align with their own corporate values.[42] Social media has a prominent effect on the ways consumers communicate with one another across borders, shaping their perspectives in reaction to global events like the Cambridge Analytica scandal.[43] Transnational activist networks have spurred citizens to engage in collective action domestically or online, while sharing strategies with other organizations around the world.[44] Therefore, the extraterritorial effects of the GDPR may manifest themselves across American society largely as a result of these multiple channels of communication.

Finally, non-state actors may directly influence the deal-making process for a bilateral agreement. While multiple channels of communication allow for similar sectors to interact across borders, different sectors might also influence each other.[45] Non-state actors may take several forms, such as multinational corporations, non-governmental organizations, and individuals. Therefore, institutional dialogue between states is not devoid from pressures to include perspectives other than those represented in the negotiations.[46]

---

[40] Keohane and Nye, *Power and Interdependence*.
[41] B. R. Baliga and Alfred M. Jaeger, "Multinational Corporations: Control Systems and Delegation Issues," *Journal of International Business Studies* 15, no. 2 (1984): 25–40.
[42] Joseph S. Nye Jr, "Multinationals: The Game and the Rules: Multinational Corporations in World Politics," August 31, 2017, https://www.foreignaffairs.com/articles/1974-10-01/multinationals-game-and-rules-multinational-corporations-world-politics.
[43] Annelise Russell and Maxwell McCombs, "The Media," in *Policy Analysis in the United States*, ed. John A. Hird, 1st ed. (Bristol University Press, 2018), 265–80, https://doi.org/10.2307/j.ctt22h6q1x.20.
[44] Sebastian Haunss, "Privacy Activism after Snowden: Advocacy Networks or Protest?," n.d., 19.
[45] Anne-Marie Slaughter, "The Accountability of Government Networks," *Indiana Journal of Global Legal Studies* 8, no. 2 (2001): 347–67; Anne-Marie Slaughter, "How to Succeed in the Networked World: A Grand Strategy for the Digital Age," *Foreign Affairs* 95, no. 6 (2016): 76–89.
[46] Keohane and Nye, *Power and Interdependence*.

Complex interdependence has been the dominant framework for thinking about Internet issues because of the Internet's ability to multiply the consequences of reciprocity of actors through the use of multiple channels, raising the importance of non-state actors in formal inter-state dialogue as a result.[47] The conditions for complex interdependence are the following. First, states engage in cooperation to overcome shared challenges and achieve shared goals. Second, multiple channels of communication allow for a variety of actors to exchange information, react to events beyond their jurisdiction, and change behavior within their jurisdiction. Third, non-state actors can present a significant challenge to the success of bilateral agreements because they represent views that are not portrayed in formal negotiations. While CWS suggests that the Internet is another instrument for a state to exercise control, complex interdependence highlights the novel challenges of the Internet that complicate this underlying assumption.

Territorializing the Internet: The Cyber Westphalian System

If complex interdependence serves to explain why states engage in cooperation in the first place, then CWS explains the ways in which states resist cooperation in order to pursue their own interests.[48] According to legal scholar Stephen Krasner, "Westphalian Sovereignty… refers to the autonomy of domestic authority structures—that is, the absence of authoritative external influences."[49] This approach is associated with realist arguments in international relations that

[47] Robert O. Keohane and Joseph S. Nye Jr, "Power and Interdependence in the Information Age," February 15, 2019, https://www.foreignaffairs.com/articles/1998-09-01/power-and-interdependence-information-age; Joseph Nye, "The Regime Complex for Managing Global Cyber Activities," Global Commission on Internet Governance (Centre for International Governance Innovation, May 2014), https://www.cigionline.org/sites/default/files/gcig_paper_no1.pdf.
[48] Demchak and U.S. Naval War College, "Three Futures for a Post-Western Cybered World."
[49] STEPHEN D. KRASNER, "Problematic Sovereignty," in *Problematic Sovereignty*, ed. STEPHEN D. KRASNER, Contested Rules and Political Possibilities (Columbia University Press, 2001), 2, https://doi.org/10.7312/kras12178.5.

places the role of the state at the center of analysis.[50] The state engages in efforts to increase its hard power, or ability to wage war successfully, relative to other states.[51]

CWS relies on the current framework of international law to assign authority to distinct states, delineate states from one another, and justify claims to sovereignty.[52] While some legal scholars have questioned the applicability of territorial jurisdiction to a digital space,[53] Laura DeNardis points that out that it is false to claim that the Internet is purely devoid of territorial significance pointing to critical Internet infrastructure like Internet exchange points (IXPs), database servers, and physical transmission lines, as the physical manifestation of the Internet.[54] In this way, the Internet is a "reflection of the current international system in a new domain,"[55] which allows for jurisdiction as defined by territory to continue. While on the one hand, bilateral agreements might encourage inter-state cooperation, bilateral agreements might also set the conditions for legal interoperability.[56] Legal interoperability provides the parameters for interactions between states while preserving the domestic legal attitudes of each state, thereby securing state sovereignty.[57]

---

[50] David A. Baldwin, "Realism," in *Power and International Relations*, A Conceptual Approach (Princeton University Press, 2016), 123–38, https://doi.org/10.2307/j.ctt1q1xsp6.8.
[51] Baldwin.
[52] Hannah L. Buxbaum, "Territory, Territoriality, and the Resolution of Jurisdictional Conflict," *The American Journal of Comparative Law* 57, no. 3 (July 1, 2009): 631–76, https://doi.org/10.5131/ajcl.2008.0018; Michael N. Schmitt and NATO Cooperative Cyber Defence Centre of Excellence, eds., *Tallinn Manual on the International Law Applicable to Cyber Warfare: Prepared by the International Group of Experts at the Invitation of the NATO Cooperative Cyber Defence Centre of Excellence* (Cambridge ; New York: Cambridge University Press, 2013).
[53] David R. Johnson and David Post, "Law and Borders: The Rise of Law in Cyberspace," *Stanford Law Review* 48, no. 5 (1996): 1367–1402, https://doi.org/10.2307/1229390.
[54] Laura DeNardis, "Internet Points of Control as Global Governance," Internet Governance Papers (Waterloo, Canada: The Centre for International Governance Innovation, August 2013), https://www.cigionline.org/sites/default/files/no2_3.pdf.
[55] A Liaropoulos, "An International Cyber-Order under Construction?," *Journal of Information Warfare* 12, no. 2 (2013): 23.
[56] John Gorham Palfrey and Urs Gasser, *Interop the Promise and Perils of Highly Interconnected Systems* (New York: Basic Books, 2012), http://proquestcombo.safaribooksonline.com/9780465021970.
[57] Amedeo Santosuosso and Alessandra Malerba, "Legal Interoperability as a Comprehensive Concept in Transnational Law," *Law, Innovation and Technology* 6, no. 1 (May 27, 2014): 51–73, https://doi.org/10.5235/17579961.6.1.51.

Moreover, CWS has found resonance amongst Internet scholars that view the Internet as another platform unto which hard power can dictate hierarchical authority among states. Since state sovereignty is related to the ability of the state to monopolize violence, Chris Demchak argues that a parallel exists between cyber conflict and "traditional kinetic war,"[58] and many of the customs of armed combat hold up in digital struggles like the principle of mutual recognition. The Internet presents a security dilemma which has encouraged states like the US to militarize their intelligence capabilities to take advantage of the volume of information provided online.[59] Milton Mueller argues that the "attempt by governments to align informational flows with their jurisdictional boundaries,"[60] including the national securitization of the internet, like that of the US, and territorialization of information flows, like that of the EU, are state efforts at preserving centralized power.[61]

The literature on regulatory regimes suggests that, even if states are able to put aside their domestic interests in order to cooperate on shared issues, challenges persist that complicate the possibility of successful cooperation.[62] For instance, states like the EU and the US have differed in their understanding of fundamental concepts, i.e. data protection, which makes negotiations difficult.[63] Bargaining failures are likely to arise as a result of preference divergence, as states

---

[58] Chris C. Demchak, "Uncivil and Post-Western Cyber Westphalia," *The Cyber Defense Review* 1, no. 1 (2016): 55.
[59] Chris C. Demchak and Peter J. Dombrowski, "Rise of a Cybered Westphalian Age: The Coming Decades," in *The Global Politics of Science and Technology - Vol. 1: Concepts from International Relations and Other Disciplines*, ed. Maximilian Mayer, Mariana Carpes, and Ruth Knoblich (Berlin, Heidelberg: Springer Berlin Heidelberg, 2014), 91–113, https://doi.org/10.1007/978-3-642-55007-2_5.
[60] Mueller, *Will the Internet Fragment?*, 212.
[61] Mueller.
[62] Daniel W Drezner, *All Politics Is Global: Explaining International Regulatory Regimes*, 2008, https://doi.org/10.1515/9781400828630.
[63] Andrew Hurrell, "Power, Institutions, and the Production of Inequality," in *Power in Global Governance*, ed. Michael Barnett and Raymond Duvall, Cambridge Studies in International Relations (Cambridge: Cambridge University Press, 2004), 33–58, https://doi.org/10.1017/CBO9780511491207.002; Wolfram F. Hanrieder, "Compatibility and Consensus: A Proposal for the Conceptual Linkage of External and Internal Dimensions of Foreign Policy," *The American Political Science Review* 61, no. 4 (1967): 971–82, https://doi.org/10.2307/1953399.

agree on the objective of a negotiation, but differ in the details of maintaining the agreement.[64] In the case of data flows, the states may disagree on the appropriate degree of regulatory rigor necessary to maintain consistent treatment across the data flow. One state may also oppose the other state's choice of institutions tasked with regulatory compliance.[65] Finally, the question of the willingness of states to uphold the negotiation and not renege on their commitment is a constant obstacle to successful cooperation.[66] For cooperation to be successful, the adjustment costs associated with changed institutional behavior and firm practice must be sufficiently low in order for the benefits from cooperation to be worth it.[67] Therefore, the legal attitudes of each state may serve as barriers to cooperation, since significant departure from precedent might incur intolerable adjustment costs to the state.[68]

The literature summarized in this section informs the selection of conditions this paper will employ for CWS. First, states are driven by domestic interests which drives competition with other states, whether it be in the explicit securitization of the Internet, like the US, or the use of data protection regulation, like the EU. Second, disagreements over fundamental concepts, i.e., data protection, cause different legal attitudes and institutional structure which may result in different cost-benefit analyses making it difficult to maintain agreements over time. Third, the commitment of states to maintain their promises, either in light of competing priorities or due to institutional mismatch, further complicates the ability of states to make an agreement that will endure over time. Fourth, jurisdictional limits must be clear in order to adhere to the international legal system.

---

[64] Drezner, *All Politics Is Global*.
[65] Drezner.
[66] Imelda Maher, "The Networked (Agency) Regulation of Competition," in *Regulatory Theory*, ed. PETER DRAHOS, Foundations and Applications (ANU Press, 2017), 693–710, www.jstor.org/stable/j.ctt1q1crtm.52.
[67] Drezner, *All Politics Is Global*.
[68] Daniel B. Rodriguez, "Turning Federalism Inside out: Intrastate Aspects of Interstate Regulatory Competition," *Yale Law & Policy Review* 14, no. 2 (1996): 149–76; Claudio M. Radaelli, "The Puzzle of Regulatory Competition," *Journal of Public Policy* 24, no. 1 (2004): 1–23.

A Third Way: Soft Power

Both of these frameworks are grounded on an underlying assumption that state power is expressed aggressively through waging war or conflict. Complex interdependence suggests that actors may lose power because they are opting for cooperation instead of conflict.[69] On the other hand, CWS suggests that that states are unlikely to cooperate because they are reticent to concede the ability to influence other actors through military aggression and impose hostile threats.[70] However, while it is true that cooperation may result in states losing their ability to utilize so-called hard power, the Internet provides states the capacity to capitalize on soft power.

Soft power allows states to pursue their domestic interests through the use of multiple channels. Soft power is defined as "the ability to achieve goals through attraction… convincing others to follow or getting them to agree to norms and institutions that produce the desired behavior."[71] Soft power can be achieved in a number of ways, whether it be the passive diffusion of a norm or culture based on its ideational appeal[72] or the conscientious refinement of domestic laws and institutions that encourage behavior to align with the preferences of the state.[73] The economic capability of a state may also provide a means of cultivating soft power, since it is able to dictate entrance and exit from its market.[74] States with large domestic markets or resource-based

---

[69] Keohane and Nye, *Power and Interdependence*; Rogerson, "INFORMATION INTERDEPENDENCE"; MARK T. PETERS, "Interdependence," in *Cashing In on Cyberpower*, How Interdependent Actors Seek Economic Outcomes in a Digital World (University of Nebraska Press, 2018), 13–44, https://doi.org/10.2307/j.ctt22726v0.7.
[70] Waheeda Rana, "Theory of Complex Interdependence: A Comparative Analysis of Realist and Neoliberal Thoughts" 6, no. 2 (2015): 8; Chris Demchak and Peter Dombrowski, "Cyber Westphalia: Asserting State Prerogatives in Cyberspace," *Georgetown Journal of International Affairs*, 2013, 29–38.
[71] Nye, "Soft Power"; Keohane and Nye, *Power and Interdependence,* 86.
[72] Fabrizio Gilardi, "Transnational Diffusion: Norms, Ideas, and Policies," in *Handbook of International Relations* (1 Oliver's Yard, 55 City Road, London EC1Y 1SP United Kingdom: SAGE Publications Ltd, 2013), 453–77, https://doi.org/10.4135/9781446247587.n18.
[73] Joseph S. Nye, "Public Diplomacy and Soft Power," *The Annals of the American Academy of Political and Social Science* 616 (2008): 94–109; Anne-Marie Slaughter, "Leading through Law," *The Wilson Quarterly (1976-)* 27, no. 4 (2003): 37–44.
[74] Bradford, *The Brussels Effect*, 2020; Daniel W. Drezner, "Globalization and Policy Convergence," *International Studies Review* 3, no. 1 (2001): 53–78.

economies are particularly able to employ this method. Scholars disagree about whether or not soft power achieved through economic or political means amounts to coercion,[75] however discussion generally concentrates on the relative ability of the pressured population to resist or opt out of the outcome which the state would like to enforce as an indicator of coercion.[76] Soft power is attractive to states because it can maintain legitimacy without needing to expend the same extent of resources as hard power demands.[77]

In the literature, the EU has been singled out as a political entity which is particularly capable of cultivating soft power by encouraging international policy convergence in favor of European regulation.[78] Anu Bradford uses the term the "Brussels effect" to explain how five features specific to the EU and to EU institutions have given rise to the de facto and de jure adoption of EU regulations. First, as the largest economy in the world,[79] the EU already attracts producers to gain entrance into its lucrative market. However, Bradford is quick to point out that "not all states with large markets become sources of global standards."[80] The regulatory capacity to enforce sanctions depends on the quality of domestic institutions in the form of resources or regulatory expertise, is the second factor.[81] Third, the EU must have a political preference for strict rules.[82] Fourth, the EU must have a predisposition to regulate inelastic targets which makes it

[75] Tom J. Farer, "Political and Economic Coercion in Contemporary International Law," *American Journal of International Law* 79, no. 2 (1985): 405–13, https://doi.org/10.2307/2201710.
[76] Richard B. Lillich, "Economic Coercion and the International Legal Order," *International Affairs (Royal Institute of International Affairs 1944-)* 51, no. 3 (1975): 358–71, https://doi.org/10.2307/2616620.
[77] Nye, "Soft Power."
[78] "Anu Bradford, The Brussels Effect, 107 NW. U. L. REV. 1 (2012). Available at: Https://Scholarship.Law.Columbia.Edu/Faculty_scholarship/271," n.d.
[79] "EU Position in World Trade - Trade - European Commission," accessed April 25, 2020, https://ec.europa.eu/trade/policy/eu-position-in-world-trade/.
[80] Bradford, *The Brussels Effect*, 2020.
[81] "Anu Bradford, The Brussels Effect, 107 NW. U. L. REV. 1 (2012). Available at: Https://Scholarship.Law.Columbia.Edu/Faculty_scholarship/271," 12.
[82] Ibid.

difficult for actors to escape compliance by shifting operations to a different jurisdiction.[83] Finally, the non-divisibility of standards is the most significant feature that persuades corporations to globalize their operations to comply with the most stringent standard in jurisdictions other than the EU.[84] Because of the nature of data, it is often technically not feasible or too costly for a corporation to segment corporate practices according to jurisdictional limits.

The Internet provides an opportunity for states to employ soft power to an even greater degree. Since the Internet allows for multiple channels of communication amongst many jurisdictions, this provides states with more avenues to promulgate their standards and norms quicker than before the Internet.[85] In a way, complex interdependence becomes a strategy unto itself.[86] Cooperation allows states to forego hard power since they rely on one another to achieve some goal or resolve a challenge. At the same time, complex interdependence enables soft power since these channels remain open allowing states to compete with their relative regulatory capacities. With the appropriate institutional structure and legal framework, states can influence the behavior of non-state actors and reinforce their preferences in jurisdictions other than their own.

Methodology

This paper is motivated by two related empirical puzzles. First, it is surprising that the institutional and legal histories of these two states directly motivate their priorities when

[83] Bruce G. Carruthers and Naomi R. Lamoreaux, "Regulatory Races: The Effects of Jurisdictional Competition on Regulatory Standards," *Journal of Economic Literature* 54, no. 1 (2016): 52–97.
[84] Annegret Bendiek and Magnus Römer, "Externalizing Europe: The Global Effects of European Data Protection," *Digital Policy, Regulation and Governance* 21, no. 1 (January 1, 2019): 32–43, https://doi.org/10.1108/DPRG-07-2018-0038.
[85] Slaughter, "How to Succeed in the Networked World: A Grand Strategy for the Digital Age."
[86] Keohane and Jr, "Power and Interdependence in the Information Age"; Slaughter, "How to Succeed in the Networked World: A Grand Strategy for the Digital Age."

negotiating the EU-US data flow. The EU developed the GDPR out of a decades-long, multilateral approach to regulation which largely emerged from facilitation by intergovernmental organizations that predated the founding of the EU.[87] On the other hand, the US regulatory approach to data protection is highly fragmented, narrow, and primarily self-regulated, which does not reach the regulatory rigor of the EU model.[88] The relative differences in the two approaches become important when the two states came together to determine a bilateral agreement. These differences can also lead to the failure of agreements like the Safe Harbor Agreement, the predecessor of the Privacy Shield. Second, whether or not the Privacy Shield represents inter-state cooperation or legal interoperability is particularly important for the GDPR, since an agreement which falls short of compliance would require the suspension of the data flow.[89] As the EU attempts to promote its own priorities with the regulatory battle with the US, the GDPR endorses a particular norm of data protection through its extraterritorial effects, even to jurisdictions like the US that formerly lacked such a perspective.

The first research question is, how do different legal approaches to data protection in the US and the EU conform to expectations of state competition, as anticipated by CWS, or cooperation, an outcome predicted by complex interdependence scholars? The second research question is, why and how does the EU's GDPR exert its influence beyond its jurisdiction, and is its dominance likely to continue?

I will compare the relative regulatory capabilities of the EU in the US in the bilateral struggle over data protection as the result of their institutional and legal histories, which provides

---

[87] Gloria González-Fuster, *The Emergence of Personal Data Protection as a Fundamental Right of the EU*, Law, Governance and Technology Series, volume 16 (Cham ; New York: Springer, 2014).
[88] Daniel J. Solove and Paul M. Schwartz, *Information Privacy Law*, Fifth edition, Aspen Casebook Series (New York: Wolters Kluwer Law & Business, 2015).
[89] Christopher Wolf, "Delusions of Adequacy? Examining the Case for Finding the United States Adequate for Cross-Border EU-U.S. Data Transfers," *Washington University Journal of Law and Policy* 43, no. 1 (2014): 227–58.

a frame of reference when considering the stability of the GDPR's dominance. This paper will employ a process tracing methodology to better understand how models of data protection emerged in the EU and US, with particular attention to the European process that led to the creation of the GDPR. Therefore, one dependent variable is the GDPR itself. Second, I will focus on discerning the conditions which influence the dynamic relationship between the EU and the US over data protection to determine the appropriateness of either framework in explaining the relationship as either cooperative or competitive. While the presence or absence of these conditions cannot be causally linked to the outcome, primary and secondary sources will support inference judgments.

I relied on primary sources like public opinion polls, news media, official records of intergovernmental organizations, and government documents like reports, bills, laws and hearings. I referred to major cases from the European Court of Justice to either to clarify provisions of the GDPR or to shed light on the legality of EU-US data protection agreements under EU law. As it pertains the EU, I sourced government documents were primarily from the EU Commission, in the form of laws, adequacy decisions, and reports. Recommendations, reports, and proposals from the Organization of Economic Cooperation and Development (OECD) as well as the Council of Europe from 1960 to 1985, shed light on European cooperation efforts on data protection prior to the formation of the EU. I also used secondary sources include various academic scholarship including journal articles, scholarly books, handbooks, news media, and textbooks.

Overview of Thesis

I will argue that the EU is in a unique position to advance its own approach with the GDPR due to its institutional and legal history that evolved out of complex interdependence. The extraterritorial effects of the GDPR indicate that the EU has embodied soft power that allows the

EU to entice behavior in the US jurisdiction to comply with the regulation, despite the Privacy Shield which intends to lower the standard for US corporations. Therefore, I complicate the dichotomy of regulatory competition or regulatory cooperation by suggesting that, while complex interdependence remains important to understanding Internet governance, other conditions not captured by complex interdependence motivate state behavior as well.

The chapter break-down is as follows. Chapter 2 presents the GDPR as a regulation, demonstrating the degree of departure from precedent it raises, as well as the historical origins of European data protection law. Chapter 3 transitions to focus on the US case, explaining how data protection developed historically as a result of different processes and principles, in order to demonstrate the extent of legal misalignment between the two states even before a digital data flow connected the two jurisdictions. Additionally, Chapter 3 will present the observed extraterritorial effects of the GDPR as evidence of market-based harmonization in the US. Chapter 4 will focus on the efforts to achieve a bilateral agreement between the two states in order to approve the US for adequacy under the GDPR. Chapter 5 will consist of a theoretical analysis of the material presented in Chapter 2, 3, and 4, and weigh the merits of the frameworks introduced in this chapter.

Chapter 2: The General Data Protection Regulation and its Origins

The passing of the GDPR was hugely consequential. The GDPR is widely regarded as the strongest data protection law in the world, governing all of the data flows which either involve the EU directly, or that include the data of EU citizens.[90] The volume of the data flow is difficult to comprehend. For reference, the EU population is 446 million people, the third largest population in the world after China and India. Facebook collects an average of 29,000 data points on a user.[91] A simple calculation finds that Facebook collects 12,934,000,000,000 data points on EU users, alone. While the average number of data points collected for non-Facebook platforms is closer to 1,500,[92] these numbers are meant to crudely illustrate the fact that the GDPR is incredibly powerful in a large part because of the amount of data it is governing.

This chapter consists of two sections. The first section presents the contents of the GDPR, including the rights afforded to the user, organizational and technical requirements for corporations, and bureaucratic scaffolding which contributes to the GDPR's enforcement. The expansiveness of the GDPR elaborates upon a European tradition which values data protection as a human right;[93] however, the GDPR raises it to the highest level of stringency under EU law. This section will allow for analysis in Chapter 3 concerning the normative appeal of the GDPR that might motivate extraterritorial adoption.

The second section presents the origins of the GDPR. The EU achieved European integration via multilateral cooperation of EU member states, thereby conforming to many

[90] Satariano, "G.D.P.R., a New Privacy Law, Makes Europe World's Leading Tech Watchdog."
[91] "WATCH: Congressman Reveals How Many Data Points Facebook Has On You," The Daily Wire, accessed April 22, 2020, https://www.dailywire.com/news/watch-congressman-reveals-how-many-data-points-ryan-saavedra.
[92] Ibid.
[93] González-Fuster, *The Emergence of Personal Data Protection as a Fundamental Right of the EU*.

expectations of complex interdependence.[94] Before the EU was even formed, international organizations like the OECD and the Council of Europe played an instrumental role in facilitating multiple channels of communication among later EU member states.[95] The GDPR incorporates many recommendations proposed by the OECD and the Council of Europe in its own language. With the founding of the EU, the EU coupled pre-existing legal agreement on data protection with a supranational tier of institutionalization.[96]

The EU Really Wants to Protect (Everyone's) Data: The General Data Protection Regulation

The GDPR affords the data subject with the broadest rights to data protection in the world, which has resulted in notable attention on GDPR-related cases to understand how these rights manifest themselves in practice.[97] A data subject is legal jargon for "an identifiable natural person… who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person."[98] "Personal data" that is protected under the GDPR is any information related to the data subject. Besides this expansive definition of personal data, the GDPR also increases the scope of applicability by affording these rights to any data subject in the EU

[94] González-Fuster; Keohane and Nye, *Power and Interdependence*.
[95] Mark Phillips, "International Data-Sharing Norms: From the OECD to the General Data Protection Regulation (GDPR)," *Human Genetics* 137, no. 8 (August 2018): 575–82, https://doi.org/10.1007/s00439-018-1919-7; Alessandro Mantelero, "Regulating Big Data. The Guidelines of the Council of Europe in the Context of the European Data Protection Framework," *Computer Law & Security Review* 33, no. 5 (October 2017): 584–602, https://doi.org/10.1016/j.clsr.2017.05.011.
[96] Alasdair R. Young, "The European Union as a Global Regulator? Context and Comparison," *Journal of European Public Policy* 22, no. 9 (October 21, 2015): 1233–52, https://doi.org/10.1080/13501763.2015.1046902.
[97] Chris Jay Hoofnagle, Bart van der Sloot, and Frederik Zuiderveen Borgesius, "The European Union General Data Protection Regulation: What It Is and What It Means," *Information & Communications Technology Law* 28, no. 1 (January 2, 2019): 65–98, https://doi.org/10.1080/13600834.2019.1573501.
[98] Commission Regulation 16/679, 2016 O.J. (L 119) p 1-88.

regardless of nationality, meaning that a citizen from the US that visits the EU may gain the rights afforded to the data subject upon entering EU jurisdiction.[99]

The data subject is afforded comprehensive rights over his or her data, setting the conditions for negotiations between the data subject and third party. Transparent communication is required between entities which may handle personal data and the data subject. This is to ensure that the data subject is aware of the location of his or her personal data. The data subject is also afforded the right to access the information, the right to rectify or correct the information, the right to restrict processing of personal information, and the right to notification of when these actions are taken or completed.[100] The data subject also has the right to data portability, meaning that the he or she might transfer the personal data records which belong to him or her from one entity to another.[101]

To a certain extent, these rights reinforce the commodification of data, or the treatment of data as property, by setting the rules for bargaining between the data subject and third party.[102] The important caveat is that these rights persist even after a bargain has taken place, both assuring stringent protection of the rights as it migrates from the data subject to third party, recognizing the nature of data as non-rival. The data subject is also afforded the right to object to profiling or automated decision-making.[103] Profiling refers to the automated processing of personal data to evaluate certain things about an individual, such as the likelihood of purchasing a good or service;

[99] Commission Regulation 16/679, 2016 O.J. (L 119) p 1-88.
[100] Europäische Union and Europarat, eds., *Handbook on European Data Protection Law*, 2018 edition, Handbook / FRA, European Union Agency for Fundamental Rights (Luxembourg: Publications Office of the European Union, 2018).
[101] Europäische Union and Europarat.
[102] JACOB M. VICTOR, "The EU General Data Protection Regulation: Toward a Property Regime for Protecting Data Privacy," *The Yale Law Journal* 123, no. 2 (2013): 513–28.
[103] Commission Regulation 16/679, 2016 O.J. (L 119) p 1-88.

however, it has since expanded to be used in political campaigns as well.[104] Automated decision-making refers to the process of deciding by automated means without human involvement. For instance, this may take place in instances where algorithms are the sole determinant of outcomes; loan accreditations are a common example.[105]

The right to erasure, also known as the right to be forgotten, is the right which has received the most popular attention due to its novelty. Only the EU and Argentina have put the right to erasure into practice.[106] The right to erasure refers to the right to have personal data about the data subject removed from Internet searches and other directories such as Google. According to *Google v. Spain*, search engines are responsible for the content they point to, but are not required to do so globally.[107] The right to erasure is intended to return agency to the data subject regarding situations when there may be disclosures of their own personal data without their knowledge or consent and may hold perpetual consequences for them in the future. [108] For instance, the right to erasure may be extended in an instance of revenge porn, when one partner publicizes intimate photographs, images or videos that involve their partner without their consent.[109] Critics claim that is provides a legal basis for user-driven censorship. Google has received 650,000 requests to remove over 2.43 million URLs under the right to be forgotten, one of which involved a doctor requesting that

---

[104] "Data Is Power: Profiling and Automated Decision-Making in GDPR Report" (Privacy International, April 9, 2018), https://privacyinternational.org/report/1718/data-power-profiling-and-automated-decision-making-gdpr.
[105] Ibid.
[106] Rodrigo Cetina Presuel and Sebastián Zárate Rojas, "Introduction to the Special Issue: The Right to the Protection of One's Own Image in Ibero-America and Its Relevance for the Right of Publicity in Common Law Countries," *Journal of Information Policy* 8 (2018): 338–45, https://doi.org/10.5325/jinfopoli.8.2018.0338; "Google and Yahoo Win Appeal in Argentine Case - The New York Times," accessed April 29, 2020, https://www.nytimes.com/2010/08/20/technology/internet/20google.html?_r=0.
[107] C-131/12 Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González, 2014 E.C.R. 317.
[108] Alessandro Mantelero, "The EU Proposal for a General Data Protection Regulation and the Roots of the 'Right to Be Forgotten,'" *Computer Law & Security Review* 29, no. 3 (June 2013): 229–35, https://doi.org/10.1016/j.clsr.2013.03.010.
[109] Ibid.

information concerning his failed medical procedures be removed.[110] Others point to the archival importance of retaining original information, suggesting that doing otherwise may cause a rewriting of history. [111] The GDPR has limitations in paragraph 3 of Article 17 chiefly for this reason.[112]

While these rights empower the data subject in theory, the practical implementation of these rights have been contested. Researchers have been able to uniquely identify 95% of individuals in a sample set with just four data points.[113] For this reason, the GDPR also require organizational and technical measures from entities that control or process data, in order to ensure the fair treatment of disclosed information.[114] Depending on the size of the corporation, a data protection officer may be required to monitor data protection compliance, lead awareness training to educate employees about appropriate data protection practices, develop internal codes of conduct, and organize regular auditing.[115] The GDPR employs the Data Protection Impact Assessment (DPIA), which is a legally required document to help aid in the auditing process.[116] The GDPR uses the privacy-by-design and privacy-by default frameworks,[117] a proposed standard

---

[110] "Google Has Received 650,000 'Right To Be Forgotten' Requests Since 2014," NPR.org, accessed April 12, 2020, https://www.npr.org/sections/thetwo-way/2018/02/28/589411543/google-received-650-000-right-to-be-forgotten-requests-since-2014; David Payne, "Google, Doctors, and the 'Right to Be Forgotten,'" *BMJ: British Medical Journal* 350 (2015), www.jstor.org/stable/26517819.

[111] Tessa Mayes, "We Have No Right to Be Forgotten Online | Tessa Mayes," *The Guardian*, March 18, 2011, sec. Opinion, https://www.theguardian.com/commentisfree/libertycentral/2011/mar/18/forgotten-online-european-union-law-internet.

[112] Commission Regulation 16/679, 2016 O.J. (L 119) p 1-88.

[113] "Researchers Spotlight the Lie of 'Anonymous' Data," *TechCrunch* (blog), accessed April 12, 2020, https://social.techcrunch.com/2019/07/24/researchers-spotlight-the-lie-of-anonymous-data/.

[114] Paul Voigt and Axel von dem Bussche, *The EU General Data Protection Regulation (GDPR): A Practical Guide* (Cham, Switzerland: Springer, 2017); Europäische Union and Europarat, *Handbook on European Data Protection Law*.

[115] Commission Regulation 16/679, 2016 O.J. (L 119) p 1-88.

[116] "Data Protection Impact Assessment (DPIA)," GDPR.eu, August 9, 2018, https://gdpr.eu/data-protection-impact-assessment-template/.

[117] Ann Cavoukian and Fred Carter, "Privacy by Design: The 7 Foundational Principles – Implementation and Mapping of Fair Information Practices" (Internet Architecture Board, December 2010), https://www.iab.org/wp-content/IAB-uploads/2011/03/fred_carter.pdf.

according to the Internet Architecture Board (IAB), to outline the ways in which data protection is maintained technically, including systems security, encryption, and pseudonymization.[118] Pseudonymization is a means of de-identifying personal data from the data subject.[119] Those entities that lie outside of the EU must make "binding and contractual commitments towards the entity that transfers data to them, via contractual or other legally binding instrument,"[120] in order to apply these safeguards, and may be accompanied by a certification. [121] Should an entity be found to not comply with the GDPR, it receives a sanction of either 10 million euros or 4% of global turnover, whichever is larger.[122]

The GDPR also forwards the establishment of a "data protection regime" in the EU, by erecting a bureaucratic apparatus for handling data protection abuses.[123] Each state has a national data protection authority (DPA) that is responsible for enforcing data protection regulation in their jurisdiction, assessing complaints, and enforcing sanctions.[124] These DPAs have the technical background to handle issues related to data protection, and are therefore adept to handle unique, regulatory challenges.[125] At the same time, this means that there might be uneven enforcement of the GDPR according to the willingness of the state to invest resources towards the data protection authority. For instance, Ireland's DPA office is notoriously underfunded.[126] This network of national authorities reports to the EU Data Protection Supervisor (EDPS), whose responsibility is

[118] Cavoukian and Carter.
[119] Ibid.
[120] Commission Regulation 16/679, 2016 O.J. (L 119) p 1-88.
[121] Voigt and Bussche, *The EU General Data Protection Regulation (GDPR)*.
[122] Commission Regulation 16/679, 2016 O.J. (L 119) p 1-88.
[123] Farrell and Newman, *Of Privacy and Power*.
[124] Farrell and Newman.
[125] Anu Bradford, "The Brussels Effect," in *The Brussels Effect*, by Anu Bradford (Oxford University Press, 2020), 25–66, https://doi.org/10.1093/oso/9780190088583.003.0003.
[126] Nicholas Vinocur, "How One Country Blocks the World on Data Privacy," POLITICO, accessed April 29, 2020, https://politi.co/2PqFc42.

to ensure consistent application of the GDPR and promote cooperation amongst the DPAs.[127] Together, the EDPS and the DPAs comprise the European Data Protection Board which develops guidelines, delivers opinions, and provides legislation consultation, in the interest of EU-wide harmonization.[128]

The GDPR is therefore novel for a number of reasons. The GDPR is the first regulation for data protection of the EU. The scope of the GDPR extends the right to data protection to all data subjects in the EU, a significant departure from the its predecessor, the EU Data Protection Directive, which limits the right to data protection to EU citizens.[129] Data subject are bestowed with new rights like the right to be forgotten, the meaning of which is still being interpreted in the courts. While its implementation has attracted criticism claiming that the GDPR is too vague and difficult to understand to practically adopt, the GDPR established a data protection regime at both the national and supranational levels to provide guidance to corporations. Moreover, these authorities are empowered to enforce massive sanctions in cases of noncompliance, such that infringement comes at a high cost to corporations. However, the GDPR has attracted the most international attention because of its use of extraterritoriality.[130] The GDPR affords the EU the authority to come to an adequacy decision regarding the ability of third countries to maintain stringent data protection for EU data beyond the EU jurisdiction. The extraterritoriality of the

[127] "About," Text, European Data Protection Supervisor - European Data Protection Supervisor, November 11, 2016, https://edps.europa.eu/about-edps_en.
[128] "About EDPB," Text, European Data Protection Board - European Data Protection Board, January 10, 2018, https://edpb.europa.eu/about-edpb/about-edpb_en.
[129] Council Directive 95/46, 1995 O.J. (L 281) pg 31-50.
[130] Adèle Azzi, "The Challenges Faced by the Extraterritorial Scope of the General Data Protection Regulation," *JIPITEC* 9, no. 2 (2018): 126–37; Benjamin Greze, "The Extra-Territorial Enforcement of the GDPR: A Genuine Issue and the Quest for Alternatives," *International Data Privacy Law*, April 21, 2019, https://doi.org/10.1093/idpl/ipz003; SCOTT, "Extraterritoriality and Territorial Extension in EU Law."

GDPR, which allows the regulation to become truly "general," is covered in more depth in Chapter 3.

Born of Complex Interdependence: The European Approach to Data Protection

The GDPR is the result of a path-dependent trajectory of European data protection law, as well as the culmination of over half a century's worth of policy-making that conforms to the expectations of complex interdependence. International organizations serve an important function in complex interdependence, as forums where states may overcome differences, advocate for their policy of choice, and resolve shared problems.[131] For a continent of 44 countries, any of which have reciprocal effects on the other, international organizations were a primarily means of finding consensus prior to the EU. Prior to the EU, the OECD and the Council of Europe provided multiple channels of communication which sometimes gave rise to competing policy recommendations, later resolved under integration efforts by the EU.[132] The EU added a supranational level of institutionalization to pre-existing agreement forged in these international organizations, ultimately solidifying multilateral cooperation among member states.

Data protection emerged as a common concern across the continent in the late 1960s, in response to sweeping technological changes which enabled a scale of electronic data processing that was previously unforeseen.[133] At the time, government institutions were the primary processors of personal information, mostly in order to estimate demand for social services. While

[131] Keohane and Nye, *Power and Interdependence*.
[132] González-Fuster, *The Emergence of Personal Data Protection as a Fundamental Right of the EU*.
[133] Bart van der Sloot, "Privacy from a Legal Perspective," in *The Handbook of Privacy Studies*, ed. Bart van der Sloot and Aviva de Groot, An Interdisciplinary Introduction (Amsterdam University Press, 2018), 63–136, https://doi.org/10.2307/j.ctvcmxpmp.6; González-Fuster, *The Emergence of Personal Data Protection as a Fundamental Right of the EU*; Alexander D. Roth, "DOCUMENTS ON DATA PROTECTION," *International Legal Materials* 19, no. 2 (1980): 282–324.

Article 8 of the European Convention of Human Rights (ECHR) enshrined privacy as a human right in 1953, it was less clear whether that extended to data protection.[134]

The first question—that is, of whether data protection is privacy and thereby subject to treatment as a human right—was taken up by the Council of Europe. The Council of Europe is an international organization whose members founded in 1949 by ten European countries, with the intention of promoting human rights, democracy and rule of law in Europe. It is also the parent institution of the European Court of Human Rights (ECfHR), a supranational court which hears cases against member states concerning human rights breaches as outlined in the European Convention of Humans Rights (ECHR).[135] This means that the ECfHR directly wrestled with the conceptual challenges of defining data protection through its case law, since by the 1970s privacy had a status as a human right, while data protection did not.[136]

The Council of Europe found that it was "urgent, pending the possible elaboration of an international agreement, at once to take steps to prevent further divergencies between the laws of member states in this field,"[137] referring to differences in the data protection laws of member states, both in content and in type, located in constitutional law, statutory law, or entirely non-existent.[138] Most of these differences can be attributed to different legal systems or traditions, but some of this variety can be also traced to linguistic differences, since the ECHR was originally written in French. The French "vie privée" means privacy in French, however translates to English as

[134] Council of Europe. 1988. "Protocol to the Convention for the Protection of Human Rights and Fundamental Freedoms (European Convention on Human Rights) as Amended by Protocol No. 11." *Council of Europe Treaty Series 155*. Strasbourg: Council of Europe.
[135] A. C. Evans, "European Data Protection Law," *The American Journal of Comparative Law* 29, no. 4 (1981): 571–82, https://doi.org/10.2307/839754.
[136] González-Fuster, *The Emergence of Personal Data Protection as a Fundamental Right of the EU*.
[137] 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 (1973), 73.
[138] González-Fuster, *The Emergence of Personal Data Protection as a Fundamental Right of the EU*.

"private life," which is consequential for state adoption of the ECHR's recommendations into domestic law.[139] Moreover, the legitimacy of ECfHR decisions can be called into question if it lacks consistency on data protection cases.[140] Should the ECfHR interpret data protection according to the laws of one-member state but not others, it may be seemed to privilege certain states above others, or engaging in judicial activism.

Between 1973 and 1974, the Council of Europe made two resolutions to address these mounting concerns. Resolution 73 (22) and Resolution 74 (29) addressed the "protection of the privacy of individuals vis a vis electronic data banks" in the private and public sectors, respectively, offering principles to be adopted in domestic law.[141] These included several which arise in the GDPR, including the right of access, consent, erasure, correction, and data security.[142] Notably, neither of these resolutions addressed the issue of information being exchanged across data banks that may be located in different jurisdictions, or the transfer of data between a member state and a non-member state. Further, by separating privacy rights as they concern the private sector, independent of those privacy rights as they concern the public sector, they do not anticipate the collapsing of the private-public distinction as private companies cooperate with public entities.[143] However, the Council of Europe was primarily concerned with harmonizing a legal

---

[139] Ibid.
[140] VÍCTOR FERRERES COMELLA, "The Impact of the European Court of Human Rights," in *Constitutional Courts and Democratic Values*, A European Perspective (Yale University Press, 2009), 139–54, www.jstor.org/stable/j.ctt1np70w.16; C. A. Gearty, "The European Court of Human Rights and the Protection of Civil Liberties: An Overview," *The Cambridge Law Journal* 52, no. 1 (1993): 89–127.
[141] Council of Europe Committee of Ministers, Resolution (73) 22 on the protection of the privacy of in- dividuals vis-à-vis electronic data banks in the private sector (1973); Council of Europe Committee of Ministers, Resolution (74) 29 on the protection of in-dividuals vis-à-vis electronic data banks in the public sector (1974).
[142] Mantelero, "Regulating Big Data. The Guidelines of the Council of Europe in the Context of the European Data Protection Framework"; Cécile de Terwangne, "The Work of Revision of the Council of Europe Convention 108 for the Protection of Individuals as Regards the Automatic Processing of Personal Data," *International Review of Law, Computers & Technology* 28, no. 2 (May 4, 2014): 118–30, https://doi.org/10.1080/13600869.2013.801588.
[143] This issue later arises, with increased data-sharing collaboration between the intelligence agencies and corporations.

agreement in the domestic law of member states; after all, the issue of cross-border data flows may be passively resolved if the laws governing the data agreed transnationally.[144]

After a comprehensive study comparing data protection laws across its member states, the Convention for the Protection of Individuals with regard to Automatic Processing of Person Data, or Convention 108,[145] was ratified by all member states of the Council of Europe in 1981, and has since been ratified by all EU member states. Convention 108 was significant for several reasons, one being that it is the first multilateral treaty to acknowledge the nuance of data protection as a concept, while also defining it as an independent concept in its own right. It was the first to define data protection.[146] Convention 108 further addressed the issue of cross-border data flows, stating that it "should make no difference for data users or data subjects whether data processing operations take place in one or several countries… data subject should be given the same safeguards for the protection of their rights and interests."[147] In response to Convention 108, the UK, Netherlands, Belgium and Ireland all passed data protection laws in the next few years, further harmonizing data protection across the continent.[148]

While the Council of Europe tackled the legal challenges of standardizing data protection, the OECD first became interested in the issue of data protection as it became a potential barrier to trans-border data flows, thereby posing a threat to free trade.[149] The OECD is an intergovernmental

---

[144] P. Howard Patrick, "PRIVACY RESTRICTIONS ON TRANSNATIONAL DATA FLOWS: A COMPARISON OF THE COUNCIL OF EUROPE DRAFT CONVENTION AND OECD GUIDELINES," *Jurimetrics* 21, no. 4 (1981): 405–20.

[145] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Strasbourg, 28 January 1981, European Treaty Series No. 108.

[146] Convention 108 defines data protection as, "the legal protection of individuals with regard to automatic processing of personal information relating to them."

[147] "Explanatory Report to the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data" (Strasbourg: Council of Europe, 1981), 3.

[148] González-Fuster, *The Emergence of Personal Data Protection as a Fundamental Right of the EU*.

[149] Michael Kirby, "The History, Achievement and Future of the 1980 OECD Guidelines on Privacy," *International Data Privacy Law* 1, no. 1 (October 5, 2010): 6–14, https://doi.org/10.1093/idpl/ipq002.

economic organization, with the main purpose of promoting economic development and free trade through non-binding policy recommendations.[150] The purpose of the OECD therefore closely links to the purpose of the EU, that is to facilitate the EU internal market and guarantee the four free movements of goods, services, capital and labor.

Starting in 1968, the OECD began committing significant resources towards the issue of electronic processing and trade, including several reports, seminars, and ministerial meetings, working parties and symposiums.[151] While the OECD was less preoccupied with the distinction between data protection and privacy and used the concepts interchangeably in its work, it did acknowledge that data protection is important towards the safeguarding of human liberties and freedoms.[152] With respect to economic competition, the OECD noted that some European countries used stringent data protection laws as a legal barrier to the exporting of data beyond its jurisdiction, which may challenge the maintenance of an open data flow. This was in order to prevent entities from avoiding domestic regulation by transferring data to 'data havens,' or countries with less stringent protection.[153]

In 1980, the OECD released "The 1980 Guidelines on the Protection of Privacy and Trans-border Flows of Personal Data," which raised eight basic principles for national application, and four basic principles for international application.[154] Many of the principles for national application were later repeated in Convention 108 which was passed the next year, reflective of the fact that

[150] "About the OECD - OECD," accessed April 30, 2020, https://www.oecd.org/about/.
[151] González-Fuster, *The Emergence of Personal Data Protection as a Fundamental Right of the EU.*
[152] OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, adopted on 23 September 1980.
[153] Kirby, "The History, Achievement and Future of the 1980 OECD Guidelines on Privacy."
[154] OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, adopted on 23 September 1980.

many member states of the OECD were also member states of the Council of Europe.[155] Contrary to Convention 108, The OECD recommended that member states ensure that trans-border flows are "uninterrupted and secure," even if it requires member states to subordinate "developing laws, policies and practices in the name of privacy and individual rights, which would create obstacles to trans-border flows of personal data."[156] This suggests that member states sacrifice data protection in the interest of their citizens for the sake of trans-border harmonization, and directly comes into conflict with the notion of data protection as a human right. Nevertheless, the OECD does provide a situation in which it recommends discontinuing data flows. If the third country "does not yet substantially observe these Guidelines"[157] in its national application when engaging in a data flow with an OECD member state, the member state has the right to discontinue the data flow. This principle is reminiscent of the adequacy decision under the GDPR, which empowers the EU to discontinue data flows to third countries that lack a comparable legal framework for data protection, thereby not being able to afford adequate protection to the personal information of EU citizens either.[158] The 1980 Guidelines served as a valuable counterweight to Convention 108. While acknowledging the data protection concerns of Convention 108, it likewise cautioned against stringent, domestic rule-making in the interest of fostering conditions towards shared economic prosperity.[159]

[155] Patrick, "PRIVACY RESTRICTIONS ON TRANSNATIONAL DATA FLOWS: A COMPARISON OF THE COUNCIL OF EUROPE DRAFT CONVENTION AND OECD GUIDELINES."
[156] OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, adopted on 23 September 1980, 3.
[157] OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, adopted on 23 September 1980, 3.
[158] Commission Regulation 16/679, 2016 O.J. (L 119) p 1-88.
[159] Kirby, "The History, Achievement and Future of the 1980 OECD Guidelines on Privacy"; Phillips, "International Data-Sharing Norms"; Patrick, "PRIVACY RESTRICTIONS ON TRANSNATIONAL DATA FLOWS: A COMPARISON OF THE COUNCIL OF EUROPE DRAFT CONVENTION AND OECD GUIDELINES."

By the time the EU was established in 1993, nearly all of its members had some type of data protection law that had developed with the guidance of the OECD and the Council of Europe.[160] An organization of supranational and intergovernmental governance, the chief purpose of the EU is European integration by economic, political and social means.[161] Therefore, EU can be thought of as a hybrid of the goals of the Council of Europe and the OECD, with the important distinction that the EU holds significantly more authority over its member states. The Treaty on the Functioning of the European Union outlines a system of competences which defines those policy topics which fall to the exclusive authority of the EU, the exclusive authority of member state, or shared authority.[162] This system favors regulation towards economic and social unity which is an exclusive competence of the EU, while maintaining respect for the sovereignty of its sub-states. Regulation has emerged as the preferred mechanism for expressing power, largely because of this structural limitation on the authority of the EU.[163] For instance, the EU is unable to collect taxes or wage war.[164]

This authoritative hierarchy is supplemented by a legal framework which consists of primary and secondary law. Primary law consists of treaties and charters, including the Charter of the Fundamental Rights of the EU which lists both data protection and privacy as distinct rights, indicative of the influence of the Council of Europe.[165] Secondary law consists of directives, regulations, decisions, recommendations and opinions, with the distinction between a directive

---

[160] González-Fuster, *The Emergence of Personal Data Protection as a Fundamental Right of the EU*.
[161] "The Historical Development of European Integration," European Union, June 18, 2018.
[162] Consolidated versions of the Treaty on European Union and the Treaty on the Functioning of the European Union (TFEU) [2016] OJ C202/1, Stephanie Switzer, "THE 'MAKING' OF THE EUROPEAN UNION," in *European Law Essentials* (Edinburgh University Press, 2009), 1–12, www.jstor.org/stable/10.3366/j.ctt1g09xcb.6.
[163] Veronica L Taylor, "Regulatory Rule of Law," in *Regulatory Theory*, ed. PETER DRAHOS, Foundations and Applications (ANU Press, 2017), 393–414, www.jstor.org/stable/j.ctt1q1crtm.33.
[164] Bradford, *The Brussels Effect*, 2020.
[165] "Types of EU Law," Text, European Commission - European Commission, accessed April 30, 2020, https://ec.europa.eu/info/law/law-making-process/types-eu-law_en.

and regulation being that that a directive provides a legislative goal for EU states to achieve, while leaving it up to the states to determine the appropriate means of implementing that law.[166] Directives serve as a way for states to harmonize their priorities while maintaining the states' sovereignty. Directives are also often a preliminary step towards a regulation, with a regulation consisting of a requirement for universal application from all members. The 1995 Data Protection Directive was the first directive with respect to data protection, and the precursor to the GDPR.

The judicial branch of the EU is the European Court of Justice (ECJ), which is tasked with both taking on cases by member states, institutions, and cases referred to it by the courts of member states, in addition to cases taken by individuals and companies directly.[167] Due to direct effect and supremacy, member states may be required to automatically apply judicial judgments to sovereign law.[168] In combination with the system of competences, this facilitates a degree of legal harmonization formerly not achieved by other international courts like the ECfHR, exemplified by the fact that Convention 108 was not binding. Nevertheless, the two courts agree on many issues, often citing the judicial decisions of one another in their own case law, and the ECHR served as a reference point for the Charter of Fundamental Rights of the EU.[169] As a result, it is no surprise that Convention 108 provided a foundation for the EU when drafting the Data Protection Directive in 1995, or later with the GDPR.[170]

The EU relies on an extensive, bureaucratic apparatus to enforce regulation with the cooperation of sub-states.[171] The European Parliament is the main legislative branch, with officials

[166] "Types of EU Law."
[167] Stephanie Switzer, "THE EUROPEAN INSTITUTIONS," in *European Law Essentials* (Edinburgh University Press, 2009), 19–34, www.jstor.org/stable/10.3366/j.ctt1g09xcb.8.
[168] Bradford, "The Brussels Effect," 2020.
[169] Anthony Arnull, *The European Union and Its Court of Justice*, 2nd ed, Oxford EC Law Library (Oxford ; New York: Oxford University Press, 2006), 399-400.
[170] González-Fuster, *The Emergence of Personal Data Protection as a Fundamental Right of the EU*.
[171] Switzer, "THE EUROPEAN INSTITUTIONS."

elected to the Parliament as representatives of the interests of their country.[172] On the contrary, the executive branch the Commission is elected from the European Parliament to represent the holistic "European vision," that is proposing legislation and implementing decisions towards the goal of a European Single Market.[173] The logic of economic integration drives decision-making by the Commission, which involves reducing barriers to trade, improving the efficient allocation of resources, and promoting competition, resembling the goals of the OECD. "The EU subscribes to a view that trade liberalization fails to achieve economic goals without a simultaneous harmonization of policies."[174]

Legal harmonization is in service to the European Single Market, standardizing conditions for trade across jurisdictions, thereby minimizing transaction costs and encouraging economies of scale.[175] Stringent rules arise in order to ensure state adherence to the EU policies, and this case especially arises with data protection since it is enshrined as a human right.[176] For niche policy areas like data protection, whose consistent enforcement may require technical expertise, there are national agencies tasked with ensuring the application of EU law. For instance, national data protection authorities (DPAs) supervise the application of data protection law, provide advice on data protection issues, manage complaints filed under the GDPR, and enforce their own fines.[177] DPAs the European Data Protection Supervisor make up the European Data Protection Board (EDPB).[178]

---

[172] Switzer.
[173] Switzer.
[174] Bradford, "The Brussels Effect," 2020, 24.
[175] Alasdair Blair and Steven Curtis, "European Integration," in *International Politics*, An Introductory Guide (Edinburgh University Press, 2009), 265–93, www.jstor.org/stable/10.3366/j.ctt1g0b1tz.18; Chris Allen et al., "The Competition Effects of the Single Market in Europe," *Economic Policy* 13, no. 27 (1998): 441–86.
[176] Bradford, "The Brussels Effect," 2020.
[177] Bradford.
[178] "About EDPB."

Unlike the OECD which is concerned with the global economy, the EU is concerned with the internal economy amongst member states. The role of international organizations prior to the founding of the EU helped foster some multilateral consensus concerning data protection, allowing the EU to expand upon their work. In 2015, the European Single Market was supplemented by a goal of a Single Digital Market, an initiative of a Europe 2020 proposed strategy towards the growth of the digital economy, like e-commerce, digital marketing and telecommunications.[179] By reinforcing its economic integration with a legal framework based on shared values like data protection, in addition to institutions at the national and supranational level, the EU is able to manage a regulatory regime which gives rise to regulations like the GDPR.

Conclusion

This chapter provides valuable insights concerning the logic of the EU behind the GDPR. The EU is predisposed to prefer cooperation due to its own institutional and legal history. Prior to the forming of the EU, international organizations like the OECD and the Council of Europe provided the first forums tasked with addressing data protection, which allowed for conceptual linkage among member states to develop. Further, since the OECD and the Council of Europe are themselves preoccupied with distinct goals—that is global economic trade and human rights in Europe, respectively—the two organizations raised a variety of data protection concerns. As a result, this challenged member states to formulate solutions that were fairly comprehensive, raising general principles for data protection that will later be adopted by the EU. This is a particularly

[179] J Scott Marcus, "Contribution to Growth:The European Digital Single Market Delivering Economic Benefits for Citizens and Businesses," n.d., 88; H.E. Carl Bildt et al., "A Transatlantic Digital Marketplace:," Building a Transatlantic Digital Marketplace: (Atlantic Council, 2016), JSTOR, www.jstor.org/stable/resrep03652.7; "Shaping Europe's Digital Future," Text, Shaping Europe's digital future - European Commission, accessed April 30, 2020, https://ec.europa.eu/digital-single-market/en.

impressive feat since much of this occurred in the 1960s to 1980s, before the advent of the commercial Internet.

As an intergovernmental and supranational organization, the EU relies on its member states in order to achieve legal harmonization and coordinate the internal market. The foundation of consensus among member states regarding data protection, already established by the OECD and the Council of Europe, minimized adjustment costs incurred by EU member states when the EU tried to implement regulation at the supranational level. The political will to dedicate resources to data protection was already shared by EU member states, which helped the EU later pass more stringent regulation like the GDPR. Further, the EU institutionalized data protection by buttressing stringent rules with the bureaucratic support of national DPAs, harmonized under the supervision of the EDPS, which ensured consistent application for all data flows in the internal digital market.

Therefore, the GDPR is the result of a path-dependent trajectory of European data protection law that builds upon over half a century's worth of policy making. Many of the rights afforded under the GDPR like the right to access, the right to rectify, and the right to notification, originated in forums prior to the EU. In turn, the GDPR was able to attain a high level of stringency, in the form of expansive rights of the data subject, compliance requirements, and high sanctions, which secured legal harmonization across the continent. While this internal process was largely motivated by the EU priority to organize its internal market, Chapter 3 will demonstrate how this institutional and legal history afforded the EU a competitive advantage in the form of soft power that allowed it to forward the GDPR extraterritorially in other jurisdictions in general, and the US in particular. The GDPR was able to gain attraction for several reasons, largely because it was the product of multilateral deliberation internally, but also because of its normative appeal in response to privacy scandals of the 21st century like Cambridge Analytica.

Chapter 3: The Extraterritorial Effects of the GDPR in the US Case

The extent to which legal incompatibility has been codified in domestic legal frameworks can serve as a significant barrier to drafting a bilateral agreement which rests upon conceptual linkage, or coming to a consensus about the extent to which data should be protected.[180] The evidence in the first section of this chapter reveals alternative logics to data protection that emerged out of two different policy-making processes, contrasting the EU approach illustrated in Chapter 2, with that of the US. Since the US does not consider data protection a constitutional right, the US subjugates data protection to the regulatory responsibility of US states, which has led to a patchwork of data protection laws across the country.[181] The logic of laissez-faire governance in service of economic growth, further narrows the likelihood that the US framework will achieve the same regulatory rigor as the EU.[182]

While these are structural differences, there are also cultural factors which give rise to this result. Data protection law is derivative from privacy, a socio-legal concept which has been debated since Aristotle.[183] A state can codify privacy in a variety of ways, since privacy is both a

[180] Hanrieder, "Compatibility and Consensus: A Proposal for the Conceptual Linkage of External and Internal Dimensions of Foreign Policy"; Maximilian von Grafenstein, "Conceptual Definitions as a Link for Regulation," in *The Principle of Purpose Limitation in Data Protection Laws*, 1st ed., The Risk-Based Approach, Principles, and Private Standards as Elements for Regulating Innovation (Nomos Verlagsgesellschaft mbH, 2018), 61–108, www.jstor.org/stable/j.ctv941v5w.4.
[181] "Reforming the U.S. Approach to Data Protection and Privacy," Council on Foreign Relations, accessed April 30, 2020, https://www.cfr.org/report/reforming-us-approach-data-protection; "In Privacy Laws, an Incomplete American Quilt - The New York Times," accessed April 30, 2020, https://www.nytimes.com/2013/03/31/technology/in-privacy-laws-an-incomplete-american-quilt.html.
[182] Mary J. Culnan, "Protecting Privacy Online: Is Self-Regulation Working?," *Journal of Public Policy & Marketing* 19, no. 1 (2000): 20–26; Solove and Schwartz, *Information Privacy Law*.
[183] Priscilla M. Regan, "Privacy as a Philosophical and Legal Concept," in *Legislating Privacy*, Technology, Social Values, and Public Policy (University of North Carolina Press, 1995), 24–41, www.jstor.org/stable/10.5149/9780807864050_regan.6.

concept which is really a combination of interrelated categories,[184] and highly dependent on cultural factors. For instance, the US is primarily concerned with privacy as it concerns shielding the individual from the government, while the EU applies privacy law to protect the individual from both public and private entities.[185] CWS anticipates that these structural differences and cultural factors represent significant challenges in harmonizing data protection across states, especially with legal attitudes as disparate as that of the EU and the US.

The second section will point to the mechanisms which have allowed for the GDPR to be exported to the US, highlighting the EU's novel use of extraterritoriality in the regulation. Extraterritoriality allows a state to extend its legal authority beyond its territorial jurisdiction. Despite the effort by the US to shield itself from EU data protection law through bilateral agreements, the extraterritorial effects of the GDPR show that the opposite is true, and the law has had a significant impact on many sectors of American society exhibiting its soft power.[186] The third section will focus on evidence that suggests the extraterritorial effects of the GDPR are manifesting in the US, a jurisdiction which has otherwise been opposed to EU data protection regulation. The US and the EU attempted to overcome legal incompatibility by using bilateral agreements to allow for a mutually beneficial outcome.[187] The outcomes of these agreements will be covered in Chapter 4.

---

[184] Solove, "Conceptualizing Privacy."
[185] Mendez and Mendez, "Comparing Privacy Regimes: Federal Theory and the Politics of Privacy Regulation in the European Union and the United States."
[186] Bradford, "The Brussels Effect," 2020.
[187] "European Commission Launches EU-U.S. Privacy Shield," Text, European Commission - European Commission, accessed April 15, 2020, https://ec.europa.eu/commission/presscorner/detail/en/IP_16_2461; Farrell, "Constructing the International Foundations of E-Commerce—The EU-U.S. Safe Harbor Arrangement."

Patching Up Privacy: The American Approach to Data Protection

The American approach to data protection is born of an entirely different legal tradition in comparison to that of the EU. Unlike the EU which adopted data protection and privacy as human rights in primary law, the US does not extend constitutional protection to privacy in the first place.[188] It is no surprise, then, that the GDPR has been so impactful in the US. For a jurisdiction that altogether lacks a comprehensive legal framework for data protection at the federal level, the US is particularly susceptible to a regulation like the GDPR since the US must pivot from no data protection regulation to significant investments towards the maintenance of adequacy.[189] This takes various forms, some of which include corporate obligation regarding compliance, as well as diplomatic resources committed to the continued success of the Privacy Shield.[190]

Supreme Court Justice Louis Brandeis was one of the first Americans to raise privacy concerns in response to technological change; in his case, instantaneous photography and the potential to have a photograph taken and circulated without consent of the subject.[191] There are constitutional amendments like the Third, Fourth or Fifth Amendments, which suggest a right to privacy implicitly.[192] However, this penumbral right to privacy is predominantly concerned with curtailing the government from intrusion into the home, or infringing upon other personal intimacies of private life, like political affiliation, sexual preferences or school records.[193] The primary constraint to the penumbral right to privacy is the explicit protection for free speech under

[188] Solove and Schwartz, *Information Privacy Law*.
[189] Lior Jacob Strahilevitz, "Reunifying Privacy Law," *California Law Review* 98, no. 6 (2010): 2007–48.
[190] Farrell and Newman, *Of Privacy and Power*.
[191] SAMUEL D. BRANDEIS LOUIS D WARREN, "The Right to Privacy.".
[192] R H Clark, "Constitutional Sources of the Penumbral Right to Privacy," *Villanova Law Review* 19 (n.d.): 53.
[193] Clark.

the First Amendment, which champions the exercise of free speech over any privacy concerns.[194] Further, there is a noticeable dearth of federal privacy laws that address the private sector at all, except for certain industries that handle categories of sensitive data like the financial services industry or the healthcare industry.[195]

The American-laissez faire system provides a significant contrast to the European model of regulation. The Europeans encourage economic competition via data protection standards, providing consistent conditions for trade across the Union thereby streamlining cross-border data flows.[196] As a sovereign country, the US does not need to preoccupy itself with economic cohesion as much as the EU does, since it does not need to justify its legitimacy to the same extent since the US is a nation-state while the EU operates like a political entity. On the contrary, the US has a preference for light regulation which encourages private entities to self-regulate.[197] The assumption is that companies will assess the appropriate level of regulation as responsive to consumer demand for regulation, and determine the means of meeting that demand according to their technical and organizational abilities.[198] However, companies have little incentive to self-regulate data protection of their own volition because of the economic profits associated with exploiting user data.[199] Companies are driven towards data extraction and analysis to either customize services in accordance with user preferences, or to conduct experiments on users in real time to understand consumer behavior.[200] The former manifests itself as features like "suggested

[194] Wolf, "Delusions of Adequacy? Examining the Case for Finding the United States Adequate for Cross-Border EU-U.S. Data Transfers."
[195] Culnan, "Protecting Privacy Online: Is Self-Regulation Working?"
[196] Blair and Curtis, "European Integration."
[197] Norman E. Bowie and Karim Jamal, "Privacy Rights on the Internet: Self-Regulation or Government Regulation?," *Business Ethics Quarterly* 16, no. 3 (2006): 323–42.
[198] Tom O'Malley and Clive Soley, "Privacy and Self-Regulation," in *Regulating the Press* (Pluto Press, 2000), 165–74, https://doi.org/10.2307/j.ctt183q680.13.
[199] Shoshana Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*, First Trade Paperback Edition (New York: PublicAffairs, 2020).
[200] Zuboff.

friends" on Facebook, while the latter is used by platforms like eBay to understand the economics of auctions.

The responsibility of data protection laws has therefore been delegated to the states, which may explain why the de jure effect of the GDPR has primarily been at the state level.[201] Among the states, California is a leader in privacy regulation.[202] In 1972, the state introduced a right to privacy from both public and private entities in its constitution, signaling a dedication akin to the ECHR.[203] As the home of Silicon Valley, whose residents include Facebook, Apple, and Google, California has a special priority to regulate the technology industry. Most regulation has been reactionary, since California is often the first to experience negative externalities due to its proximity to the industry. For instance, data breach notifications were first required in California in 2012, and by 2013 almost every other state had adopted a similar law.[204] The string of copy-cat laws that followed the passing of the CCPA by other states further indicate evidence of the so-called "California effect" which is the shift of regulation in other state jurisdictions in the direction of a state with stricter regulatory standards.[205] Therefore, California may be a catalyst towards potentially stitching together the US patchwork system for data protection regulation towards a federal data protection law.[206]

While neither privacy nor data protection are a priority of the federal government, national security is enshrined as a federal responsibility in the US Constitution, which has also served as a

---

[201] Alessandra Suuberg, "The View from the Crossroads: The European Union's New Data Rules and the Future of U.S. Privacy Law," *Tulane Journal of Technology and Intellectual Property* 16 (2013): 267.
[202] Wolf, "Delusions of Adequacy? Examining the Case for Finding the United States Adequate for Cross-Border EU-U.S. Data Transfers."
[203] Margaret Betzel, Privacy Law Developments in California
[204] Wolf, "Delusions of Adequacy? Examining the Case for Finding the United States Adequate for Cross-Border EU-U.S. Data Transfers."
[205] David Vogel, *Trading up: Consumer and Environmental Regulation in a Global Economy* (Cambridge, Mass: Harvard University Press, 1995).
[206] "Road to Adequacy: Can California Apply Under the GDPR?," Lawfare, April 22, 2019, https://www.lawfareblog.com/road-adequacy-can-california-apply-under-gdpr.

barrier to the right to privacy for American citizens. The bureaucratization of national security did not begin until after WWII, when the US emerged as a great power.[207] The Central Intelligence Agency (CIA) was erected in 1947 to gather information on foreign adversaries, often in cooperation with other countries like the Five Eyes, an intelligence alliance among the US, Australia, Canada, New Zealand and the United Kingdom which consists of the sharing of intercepted telephone calls, texts, e-mails, and other digital correspondence.[208] After WWII, the justification for the continued existence of the Five Eyes alliance was the Cold War. Following the eclipse of the Cold War, terrorism emerged as the latest transnational threat to national security which further demanded information gathering.[209] Intelligence alliances exist in Europe as well like the Club de Bern is an intelligence sharing agreement among the sub-states of the EU, Norway, and Switzerland, however this alliance is not organized at the EU level.[210]

The US struggled to distinguish the responsibilities of the CIA from the Federal Bureau of Investigations (FBI), which is the domestic intelligence and security agency. The FBI also has a law enforcement function while the CIA does not. The two agencies often ran into conflict with one another concerning jurisdiction, exemplified by the Watergate Scandal during which Nixon encouraged strained inter-agency relations in order to cover up presidential abuses of power.[211] After fall-out from the Watergate Scandal, barriers were erected to limit the possibility of domestic surveillance on US citizens with the passing of the Privacy Act of 1974 to further cement the

---

[207] Laura K Donohue, *The Future of Foreign Intelligence: Privacy and Surveillance in a Digital Age*, 2016, http://public.ebookcentral.proquest.com/choice/publicfullrecord.aspx?p=4717489.
[208] Elizabeth Sherwood-Randall, "ALLIANCES AND AMERICAN NATIONAL SECURITY" (Strategic Studies Institute, US Army War College, 2006), JSTOR, www.jstor.org/stable/resrep11189.
[209] Farrell and Newman, *Of Privacy and Power*; Pia Philippa Seyfried, "A European Intelligence Service?" (Federal Academy for Security Policy, 2017), JSTOR, https://doi.org/10.2307/resrep22196.
[210] Wolf, "Delusions of Adequacy? Examining the Case for Finding the United States Adequate for Cross-Border EU-U.S. Data Transfers."
[211] Mark Riebling, *Wedge: From Pearl Harbor to 9/11: How the Secret War between the FBI and CIA Has Endangered National Security*, 1st Touchstone ed., Updated with a new epilogue (New York: Simon & Schuster, 2002, 2002).

difference between the FBI and the CIA.[212] A third intelligence agency, the National Security Agency (NSA), operates under the purview of the Department of Defense and specializes in cryptology efforts, computer network operations, and cybersecurity.[213] While the work of the NSA requires less coordination with the other two agencies, it is especially important to this discussion because the information it collects is primarily through the Internet.

Many of these barriers between the CIA and FBI fell away after the September 11th terrorist attacks.[214] Four planes were hijacked by 19 members of the Islamic terrorist group al-Qaeda and crashed into the World Trade Center in New York City, the Pentagon in Arlington, VA, and a field in Shanksville, Pennsylvania, but it was intended to target Washington D.C. The attacks resulted in nearly 3,000 fatalities, and is the single deadliest terrorist attack in human history.[215] The US government was criticized for not doing enough to prevent the attacks, compelling Congress to pass legislation which expanded the powers of existing policing and intelligence agencies, as well as establishing the Department of Homeland Security in 2002 to coordinate anti-terrorist efforts.[216]

The "wall" between the CIA and the FBI fell away, as the war on terror required increased coordination between domestic law enforcement and foreign intelligence. [217] The Patriot Act was signed into law in 2001 with a single opposing vote in the Senate.[218] It expanded the scope, power, and availability of information to the CIA, FBI and the NSA. The Patriot Act allowed for the

---

[212] R Seamon and W Gardner, "The Patriot Act and the Wall between Foreign Intelligence and Law Enforcement," *Harvard Journal of Law & Public Policy* 28, no. 2 (2005): 319–464.
[213] "About Us," accessed April 30, 2020, https://www.nsa.gov/about/; "National Security Agency Central Security Service > What We Do > Understanding the Threat," accessed April 30, 2020, https://www.nsa.gov/what-we-do/understanding-the-threat/; Riebling, *Wedge*.
[214] Seamon and Gardner, "The Patriot Act and the Wall between Foreign Intelligence and Law Enforcement"; Farrell and Newman, *Of Privacy and Power*; Richard J. Harknett and James A. Stever, "The Struggle to Reform Intelligence after 9/11," *Public Administration Review* 71, no. 5 (2011): 700–706.
[215] Congressional Record, V. 148, PT. 7, May 23, 2002 to June 12, 2002.
[216] Seamon and Gardner, "The Patriot Act and the Wall between Foreign Intelligence and Law Enforcement."
[217] Seamon and Gardner.
[218] "H.R. 3162 (107th): Uniting and Strengthening America by Providing Appropriate ... -- Senate Vote #313 -- Oct 25, 2001," GovTrack.us, accessed April 30, 2020, https://www.govtrack.us/congress/votes/107-2001/s313.

collection of foreign intelligence information from both US and non-US citizens, broadened the lawful interception of wiretapping, and necessitated obligatory and voluntary disclosure of customer communications by cable companies.[219] The Patriot Act also empowered all three agencies to use National Security Letters (NSLs) which is a demand letter issues to a particular entity or organization to turn over various records including telephone, e-mail, financial records and other data pertaining to individuals without a court order.[220] Subpoenas to Internet Service Providers (ISPs) may include detailed information such as: name, address, local and long-distance telephone billing records, telephone number or other subscription number or identity, length of service of a subscriber, session times, types of services used, IP addresses, bank accounts, and credit card numbers.[221] The role of ISPs is particularly poignant for the purposes of this discussion, since it allows US surveillance agencies to employ Internet to achieve a level of detail which was previously impossible.

Other provisions which have attracted attention include the authorization of indefinite detentions of immigrants and the permission to law enforcement to search a home or business without the knowledge of the business-owner or resident.[222] The breadth of information gathering was justified out of fear of lone wolf terrorist attacks, or an attack by an individual that acts

[219] Nathan C. Henderson, "The Patriot Act's Impact on the Government's Ability to Conduct Electronic Surveillance of Ongoing Domestic Communications," *Duke Law Journal* 52, no. 1 (2002): 179–209, https://doi.org/10.2307/1373134.
[220] "National Security Letters," American Civil Liberties Union, accessed April 30, 2020, https://www.aclu.org/other/national-security-letters.
[221] USA PATRIOT Act (U.S. H.R. 3162, Public Law 107-56).
[222] "NPR: The Patriot Act: Key Controversies," accessed April 30, 2020, https://www.npr.org/news/specials/patriotact/patriotactdeal.html; Dara Lind, "Everyone's Heard of the Patriot Act. Here's What It Actually Does.," Vox, June 2, 2015, https://www.vox.com/2015/6/2/8701499/patriot-act-explain; Henderson, "The Patriot Act's Impact on the Government's Ability to Conduct Electronic Surveillance of Ongoing Domestic Communications"; "What Is the USA Patriot Web," accessed April 30, 2020, https://www.justice.gov/archive/ll/highlights.htm.

independent of assistance from a terrorist organization. There were two extensions to key provisions granted in 2005 and 2011, however to increasing bipartisan scrutiny.[223]

The 2013 Snowden Revelations marked a watershed moment for US intelligence. Edward Snowden, then a contractor for the NSA, stole over 1,7 million US intelligence files, in addition to 15,000 Australian intelligence files, and 58,000 British intelligence files.[224] With the cooperation of journalists at various media outlets including the New York Times, the Washington Post, and the Guardian, among others, Snowden confirmed the extent of information sharing amongst the Five Eyes countries.[225] The documents also shed light on other secret treaties between the NSA and the intelligence agencies of other countries, including Denmark, France, Germany Italy, the Netherlands, Norway, Spain, Switzerland, Singapore, and Israel, as well as cases when the NSA engaged in the surveillance of populations without the consent of the domestic government.[226] The NSA program, "Treasure Map," in collaboration with British intelligence, seeks to map the Internet by not only identifying the information which is on the Internet, but also identifying the devices which connect to the Internet. [227] The disclosures, which were spread out over the course of the next year, further exposed the private-public collaboration enabled under the Patriot Act with US intelligence agencies. The metadata of international communications were sourced from internet companies like Microsoft, Yahoo, Google, Facebook, YouTube, Skype,

---

[223] Jasmine Farrier, "The Patriot Act's Institutional Story: More Evidence of Congressional Ambivalence," *PS: Political Science and Politics* 40, no. 1 (2007): 93–97.
[224] "Only '1% of Snowden Files Published,'" *BBC News*, December 3, 2013, sec. UK, https://www.bbc.com/news/uk-25205846; "Pentagon Says Snowden Took Most U.S. Secrets Ever: Rogers - Bloomberg," accessed April 12, 2020, https://web.archive.org/web/20140110092104/http://www.bloomberg.com/news/2014-01-09/pentagon-finds-snowden-took-1-7-million-files-rogers-says.html.
[225] Christian Grothoff SPIEGEL Michael Sontheimer, Marcel Rosenbach, Laura Poitras, Andy Müller-Maguhn, DER, "Snowden Documents Indicate NSA Has Breached Deutsche Telekom - DER SPIEGEL - International," accessed April 12, 2020, https://www.spiegel.de/international/world/snowden-documents-indicate-nsa-has-breached-deutsche-telekom-a-991503.html.
[226] Farrell and Newman, *Of Privacy and Power*.
[227] "Snowden Revelations," Lawfare, July 15, 2015, https://www.lawfareblog.com/snowden-revelations.

AOL, LinkedIn and Apple, of both American residents and residents of other countries, whether compelled by an NSL or not.[228] Not only does the NSA engage in espionage, but it also manipulates information presented online, and engages in aggressive cyber operations to plant malware on the devices of intelligence threats.[229]

Like the contents of the documents which he revealed, Snowden quickly became the center of controversy himself, at least, in the US. While the international community largely praised Snowden for whistleblowing, Snowden was a divisive character domestically. On the one hand, Snowden was championed as a patriot for standing up for the right to individual liberty from government surveillance.[230] While President Obama downplayed the significance of the disclosures, and some journalists questioned the significance of the released documents since they are predominantly concerned with foreign intelligence rather than domestic, the Department of Defense said that this was the biggest theft of US secrets in history.[231] This prompted some to view him as a traitor, undermining US operations around the world and potentially putting the country at more risk of harm, echoing the sentiments which led to the Patriot Act in the first place. Prior to the first leak, Snowden fled to China and then Russia to seek asylum, which further antagonized the American public. Just a few days after the first leak, Snowden was charged with two charges under the Espionage Act, and another charge of embezzlement, which amounts to thirty years of prison if he returned to the US. A month after the first leak, a Reuters poll showed that 23% of

[228] "Snowden Revelations."
[229] "Snowden Revelations."
[230] Adam Gabbatt, "Edward Snowden a 'hero' for NSA Disclosures, Wikipedia Founder Says," *The Guardian*, November 25, 2013, sec. World news, https://www.theguardian.com/world/2013/nov/25/edward-snowden-nsa-wikipedia-founder.
[231] "Pentagon Says Snowden Took Most U.S. Secrets Ever: Rogers - Bloomberg."

Americans consider Snowden a traitor, while 31% consider him a patriot, with 46% saying that they were unsure.[232]

The contentious portrayal of Snowden distracted from some of the other issues raised by the leaks. For instance, there was little discussion about whether the NSA was gathering information that was necessary for purposes of national security.[233] The NSA was able to gain some intelligence about terrorist activity as a result of its surveillance programs, but it is less clear if the NSA needed to spy on high-ranking government officials of US allies, like Chancellor of Germany Angela Merkel, or the boards of international non-governmental organizations like Human Rights Watch.[234] One leaked document also suggested that the NSA may not have been very covert in their surveillance, showing that the NSA accidentally triggered an Internet shutdown in parts of Syria in 2012 when trying to install surveillance software on a Syrian router. [235] In fact, the full extent of information gathering is still unknown, since only 1% of the stolen documents have been made public by the media, at the request of heads of states. [236]

The domestic impact of the Snowden Revelations did not result in a new privacy law. The USA Freedom Act was passed in 2015, which was a reform of the Patriot Act. However, while implementing guardrails for bulk collection of telecommunications metadata, it restored provisions for roving wiretaps, and reauthorized the tracking of lone wolf terrorists which motivated large-scale surveillance efforts in the first place.[237] Proposed amendments which

---

[232] "More Americans See Man Who Leaked NSA Secrets as 'patriot' than Traitor: Poll," *Reuters*, June 12, 2013, https://www.reuters.com/article/us-usa-security-poll-idUSBRE95B1AF20130612.
[233] Harknett and Stever, "The Struggle to Reform Intelligence after 9/11."
[234] "Snowden Revelations."
[235] "Snowden Revelations"; James Bamford, "Edward Snowden: The Untold Story," *Wired*, August 13, 2014, https://www.wired.com/2014/08/edward-snowden/.
[236] Francis Elliott, "Cameron Hints at Action to Stop Security Leaks," *The Times*, October 28, 2013, sec. unknown section, https://www.thetimes.co.uk/article/cameron-hints-at-action-to-stop-security-leaks-krg6tl9w80c; "Only '1% of Snowden Files Published.'"
[237] Alex Byers, "USA Freedom Act vs. USA PATRIOT Act," POLITICO, accessed April 30, 2020, https://www.politico.com/story/2015/05/usa-freedom-act-vs-usa-patriot-act-118469.html; "Senate Approves USA

intended to be more stringent concerning the data protection of citizens, were dismissed, privacy considered a necessary sacrifice in order to ensure the safety of the country. Perhaps, the most consequential outcome of the Snowden Revelations is that is showed Americans that their digital footprint can be manipulated by private and public actors alike which create detailed profiles of their lives, and that their rights may be better protected under the laws of other countries.[238] Neither the federal laws which shielded data in certain sectors, nor the state-driven patchwork system, were sufficiently competent to protect citizens from privacy infringement online. Meanwhile, the EU responded to the Snowden Revelations by passing the GDPR in 2016.[239]

Becoming "General": Applying Extraterritoriality with the GDPR

Chapter 4 will highlight the role of the Snowden Revelations in the context of EU-US relations over data protection; however, the Revelations also had an effect on the drafting of the GDPR. Prior to discussing the extraterritorial effects of the GDPR on the US jurisdiction, this section will address the logic of the EU to employ extraterritoriality for data protection. Since data protection is a human right according to the EU, it was important for the EU to ensure that the data was being protected in data flows that involve third countries too.[240] It would be illogical to suggest that EU citizens lose a fundamental right once their data leaves the jurisdiction of the EU, just like EU citizens retain other fundamental rights via citizenship regardless of where they are located.

Freedom Act, Obama Signs It, After Amendments Fail," NPR.org, accessed April 12, 2020, https://www.npr.org/sections/thetwo-way/2015/06/02/411534447/senateis-poised-to-vote-on-house-approved-usa-freedom-act; Chris Plante, "A Short, Crucial Explanation of the USA Patriot Act and USA Freedom Act," The Verge, October 20, 2015, https://www.theverge.com/2015/10/20/9573619/usa-patriot-act-freedom-explainer.

[238] Farrell and Newman, *Of Privacy and Power*.

[239] Hallie Coyne, "The Untold Story of Edward Snowden's Impact on the GDPR," *The Cyber Defense Review* 4, no. 2 (2019): 65–80, https://doi.org/10.2307/26843893.

[240] Gunasekara, "The 'Final' Privacy Frontier?"; Suuberg, "The View from the Crossroads"; Phillips, "International Data-Sharing Norms."

The GDPR employs extraterritoriality to reinforce stringency concerning data protection.[241] However, the feasibility of achieving the necessary level of compliance in jurisdictions like the US which lack a comparable regulatory framework for data protection necessitated the EU to review on a case by case basis the ability of third countries to adequately protect EU data.

The nature of data further complicates matters since it means that data may be simultaneous used by multiple entities in multiple jurisdictions. The quality of data does not change, regardless of how many times it may be used and re-used, meaning that multiple cross-border data transfers do not reduce the intrinsic value of the data. At the same time, the transaction cost of transferring data from one jurisdiction to another is low. This allows data to occupy several jurisdictions at once, should legal barriers not be erected to govern its transfer. [242] Additionally, it is a high ask of entities to establish two different processes for managing ex-EU data flows; that is, one for EU citizens and another for non-EU citizens.[243] This may require users to disclose whether or not they are an EU citizen upon entering a site, which is a data protection violation in it of itself.

The GDPR solves this novel problem by using extraterritoriality. First, the GDPR affords data protection to all data generated in the jurisdiction of the EU.[244] This standardizes the process for cross-border data flows regardless of whether the data belongs to an EU citizen or not. Therefore, the GDPR expands beyond the nationality requirement that was previously used by the Data Protection Directive. Entities that handle data that originated in the EU must adhere to the

[241] SCOTT, "Extraterritoriality and Territorial Extension in EU Law"; Azzi, "The Challenges Faced by the Extraterritorial Scope of the General Data Protection Regulation."
[242] Shakila Bu-Pasha, "Cross-Border Issues under EU Data Protection Law with Regards to Personal Data Protection," *Information & Communications Technology Law* 26, no. 3 (September 2, 2017): 213–28, https://doi.org/10.1080/13600834.2017.1330740.
[243] "Google's AMP Project Announces New Consent Component Ahead of GDPR Compliance Deadline - Search Engine Land," accessed April 15, 2020, https://searchengineland.com/googles-amp-project-announces-new-consent-component-ahead-of-gdpr-compliance-deadline-295633.
[244] Commission Regulation 16/679, 2016 O.J. (L 119) p 1-88.

GDPR for the entire duration of processing, regardless of where the entity is located.[245] Further, the entity must be approved for the transfer prior to processing. An adequacy decision, determined solely by the EU Commission the executive branch of the EU, affords a third country adequacy for all data transfers between itself and the EU. To achieve this, a country must demonstrate that it has a legal framework comparable to that of the GDPR which serves to ensure the continued protection of data. In the absence of such a decision, a country may make a bilateral agreement with the EU outlining the conditions for data transfers.[246]

Alternatively, corporate entities may ensure a legal data transfer in a variety of ways. Binding corporate rules are one method, often used by multinational corporations, which are a set of intra-corporate policies, practices, processes and guidelines that must be approved individually by the relevant national DPAs before a transfer takes place.[247] Companies may also employ standard contractual clauses, pre-approved by the Commission, in addition to informing the data subject of the data transfer.[248] Or, companies may use a certification mechanism or code of conduct, in combination with informing the data subject of the data transfer, to ensure compliance. Should an entity not be located in a country that has adequacy, or take any of the aforementioned measures in order to ensure compliance, a legal transfer may occur if the data subject has explicitly consented to transfer and has been informed of all the risks involved with the transfer.[249]

The GDPR uses extraterritoriality in order to extend the power of the EU by dictating the conditions for data flows, whether it be at the state level or at the corporate level. Some academics

---

[245] Voigt and Bussche, *The EU General Data Protection Regulation (GDPR).*
[246] Europäische Union and Europarat, *Handbook on European Data Protection Law.*
[247] "What Rules Apply If My Organisation Transfers Data Outside the EU?," Text, European Commission - European Commission, accessed April 13, 2020, https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/what-rules-apply-if-my-organisation-transfers-data-outside-eu_en.
[248] "What Rules Apply If My Organisation Transfers Data Outside the EU?"
[249] "What Rules Apply If My Organisation Transfers Data Outside the EU?"

claim that the GDPR qualifies as regulatory protectionism, since adequacy hinges upon approval from EU officials, like the Commission or national DPAs.[250] Normally, the motivation for regulatory protectionism arises from a desire to shield domestic corporations from foreign competition.[251] To a certain extent, this is true. The tech industry in Europe cannot economically compare to that in the US, for instance. However, the GDPR was not passed in order to better the economic playing field for the European tech industry. It was passed in order to safeguard the rights of European citizens, that being data protection. [252]

Further, the domestic consumer is expected to absorb the consequences of regulatory protectionism since the price of goods rises.[253] On the contrary, extraterritoriality has externalized the effects of the GDPR allowing the EU to "export" its regulation to other jurisdictions, whether it be via de jure or de facto effects.[254] De jure effects would be legislative action that is either motivated by the GDPR or arises in order for a country to achieve adequacy. De facto effects may compel legislative action, as corporations globalize their policies in order to be compliant with the GDPR and consumers of other jurisdictions recognize the benefits of data protection. While academics have attributed these effects to particular features of the EU or the nature of the policy area, this paper adds that the GDPR is distinctly able to achieve these effects because of its use of extraterritoriality.[255] This is not to discredit these claims. It is unlikely that the GDPR would have been as successful as it has, should it have been implemented by another state. However, GDPR

[250] Ziyang Fan and Anil Gupta, "The Dangers of Digital Protectionism," *Harvard Business Review*, August 30, 2018, https://hbr.org/2018/08/the-dangers-of-digital-protectionism.
[251] Alan O. Sykes, "Regulatory Protectionism and the Law of International Trade," *University of Chicago Law Review* 66, no. 1 (1999).
[252] Bradford, "The Brussels Effect," 2020.
[253] Sykes, "Regulatory Protectionism and the Law of International Trade"; Slaughter, "Leading through Law."
[254] Lawrence A. Kogan, "Exporting Europe's Protectionism," *The National Interest*, no. 77 (2004): 91–99.
[255] Bradford, "The Brussels Effect," 2020; Gady, "EU/U.S. Approaches to Data Privacy and the 'Brussels Effect': A Comparative Analysis"; SCOTT, "Extraterritoriality and Territorial Extension in EU Law"; Greze, "The Extra-Territorial Enforcement of the GDPR."

may also not have been as successful as it has, should it have been passed without its innovative use extraterritoriality, which was necessary given the nature of data.[256] Rather, extraterritoriality adds to the EU's ability to take advantage of regulatory competition, compelling behavior in other jurisdictions to align with the GDPR. Extraterritoriality can therefore be understood as a necessary rule that the GDPR uses to maintain protection, while also an effect which arises from digital interdependence with other states. For this reason, these effects will be referred to as the extraterritorial effects of the GDPR.

The Extraterritorial Effects of the GDPR: The US Case

The EU and the US are locked into economic interdependency, with the size of the EU-US data flow increasing by seven times between 2008 and 2013.[257] The GDPR has become the leading regulatory framework for data protection globally, and the US illustrates some of the avenues by which the GDPR exerts regulatory power that is embodied in its extraterritorial effects. In order to assess whether the EU has or has not been able to extend the GDPR to other jurisdictions, it makes sense to focus on a jurisdiction which is both reticent to expand the right to data protection to its own citizens, and is also home to the world's top tech companies. Therefore, the US has the potential to be resistant to the extraterritorial effects of the GDPR. However, the opposite is coming to light. There are observed de facto *and* de jure effects arising from *within* the US.

The extraterritorial effects will be presented in two parts, the de facto and the de jure effects. This is to highlight that extraterritorial effects may manifest through different mechanisms. The de facto effects concern the role of multinational corporations and consumers as multiple

[256] Bu-Pasha, "Cross-Border Issues under EU Data Protection Law with Regards to Personal Data Protection."
[257] "Global Flows in a Digital Age | McKinsey," accessed April 4, 2020, https://www.mckinsey.com/business-functions/strategy-and-corporate-finance/our-insights/global-flows-in-a-digital-age.

channels of communication that may carry regulation to other jurisdictions.[258] Firms may choose to globalize a regulation across corporate operations for a number of reasons, including brand image, technical divisibility, and compliance costs.[259] Risk-averse consumers favor consumer safety, which means consumers may become jealous of consumers in other jurisdictions that have data protection while they do not, encouraging them to advocate for their rights. The de jure effect refers to the responsiveness of US policymakers and institutions to data protection legislation.[260] The de facto effects have motivated an indirect de jure effect in the US. Multinational corporations hope to offset the burden of compliance onto policymakers, while consumers seek clarity concerning their rights in the US. States have primarily been leading the charge on adopting GDPR-like laws, with speculation of a federal law in the future.

The De Facto Effects

The de facto effect will focus on changes within the US that reflect shifts in consumer preferences and corporate behavior toward a general favorability of regulations like the GDPR. It is difficult to causally link these developments to the GDPR, specifically. However, more often than not, those within the US cite the GDPR as either their motivation or inspiration. These include executives of tech companies, leaders of advocacy groups, as well as the average American.

Polling and sentiment analysis indicate that Americans today care more about their privacy online today, and some are changing their behavior online to align with their beliefs. Despite the fact that almost half of Americans are unaware of what the GDPR is by name, a Hill.TV/American

[258] Charles L. Cochran, "De Facto and De Jure Recognition: Is There a Difference?," *The American Journal of International Law* 62, no. 2 (1968): 457–60; Kenneth A. Schultz, "What's in a Claim? De Jure versus De Facto Borders in Interstate Territorial Disputes," *The Journal of Conflict Resolution* 58, no. 6 (2014): 1059–84.
[259] Drezner, *All Politics Is Global*; Jr, "Multinationals."
[260] Schultz, "What's in a Claim? De Jure versus De Facto Borders in Interstate Territorial Disputes"; Bradford, "The Brussels Effect," 2020.

Barometer poll found that 92% of Americans agree with at least one of the provisions of the GDPR.[261] While this may at first seem disconcerting, it reflects that the contents of GDPR hold wide appeal to Americans and indicative of the regulation's "ideational power," a term used to describe the normative diffusion of ideas.[262] Between 53 and 66% of Americans are not confident that private firms or tech companies are able to keep their information private or secure. [263] They are not wrong—there were over 4 billion records stolen in data breaches in 2019.[264] As a result, 65% of Americans said in 2018 that data privacy is the number one issue that companies should be addressing, even trumpeting healthcare and job creation.[265] Further, Americans are calling for the government to do more to regulate the tech industry, with 78% of Americans agreeing that Congress should have data protection legislation as a priority. A Pew poll found that there is agreement from both Democrats and Republicans that tech regulation is necessary, which is rare given the bipartisan nature of American politics today.[266]

Privacy is also developing an activism culture in the US in the form of strategic cases, campaigning and online movements. Edelson PC is the biggest litigator of consumer class action cases in the US, and has successfully litigated against Facebook, Amazon, Apple and Google, for specifically violating consumer privacy laws.[267] When domestic laws are insufficient for

---

[261] Matthew Sheffield, "Americans Overwhelmingly Want Congress to Restrict Sharing of Personal Data, Poll Finds," Text, TheHill, December 14, 2018, https://thehill.com/hilltv/what-americas-thinking/421384-opting-out-of-data-sharing-is-what-americans-want-most-from-a.
[262] Bradford, *The Brussels Effect*, 2020; Gilardi, "Transnational Diffusion."
[263] "10 Tech-Related Trends That Shaped the Decade," *Pew Research Center* (blog), accessed April 13, 2020, https://www.pewresearch.org/fact-tank/2019/12/20/10-tech-related-trends-that-shaped-the-decade/.
[264] "2019 Data Breaches: 4 Billion Records Breached So Far," accessed April 13, 2020, https://us.norton.com/internetsecurity-emerging-threats-2019-data-breaches.html.
[265] Finn Partners; Harris Poll, "Harris Poll And Finn Partners Unveil New Metric For The Return On Investment For Social Good," accessed April 13, 2020, https://www.prnewswire.com/news-releases/harris-poll-and-finn-partners-unveil-new-metric-for-the-return-on-investment-for-social-good-300747201.html.
[266] "10 Tech-Related Trends That Shaped the Decade."
[267] Conor Dougherty, "Jay Edelson, the Class-Action Lawyer Who May Be Tech's Least Friended Man," *The New York Times*, April 4, 2015, sec. Technology, https://www.nytimes.com/2015/04/05/technology/unpopular-in-silicon-valley.html.

consumers to claim their rights domestically, they turn to foreign courts. For instance, David Carroll first used the UK Data Protection Act of 1998 to sue Cambridge Analytica, which triggered UK ICO to fine Facebook under the GDPR.[268] The passing of the California Consumer Protection Act 2018 (CCPA), which is the first GDPR-inspired state law in the US, is largely attributed to the activism of Alastair McTaggart.[269] Organizations like the Electronic Frontier Foundation coordinate online campaigns to encourage citizens to vote against bills that may be putting their privacy at risk, usually collaborating with European advocacy groups like Privacy International in the UK.[270]

The media has also responded to this new demand for privacy awareness, signaling that privacy is emerging as a policy area in its own right. In 2019, the New York Times launched "The Privacy Project," to debate ideas, document events, and even offer suggestions about what readers can do about their online privacy.[271] While the media has covered big events like Cambridge Analytica and the Facebook congressional hearings, it is also picking up on subtler data protection

[268] "ICO Issues Maximum £500,000 Fine to Facebook for Failing to Protect Users' Personal Information" (ICO, October 25, 2018), https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2018/10/facebook-issued-with-maximum-500-000-fine/; Alex Hern, "Facebook Agrees to Pay Fine over Cambridge Analytica Scandal," *The Guardian*, October 30, 2019, sec. Technology, https://www.theguardian.com/technology/2019/oct/30/facebook-agrees-to-pay-fine-over-cambridge-analytica-scandal.

[269] "Alastair Mactaggart: First CCPA, Tackles CPRA Next," accessed April 13, 2020, https://www.natlawreview.com/article/next-act-architect-california-consumer-privacy-act-california-privacy-rights-act.

[270] Press Release, "Human Rights and Privacy Groups Launch Global Action to Oppose Mass Surveillance," Electronic Frontier Foundation, November 26, 2013, https://www.eff.org/press/releases/human-rights-and-privacy-groups-launch-global-action-oppose-mass-surveillance; Gert Vermeulen and Eva Lievens, *Data Protection and Privacy under Pressure. Transatlantic Tensions, EU Surveillance, and Big Data.* (Antwerpen: Maklu, 2018); Haunss, "Privacy Activism after Snowden: Advocacy Networks or Protest?"

[271] "New York Times Launches 'The Privacy Project,'" accessed April 13, 2020, https://iapp.org/news/a/new-york-times-launches-the-privacy-project/.

dilemmas. For instance, the success of rising tech companies like TikTok[272] or Clearview AI[273] is subject to scrutiny, with negative publicity potentially resulting in financial consequences. A massive increase in the user base for platforms like Zoom or Microsoft Teams as a result of the COVID-19 pandemic has likewise called attention to their privacy policies, causing Zoom to publicly defend their corporate practices.[274]

As a result, the private sector has been forced to respond. Because American law handles privacy abuses as a tort, privacy has been marketed as a mark of quality by tech companies, signaling that the product is "safe" for the consumer to use.[275] For instance, following the Cambridge Analytica scandal in 2018, Facebook launched an ad campaign dedicated to "keep you safe and your privacy."[276] In 2019 alone, Apple launched two privacy-centered ad campaigns.[277]

---

[272] Rebecca Jennings, "What's Going on with TikTok, China, and the US Government?," Vox, December 16, 2019, https://www.vox.com/open-sourced/2019/12/16/21013048/tiktok-china-national-security-investigation; "TikTok Said to Be Under National Security Review - The New York Times," accessed April 30, 2020, https://www.nytimes.com/2019/11/01/technology/tiktok-national-security-review.html.

[273] Ben Gilbert, "Clearview AI Scraped Billions of Photos from Social Media to Build a Facial Recognition App That Can ID Anyone — Here's Everything You Need to Know about the Mysterious Company," Business Insider, accessed April 30, 2020, https://www.businessinsider.com/what-is-clearview-ai-controversial-facial-recognition-startup-2020-3; Jon Porter, "Clearview AI's Source Code and App Data Exposed in Cybersecurity Lapse," The Verge, April 17, 2020, https://www.theverge.com/2020/4/17/21224718/clearview-ai-exposed-server-source-code-windows-ios-android-mac-apps-cloud-storage.

[274] Alison Durkee, "Zoom Gets Federal Government's Attention As Privacy Concerns Mount," Vanity Fair, accessed April 30, 2020, https://www.vanityfair.com/news/2020/04/zoom-privacy-concerns-ftc-investigation; Sara Morrison, "Zoom Responds to Its Privacy (and Porn) Problems," Vox, March 31, 2020, https://www.vox.com/recode/2020/3/31/21201019/zoom-coronavirus-privacy-hacks; Natasha Singer, Nicole Perlroth, and Aaron Krolik, "Zoom Rushes to Improve Privacy for Consumers Flooding Its Service," *The New York Times*, April 8, 2020, sec. Business, https://www.nytimes.com/2020/04/08/business/zoom-video-privacy-security-coronavirus.html; Tom Warren, "Zoom Grows to 300 Million Meeting Participants despite Security Backlash," The Verge, April 23, 2020, https://www.theverge.com/2020/4/23/21232401/zoom-300-million-users-growth-coronavirus-pandemic-security-privacy-concerns-response; "Zoom Goes From Conferencing App to the Pandemic's Social Network," *Bloomberg.Com*, April 9, 2020, https://www.bloomberg.com/news/features/2020-04-09/zoom-goes-from-conferencing-app-to-the-pandemic-s-social-network.

[275] Neil M. Richards and Daniel J. Solove, "Prosser's Privacy Law: A Mixed Legacy," *California Law Review* 98, no. 6 (2010): 1887–1924; Eugene Volokh, "TORT LAW VS. PRIVACY," *Columbia Law Review* 114, no. 4 (2014): 879–948.

[276] "Facebook Launches a New Ad Campaign With an Old Message," *Wired*, accessed April 13, 2020, https://www.wired.com/story/facebook-launches-a-new-ad-campaign-with-an-old-message/.

[277] "Apple Urges Customers to Keep Data Safe in New 'Privacy on IPhone' Ad," AppleInsider, accessed April 13, 2020, https://appleinsider.com/articles/19/10/25/apple-shares-new-privacy-on-iphone-ad-urges-users-to-protect-personal-data; "'Privacy. That's IPhone' Ad Campaign Launches, Highlights Apple's Stance on User Protection,"

However, Apple has realized its dedication to consumer privacy in practice as well. In 2016, Apple refused to cooperate with the FBI after the FBI ordered Apple to develop a software which would allow it to hack into the phones of terrorists involved in the San Bernardino Shootings. Tim Cook, former CEO of Apple, empathized with the position of the FBI but ultimately was not willing to sacrifice the privacy of all other Apple users for this singular case. In January of 2020, the FBI again required for assistance from Apple to unlock the iPhone of a shooter in Florida.[278]

Companies also have an incentive to globalize their company policies in order to streamline intra-company coordination among different locations. For instance, if a company is subject to GDPR in Ireland but not subject to GDPR in the US, the company would want to adopt GDPR-like company policy in order to standardize operations. This is especially true if the data of EU citizens is stored on the same server as the data of American citizens, in which case it is easier for a company to extend GDPR-compliance over all data rather than invest in another server. One lawyer notes that organizations are applying "GDPR everywhere," since users tend to be "of unknown citizenship," and to request disclosure of citizenship may constitute the very data protection infringement the GDPR tries to prevent.[279]

Further, a company might suffer from damages to its brand image if it treats consumers differently according to their jurisdiction. These pressures motivated Satya Madella, the CEO of

AppleInsider, accessed April 13, 2020, https://appleinsider.com/articles/19/03/14/privacy-thats-iphone-ad-campaign-launches-highlights-apples-stance-on-user-protection.

[278] Russell Brandom, "The FBI Has Asked Apple to Unlock Another Shooter's IPhone," The Verge, January 7, 2020, https://www.theverge.com/2020/1/7/21054836/fbi-iphone-unlock-apple-encryption-debate-pensacola-ios-security; Jack Nicas and Katie Benner, "F.B.I. Asks Apple to Help Unlock Two IPhones," *The New York Times*, January 7, 2020, sec. Technology, https://www.nytimes.com/2020/01/07/technology/apple-fbi-iphone-encryption.html; Julia Carrie Wong, "The FBI and Apple Are Facing off over an IPhone Again. What's Going On?," *The Guardian*, January 15, 2020, sec. US news, https://www.theguardian.com/us-news/2020/jan/14/fbi-apple-faceoff-iphone-florida-shooting.

[279] "Google's AMP Project Announces New Consent Component Ahead of GDPR Compliance Deadline - Search Engine Land."

Microsoft, to globalize the GDPR across all of Microsoft operations.[280] Further, since other countries are adopting GDPR-like laws, companies may prefer to globalize these data protection policies in order to remain competitive on the global market. Still, this calculus differs according to the corporation.[281]

Tech companies have turned to the legislation to clarify their legal responsibility towards data protection, as well as prevent the possibility of overinvesting in consumer expectations.[282] In the Congressional hearings on Facebook, Mark Zuckerberg advocated for a national data protection law while Facebook was under investigation for privacy abuses.[283] These sentiments have been echoed by 51 CEOs including Jeff Bezos of Amazon, Doug McMillon of Walmart, and Keith Block of Salesforce, in a letter to congressional leaders which represented business from all sectors of the economy.[284] The response of lawmakers to these pressures are covered in the next section.

The De Jure Effects

These de facto effects have motivated a push towards a de jure effect. Unlike other countries which adopted GDPR-like laws immediately after the regulation was passed, the US de jure effect is indirect, the culminated result of the de facto effects. There has been progress towards

---

[280] "Privacy Is a Human Right, We Need a GDPR for the World: Microsoft CEO," World Economic Forum, accessed April 4, 2020, https://www.weforum.org/agenda/2019/01/privacy-is-a-human-right-we-need-a-gdpr-for-the-world-microsoft-ceo/.
[281] Nick Statt, "Facebook Says It Will Not Extend GDPR Privacy Protections beyond EU," The Verge, April 3, 2018, https://www.theverge.com/2018/4/3/17194504/facebook-mark-zuckerberg-gdpr-privacy-protections-europe.
[282] "Forget the Techlash. The Lawlash Is Long Overdue | WIRED," accessed April 30, 2020, https://www.wired.com/story/opinion-forget-the-techlash-the-lawlash-is-long-overdue/.
[283] Elizabeth Schulze, "Mark Zuckerberg Says He Wants Stricter European-Style Privacy Laws — but Some Experts Are Questioning His Motives," CNBC, April 1, 2019, https://www.cnbc.com/2019/04/01/facebook-ceo-zuckerbergs-call-for-gdpr-privacy-laws-raises-questions.html.
[284] Kyle BrasseurTue, Sep 10, and 2019 2:43 Pm, "Amazon's Bezos among 51 CEOs Calling for National Data Privacy Law," Compliance Week, accessed April 14, 2020, https://www.complianceweek.com/data-privacy/amazons-bezos-among-51-ceos-calling-for-national-data-privacy-law/27678.article.

copycat laws at both the state and federal level, with revitalized commitment from US institutions like the US Federal Trade Commission and the US Department of Justice for privacy enforcement.

California has been the first of the US states to pass and enact a data protection law, the California Consumer Protection Act (CCPA) in 2018. While the CCPA is narrower in comparison to the GDPR with respect to applicability and scope, it is arguably the strongest consumer privacy law in the US, and was motivated by the GDPR.[285] There is overlap in the rights of the data subject, including the right to disclosure, data portability, deletion and transparency requirements from the company.[286] On the other hand, the CCPA does not afford the data subject the right to rectification, the right to resist processing or the right to object to processing. In contrast to the GDPR, the CCPA provides a right to "opt-out" of personal information sales, which requires companies to have a "Do Not Sell My Data" link on their homepage. If a consumer decides to opt-out, a reauthorization request should not occur for another twelve months.[287] The same identifiers, or categories of data, are covered under both laws. If damages are pursued via private right of action, consumers are able to seek damages ranging from $100 to $750 per consumer per incident.[288] While this is not comparable to the sanctions that a company can endure under the GDPR, a single consumer may seek damages for several incidents that occurred in a single visit to the website. If damages are pursued under civil fines, then the data subject can pursue penalties of $2,500 per incident, and $7,500 if it is intentional infringement.[289]

---

[285] Caitlin Chin, "Highlights: The GDPR and CCPA as Benchmarks for Federal Privacy Legislation," *Brookings* (blog), December 19, 2019, https://www.brookings.edu/blog/techtank/2019/12/19/highlights-the-gdpr-and-ccpa-as-benchmarks-for-federal-privacy-legislation/.
[286] "CCPA and GDPR Comparison Chart," accessed April 14, 2020, https://iapp.org/resources/article/ccpa-and-gdpr-comparison-chart/.
[287] "CCPA and GDPR Comparison Chart."
[288] TITLE 1.81.5. California Consumer Privacy Act of 2018 [1798.100 - 1798.199] (Title 1.81.5 Added by Stats. 2018, Ch. 55, Sec. 3.) (2018).
[289] "CCPA and GDPR Comparison Chart."

California has encouraged other states to follow its lead. David Vogel suggests that economic competition allows for regulatory convergence across the US, with other states willing to "trade up" their approaches in order to remain competitive with higher-regulating jurisdictions.[290] This leads to a "race to the top" or more stringent standards, uniformly. While economists have pointed to the so-called "California effect" in safety and environmental regulation, there is reason to believe that the California effect is taking place with data protection as well. As mentioned, data protection regulation may follow the same trends of safety regulation because of the codification of privacy in US tort law.[291] Further, because California has constitutional protection for privacy in its state constitution, it supports stringency in data protection.[292] In fact, this is exactly what can be observed. Despite the fact that the CCPA only came into effect just at the beginning of 2020, it has already motivated other states including New York, Massachusetts, Hawaii, Maryland and North Dakota, to pass GDPR-like legislation.[293]

Due to the public attention on data protection issues, in combination with a proliferation of state laws in the interest of data protection, there have also been calls for a national data protection law. While there is bipartisan consensus concerning the need for more data protection regulation, there is little consensus about how to go about it. For instance, Republicans are opting for pre-

[290] Vogel, *Trading Up*.
[291] Volokh, "TORT LAW VS. PRIVACY."
[292] "Betzel, Margaret, 'Privacy Law Developments In California,' I/S: A Journal of Law and Policy for the Information Society, Vol. 2, No. 3 (2006), 831-877.," n.d.
[293] Davis Wright Tremaine LLP-Rachel R. Marmor et al., "'Copycat CCPA' Bills Introduced in States Across Country | Lexology," accessed April 30, 2020, https://www.lexology.com/library/detail.aspx?g=163d5d78-e738-4ca1-a803-88f19db6b1ad; "'Copycat CCPA' Bills Introduced in States Across Country | Privacy & Security Law Blog | Davis Wright Tremaine," accessed April 30, 2020, https://www.dwt.com/blogs/privacy--security-law-blog/2019/02/copycat-ccpa-bills-introduced-in-states-across-cou; "Washington State Takes The Lead In CCPA Copycat Legislation Race, Trends Emerge," The National Law Review, accessed April 30, 2020, https://www.natlawreview.com/article/washington-state-takes-lead-ccpa-copycat-legislation-race-trends-emerge; "The Far-Reaching Implications of the California Consumer Privacy Act (CCPA)," *Bloomberg Law* (blog), accessed April 30, 2020, https://pro.bloomberglaw.com/the-far-reaching-implications-of-the-california-consumer-privacy-act-ccpa/.

emption of state laws, while the Democrats are seeking a private right of action.[294] However, both point to different aspects of the GDPR as inspiration for their positions. In February of 2020, Democratic senator Kristen Gillibrand proposed the Data Protection Act which calls for the creation of a data protection agency, which is an "independent federal agency that would protect Americans' data, safeguard their privacy, and ensure data practices are fair and transparent."[295] Gillibrand points to the role of the EDPS, and suggests that the US implement a similar approach. However, this would require an expansion of the powers of the central government, and so passing the Data Protection Act necessitates a large amount of political will.

There have been other proposals like the Consumer Data Privacy and Security Act released by Republican senator Jerry Moran, which have received bipartisan support.[296] In his bill, Moran suggests that data protection is enforced by empowering the existing institutions like the Federal Trade Commission (FTC) and the state attorneys general. The FTC is the US institution which regulates economic competition, and has already adopted privacy concerns as a foundational claim for unfair competition in the past. According to the FTC website, the $5 billion fine against Facebook issued in 2019 is the largest fine in the name of consumer privacy ever, by the

[294] Emily Birnbaum, "GOP Senator Introduces Privacy Legislation after Bipartisan Talks Break Down," Text, TheHill, March 12, 2020, https://thehill.com/policy/technology/487157-gop-senator-introduces-privacy-legislation-after-bipartisan-talks-break.

[295] "Confronting A Data Privacy Crisis, Gillibrand Announces Landmark Legislation To Create A Data Protection Agency | Kirsten Gillibrand | U.S. Senator for New York," accessed April 14, 2020, https://www.gillibrand.senate.gov/news/press/release/confronting-a-data-privacy-crisis-gillibrand-announces-landmark-legislation-to-create-a-data-protection-agency; "A Senate Bill Would Create a New US Data Protection Agency," *TechCrunch* (blog), accessed April 14, 2020, https://social.techcrunch.com/2020/02/13/gilliband-law-data-agency/.

[296] "Sen. Moran Introduces Landmark Federal Data Privacy Legislation," U.S. Senator for Kansas, Jerry Moran, accessed April 30, 2020, https://www.moran.senate.gov/public/index.cfm/2020/3/sen-moran-introduces-landmark-federal-data-privacy-legislation; "Moran Tees Up Data Privacy Bill As Senate Effort Splinters," accessed April 30, 2020, https://news.bloomberglaw.com/privacy-and-data-security/moran-tees-up-data-privacy-bill-as-senate-effort-splinters.

institution.[297] This even beats out the biggest penalty under the GDPR to date, that being the $57 million fine imposed on Google in 2019.[298]

Conclusion

The US provides a sharp contrast to the EU model presented in Chapter 2. Because privacy does not rise to the status of an explicit right, privacy is curtailed in lieu of other priorities, whether it be the right to free speech or the economy. The laissez faire governance of the US economy lacks the regulatory rigor of the EU since it is dependent on the will of companies to self-regulate for data protection issues. American corporations are unlikely to match the commitment of the EU to data protection through self-regulation being so would be costly, and corporations otherwise use this data to improve the quality of their products.

In the US case, federal issues which concern the state itself, like national security, trump issues like data protection that are regulated by the states. The US has a far greater institutional capacity in national security than the EU for data protection, investing extensively in its intelligence agencies and limiting barriers to coordination amongst them. As evidenced by the public response to the Snowden Revelations, there was little transparency between the US government and its people concerning the practices of the intelligence community suggesting that there were few channels of communication prior to the leaks. This presents the US as not only ill-prepared for a bilateral commitment in the interest of preserving data protection, but it also questions its priorities align with those of the EU at all.

---

[297] "FTC Imposes $5 Billion Penalty and Sweeping New Privacy Restrictions on Facebook," Federal Trade Commission, July 24, 2019, https://www.ftc.gov/news-events/press-releases/2019/07/ftc-imposes-5-billion-penalty-sweeping-new-privacy-restrictions.

[298] "French Data Protection Watchdog Fines Google $57 Million under the GDPR | TechCrunch," accessed April 30, 2020, https://techcrunch.com/2019/01/21/french-data-protection-watchdog-fines-google-57-million-under-the-gdpr/.

Regardless of the American legal framework for data protection, the EU must ensure that its citizens rights are protected extraterritorially. The nature of data entails that the GDPR uses extraterritoriality to expand its reach, necessitating that third countries reach adequacy as the EU Commission sees fit. However, evidence of changed behavior in jurisdictions beyond the EU suggest that the GDPR is being adopted informally too. The question of whether the soft power of the GDPR is an explicit strategy of the EU or an unintended byproduct of extraterritoriality, is explored in further depth in Chapter 4. Either way, complex interdependence plays an instrumental role in explaining the multiple channels by which the extraterritorial effects take hold, whether they be manifested de facto or de jure.

The US is arguably the most important jurisdiction beyond the EU for the data protection of EU citizens, since the US is the biggest trading partner of the EU with respect to the digital economy. American corporations were among the first to respond to the GDPR, for a variety of reasons. First, companies are able to save on adjustment costs across jurisdictions if it chooses to streamline global operations in accordance with the most stringent law overall. As the GDPR is being adopted directly into law in ex-EU jurisdictions, multinational corporations are being cornered into compliance. Microsoft and others have already globalized the GDPR in corporate practices. Second, it also may be technically impossible for a company to separate data practices according to the identity or location of the user. Further, a blow to brand name capital if a company is revealed to be treating consumers in one market to a different standard in comparison to other markets. As a result, Apple and Facebook have marketed data protection as an added service to its users in ad campaigns, intended to showcase the firm's commitment to privacy.

Moreover, US consumers are reacting to transnational influences due to the central role the US plays in the global economy. While US consumers are not aware of the GDPR itself, polling

data reflects that the major provision of the GDPR resonate with a majority of US consumers, suggesting that the law has ideational appeal with the population. US consumers have also taken to privacy activism, pursuing class action lawsuits against US corporations, and pushing for stronger US data protection laws domestically. Media coverage has reflected a general rise in the issue salience of data protection spending considerable resources to address privacy as a news topic in its own right.

As a result of these changes in US consumers and multinational corporations, there has been an indirect de jure effect. At the state level, there have been several laws passed that resemble the GDPR, however to a lesser scope. Corporations have advocating for a US federal law in order to offset responsibility onto US institutions, as well as gain clarity concerning the expectations of the US market. In response to this pressure, both of the major political parties in Congress have proposed bills that emulate parts of the GDPR, most notably a bill that would establish a data protection agency which would operate similarly to the EDPB in the EU. Further, US institutions have taken to following the EU's lead in terms of sanctions, with the FTC issuing Facebook one of the largest fines it has ever given for data protection. Therefore, the extraterritorial effects are not just motivating what can be construed as inconsequential adjustments in the behaviors of US consumers and practices of multinational corporations. Legislative bodies are also responsive to the GDPR, suggestive of structural reform in US data protection law as well.

While the extraterritorial effects of the GDPR in the US case suggest that legal differences between the two states have been resolved with market-based harmonization, the EU also relies on treaty-based harmonization with third countries to secure data protection in cross-border flows. Since the US was not going to approved for adequacy on the merits of its legal framework, it had to enter into negotiations with the EU. As mentioned, the extent to which legal incompatibility has

been codified in domestic legal frameworks serves as a significant barrier to drafting a bilateral agreement. Therefore, despite the fact that the GDPR has resonated with other areas of US society, ultimately intergovernmental discourse dictates the terms of agreement with regards to the shared data flow. The US hoped to find a legally interoperable solution, allowing it to preserve its own legal framework and intelligence practices, while assuring the EU that their right to data protection was being upheld. Meanwhile, the EU intended to extend their own regulatory framework to the US. Chapter 4 presents material on bilateral negotiations that have occurred with respect to the transatlantic data flow, and addresses the success of each actor in the pursuit of these goals.

Chapter 4: Commercialization of Data Flows Foster Attempts at EU-US Cooperation

The GDPR directly governs 446 million EU citizens, but may indirectly govern another 328 million US citizens through its extraterritorial effects. Rohit Chopra, a commissioner at the FTC, hints at the irony of this, saying that, "Ironically, many Americans are going to find themselves protected from a foreign law."[299] The extraterritorial effects of the GDPR motivate market-based harmonization, aligning the behaviors of US consumers, corporations, and legislation bodies to align with EU expectations because of unique features of the EU's pro-regulatory framework.[300] This chapter calls into question the receptivity of another key stakeholder in the debate— US institutions, particularly the FTC and the US Chamber of Commerce.

The last chapter pointed out the extent to which the EU and the US differ in their respective regulatory approaches to data protection. While the EU reinforces a pro-regulatory framework with a bureaucratic apparatus to uphold the right of its citizens to data protection, the US takes an alternative approach. Because data protection does not rise to the level of a right, the US regularly subjugates privacy concerns for other priorities like national security, and leaves it to companies to self-regulate, expecting firms to be responsive to consumer demands for data protection. Therefore, extraterritorial effects of the GDPR are all the more surprising.

Bilateral agreements provide an opportunity to see if the EU is able to extend its data protection regulation to foreign institutions, even those with significantly different frameworks like the US.[301] Of the manners in which adequacy might be approved, bilateral agreements stand

---

[299] "Europe, Not the U.S., Is Now the Most Powerful Regulator of Silicon Valley - The Washington Post," accessed April 30, 2020, https://www.washingtonpost.com/.
[300] Bradford, "The Brussels Effect," 2020.
[301] Bradford identifies two mechanisms that the EU can use to encourage policy convergence to EU regulation in other jurisdictions: market-based harmonization and treaty-based harmonization. This chapter will focus on the latter. Bradford.

to be the most contentious. Henry Farrell points to intergovernmental dialogue which allows states to avoid zero-sum games. "If actors representing different systems wish to avoid mutually assured stalemate, and to identify potential solutions, they typically must engage in dialogue with each other… efforts to resolve interdependence can involve just such dialogue."[302] The repeated efforts by the EU and US to negotiated agreements on data protection illustrate expectations of complex interdependence. At the same time, the vastly different regulatory frameworks presented a contentious environment for deal-making, with both actors attempting to maintain their own legal attitudes within their own jurisdictions, while compelling the other actor to make concessions in the interest of economic interdependence. So far, the EU and the US have twice engaged in bilateral agreements for the data protection of data flows. The first, the Safe Harbor Agreement (2000), was agreed upon after the Data Protection Directive (1995).[303] The second, the Privacy Shield (2016), was agreed upon after the GDPR (2016).[304] The deal-making processes were subject to external events like the Snowden Revelations, which dictated the conditions of agreement and resulted in significantly different outcomes in each case.[305]

This chapter intends to contrast the two rounds of negotiations under these different conditions. This chapter reviews three key elements of the EU-US negotiations for data protection: the Safe Harbor Agreement, the Snowden Revelations, and the Privacy Shield. These key moments

---

[302] Farrell, "Constructing the International Foundations of E-Commerce—The EU-U.S. Safe Harbor Arrangement," 301.
[303] Stephen J. Kobrin and Steve Kobrin, "Safe Harbours Are Hard to Find: The Trans-Atlantic Data Privacy Dispute, Territorial Jurisdiction and Global Governance," *Review of International Studies* 30, no. 1 (2004): 111–31.
[304] "EU Commission and United States Agree on New Framework for Transatlantic Data Flows"; "EU-US Data Transfers Won't Be Blocked While Privacy Shield Details Are Hammered Out, Says WP29 | TechCrunch," accessed April 4, 2020, https://techcrunch.com/2016/02/03/eu-us-data-transfers-wont-be-blocked-while-privacy-shield-details-are-hammered-out-says-wp29/?guccounter=1&guce_referrer=aHR0cHM6Ly9lbi53aWtpcGVkaWEub3JnLw&guce_referrer_sig=AQAAAMmVFFYWXYECAg_HghpkMSRRZZZH9-1fIiVuM0kjJxMQtk7WwjN46LuBTiy3aeIHv2MDPuQ_n226LUnTard9K5Y1H_q8FOzkyL-4uAJm0QazCoWdYlVDKc5lSp_2mXwNZvuobkg52FNoWeO0yrRk49QlAQ8lcWsKPxXj__oHrmi3.
[305] Coyne, "The Untold Story of Edward Snowden's Impact on the GDPR."

in the negotiation process reveal the struggle to maintain cooperation, an expectation of complex interdependence, when there is significant mismatch in the goals of the states involved in negotiations, suggesting that CWS may serve as a barrier to successful cooperation.[306] While the US committed to adhering to a level of regulation approved by the EU, its dedication wavered when it was expected to follow-through on that commitment. The enduring desire of the EU to export its regulation at the cost of watering down the rights of its citizens is illustrative of the trade-offs a state must make in order in order to maintain a transnational strategy. These cases, described in detail below, call into question elements of both complex interdependence and CWS, and will be explored further in Chapter 5.

Finding a Safe Harbor for Data Protection: The First Bilateral Attempt

By the turn of the century, it became clear that the EU and the US had to pursue a transatlantic privacy agreement. Prior to the 1990s, the Internet was primarily used for processing of government information, data storage, and research. With the invention of the World Wide Web and the formation of the first Internet service providers, the identity of the average Internet user expanded broadly.[307] Commercial entities were selling goods and services online, the explosion of "dot-com companies" promoting the Internet's economic promise. Also, the Internet was becoming a social space, a gathering ground for people of different nationalities to exchange information in spite of barriers like distance.[308] Between 1995 and 2000, the number of global

[306] Farrell and Newman, *Of Privacy and Power*.
[307] Shane Greenstein, *How the Internet Became Commercial* (Princeton University Press, 2015), https://doi.org/10.2307/j.ctvc777gg.
[308] Laura DeNardis and GLOBAL COMMISSION ON INTERNET GOVERNANCE, "INTRODUCTION:," A Universal Internet in a Bordered World (Centre for International Governance Innovation, 2016), JSTOR, www.jstor.org/stable/resrep05249.5.

internet users rose from 44.4 to 412.8 million.[309] At the same time, the EU was receiving early warning signs about the danger the Internet might pose to data protection. The disclosure of the Echelon surveillance program from 1972 to 2000, shed light on the fact that the network can be strategically co-opted to function as a surveillance tool,[310] while the Y2K "bug" illustrated that the network is fallible to human error, suggesting that risks like security persist into the Internet age.[311]

At the same time, the EU was drafting its Data Protection Directive, which was passed in 1995. The Data Protection Directive held many of the same provisions as the GDPR, however, because it was a directive and not a regulation, the particular implementation of the directive into national law was left to the EU states.[312] The scope of the Directive also limited applicability to EU citizens.[313] At this point, data protection was generally valued by EU states because of the roles of the OECD and the Council of Europe in shaping a European consensus.[314] But the enforcement of the Directive varied significantly amongst EU states in the absence of an EDPS board to harmonize enforcement. The Directive was also less stringent than the GDPR because the EU Charter of Human Rights was not adopted until 2009, meaning that data protection was not yet afforded human right status in EU primary law. However, the EU also sometimes uses directives as a means of preparing member states for more stringent regulation later on, which was true in the case of data protection as well.[315] Importantly, the Directive also introduced the authority of the EU Commission to determine adequacy for third countries, by the same parameters

[309] "Topic: Internet Usage Worldwide," www.statista.com, accessed April 30, 2020, https://www.statista.com/topics/1145/internet-usage-worldwide/.
[310] Franco Piodi et al., *The ECHELON Affair: The European Parliament and the Global Interception System* (Luxembourg: Publications Office, 2014).
[311] "Report to the European Council On the Year 2000 (Y2K) Computer Problem Experience" (Brussels, Belgium: European Commission, June 16, 2000).
[312] "Types of EU Law."
[313] Council Directive 95/46, 1995 O.J. (L 281) pg 31-50.
[314] González-Fuster, *The Emergence of Personal Data Protection as a Fundamental Right of the EU*.
[315] Palfrey and Gasser, *Interop the Promise and Perils of Highly Interconnected Systems*.

which the GDPR outlines adequacy. Australia, Canada, and several Eastern European countries introduced laws or revised existing ones, in order to conform to the provisions of the Directive and achieve adequacy.[316]

The fragmented state of data protection law in the US did not rise to the level of adequacy. While the US believed that a self-regulation approach provides sufficient data protection according the US, law the EU preferred a state-led approach in line with its vision of trade liberalization by legal harmonization. The EU and the US proceeded to pursue an agreement to overcome the domestic legal incompatibilities in order to preserve their economic relationship. However, under the guise of bilateral cooperation was an ongoing battle in competing standards. "Both the US and the EU sought to preserve and extend their domestic systems of privacy protection. Each sought, in effect, to dictate the terms under which privacy would be protected in the burgeoning sphere of international e-commerce."[317]

The EU perceived this situation as an opportunity to promote its regulatory preference via bilateral cooperation. One EU regulator stated that a bilateral agreement is much preferred to having companies individually comply with the Directive via the other channels offered under the Safe Harbor Agreement. "Contracts only deal with the transfers they are concluded to deal with. They are much less likely to have any secondary or spin-off effects. Whereas the Safe Harbor was much more likely to have a general upward pulling or pushing effect on privacy in general."[318] Since the EU is unable to use traditional means of coercion in the international community like war-mongering, the EU has instead turned to use its regulatory power to motivate effects like those outlined in Chapter 3. "The Commission bet that US businesses, as they adhered to Safe Harbor,

[316] Farrell and Newman, *Of Privacy and Power*.
[317] Farrell, "Constructing the International Foundations of E-Commerce—The EU-U.S. Safe Harbor Arrangement," 291.
[318] Farrell and Newman, *Of Privacy and Power,* 133.

would internalize European privacy rules and build pressure for stronger privacy in the US."[319] Part of the EU strategy with respect to foreign affairs is inducing other jurisdictions to align with EU regulation.[320] If a jurisdiction attempts to resist EU jurisdiction outright, it is only a matter of time before it is induced to align with the regulation. At that point, it is not only access to the EU market which requires compliance, but also access to all related markets which adopted the regulation. Of course, this strategy runs into a problem with the US, since the US market is comparable to that of the EU.

The EU underestimated the US reticence towards data protection. Or rather, the EU underestimated the US reticence towards extending data protection to the private sector. The strongest US privacy laws safeguard the US citizen from the government. A 1997 report from the White House titled, "A Framework for Global Electronic Commerce," outlines the ways the US "sought to embed and protect the US self-regulatory approach as the global standard, hence both shielding US commerce from foreign regulators and encouraging the latter over time to take a more laissez-faire approach."[321] The FTC, the US agency tasked with negotiating the Safe Harbor Agreement, was also highly sensitive to the needs of US companies. US companies were alarmed at the EU Data Protection Directive, anticipating that compliance would come at a high cost and risk investments in Europe, putting them at a disadvantage to their European competitors.[322] The

[319] Farrell and Newman, 134.
[320] Anu Bradford, "The EU as a Regulatory Power," CONNECTIVITY WARS (European Council on Foreign Relations, 2016), JSTOR, https://doi.org/10.2307/resrep21667.20.
[321] "The Framework for Global Electronic Commerce," accessed April 30, 2020, https://clintonwhitehouse4.archives.gov/WH/New/Commerce/; "White House Unveils E-Commerce Plans," accessed April 30, 2020, https://archive.nytimes.com/www.nytimes.com/library/tech/98/11/cyber/articles/30magaziner.html.
[322] Farrell, "Constructing the International Foundations of E-Commerce—The EU-U.S. Safe Harbor Arrangement"; "- THE EU DATA PROTECTION DIRECTIVE: IMPLICATIONS FOR THE U.S. PRIVACY DEBATE," accessed April 30, 2020, https://www.govinfo.gov/content/pkg/CHRG-107hhrg71497/html/CHRG-107hhrg71497.htm.

FTC saw bilateral cooperation as way to appease the EU, while minimizing its own commitment to the agreement.

The US was granted adequacy in 2000, with the Safe Harbor Agreement taking the form of an exchange of letters between the EU and the US. Ambassador Aaron, US Ambassador to the EU, developed the basic idea behind the agreement borrowed from financial markets regulation. Aaron pushed for the Commission to provide adequacy to US companies, rather than the country as whole, if those companies conceded to compliance with the Safe Harbor.[323] There were three "pillars" of the agreement. Firms had to agree to the Safe Harbor Principles, a set of principles outlined in the Data Protection Directive, and "sign up either to self-regulatory organizations or the FTC."[324] While the US Chamber of Commerce administered the agreement, the FTC was the regulator of US firms on the part of the Americans and had to resolve privacy complaints from European citizens. Third, European DPAs had the authority to block data flows if notified by the self-regulatory organization or the FTC that a firm was violating the Safe Harbor Agreement. The Commission had the power to withdraw its decision altogether if it felt that European data was not being appropriately handled under the agreement. "While the US could continue to claim publicly that its basic stance of protecting privacy through self-regulation was unchanged, the EU could say that it had succeeded in dictating the terms of self-regulation."[325]

Despite the fact that negotiators were hopeful of a lasting arrangement, the Safe Harbor Agreement operated under insufficient institutional development of the US side. First, was the

---

[323] "Full Text of Letter Containing Comments of 'Safe-Harbor' Pact," *Wall Street Journal*, April 6, 2000, sec. Front Section, https://www.wsj.com/articles/SB954961643812226656; Michelle P. Egan, ed., *Creating a Transatlantic Marketplace: Government Policies and Business Strategies*, European Policy Research Unit Series (Manchester ; New York: Manchester University Press, 2005); Kobrin and Kobrin, "Safe Harbours Are Hard to Find: The Trans-Atlantic Data Privacy Dispute, Territorial Jurisdiction and Global Governance."

[324] "Full Text of Letter Containing Comments of 'Safe-Harbor' Pact."

[325] Farrell and Newman, *Of Privacy and Power,* 133.

expectation that the FTC was going to have the EU's best interest at heart when enforcing the Safe Harbor Agreement. The primary concern of the FTC is to enforce antitrust law and promote consumer protection, neither of which involves ensuring the privacy of foreign citizens. A 2008 report by Galexia found that of 1,109 companies signed onto the agreement, only 348 met the basic requirements of the Principles.[326] Many organizations did not have a public privacy policy, had a privacy policy that failed to mention Safe Harbor, or had a privacy policy that did not offer a method of alternative dispute settlement for the consumer. By 2008, the Chamber of Commerce issued a certification mark that would demonstration the commitment of the company to the Safe Harbor Agreement. The report found that over 300 companies had false claims about membership and certification listed on their website.[327]

Besides monitoring, the FTC was also criticized for falling behind in enforcement and follow-through. The FTC was only able to enforce the agreement if there was a demonstrated gap between the privacy promise of the firm and the demonstrated practice of the firm—this is in keeping with the US idea of data protection as a tort. It was unclear if the FTC had a legal basis for enforcement if no privacy policy is available.[328] The Americans seemed to not be concerned. In 2007, an administrator for the US Chamber of Commerce gave a presentation to the International Trade Association on progress under the Safe Harbor Agreement, stating that the EU considers the Agreement to be the "'best practice' for data protection and gold standard for data protection."[329] This statement contradicted studies done by the EU Commission which called for stronger enforcement.[330]

---

[326] Chris Connolly, "The US Safe Harbor: Fact or Fiction?" (Galexia, 2008).
[327] Connolly.
[328] Connolly.
[329] Damon Greer, "The US EU Safe Harbor Framework: Cross Border Data Flows, Data Protection, and Privacy."
[330] "The Application of Commission Decision 520/2000/EC of 26 July 2000 Pursuant to Directive 95/46 of the European Parliament and of the Council on the Adequate Protection of Personal Data Provided by the Safe Harbour

By 2012, the EU was beginning to draft the GDPR to serve as an update to the Directive.[331] With the passage of the EU Charter of Human Rights in 2009, it was necessary to further harmonization efforts for the internal market. Despite concerns that the agreement might be faltering, a joint statement from the EU Commission and the US Chamber of Commerce that the "United States and the European Union reaffirm their respective commitments to the US-EU Safe Harbor Framework."[332] The US seemed to be coming around to meet the EU on their own terms, with President Obama proposing a Consumer Privacy Bill of Rights in 2012 stating that "consumer trust is essential for the growth of the digital economy…. For businesses to succeed online, consumers must feel secure."[333] Not only did the Snowden Revelations derail the Safe Harbor Agreement in 2013, it motivated the EU to use the GDPR as a way to communicate European commitment to data protection in the negotiating of the Privacy Shield.

The Snowden Revelations Derail the Safe Harbor Agreement

The commercialization of the Internet provided a ripe opportunity for surveillance because of the number of users which were online, and because of the amount of information the users left behind in their digital footprints.[334] Companies were already using this data to optimize services,

---

Privacy Principles and Related Frequently Asked Questions Issued by the US Department of Commerce" (European Commission, February 13, 2002); "The Implementation of Commission Decision 520/2000/EC on the Adequate Protection of Personal Data Provided by the Safe Harbour Privacy Principles and Related Frequently Asked Questions Issued by the US Department of Commerce" (Brussels, Belgium: European Commission, October 20, 2004).

[331] "Commission Proposes a Comprehensive Reform of Data Protection Rules to Increase Users' Control of Their Data and to Cut Costs for Businesses," January 25, 2012, https://ec.europa.eu/commission/presscorner/detail/en/IP_12_46.

[332] "EU-U.S. Joint Statement on Data Protection by European Commission Vice-President Viviane Reding and U.S. Secretary of Commerce John Bryson," March 19, 2012, https://ec.europa.eu/commission/presscorner/detail/en/MEMO_12_192.

[333] "We Can't Wait: Obama Administration Unveils Blueprint for a 'Privacy Bill of Rights' to Protect Consumers Online," whitehouse.gov, February 23, 2012, https://obamawhitehouse.archives.gov/the-press-office/2012/02/23/we-can-t-wait-obama-administration-unveils-blueprint-privacy-bill-rights.

[334] Donohue, *The Future of Foreign Intelligence*.

which was seen as economically efficient and non-invasive from the perspective of US data protection law. The Patriot Act allowed US intelligence agencies to access that commercial data, circumventing safeguards like the US Privacy Act of 1974 in the name of national security. But this data was not only used to combat terrorism. The NSA was also found to be amassing data for information's sake, spying on the boards of NGOs, high-ranking government officials of US allies, and developing a "treasure map" to locate every device which is connected to the Internet in the world.[335]

The 2013 Snowden Revelations derailed any progress made under the Safe Harbor Agreement. The Safe Harbor Agreement solely addressed the transatlantic exchange of commercial user data. Negotiations for an EU-US Umbrella Agreement began in 2011, to outline a data protection framework in the interest of UE-US law enforcement coordination, "for the purpose of prevention, detection, investigation, and prosecution of criminal offenses, including terrorism."[336] The Umbrella Agreement was therefore restricted to data-sharing between law enforcement agencies. Should intelligence needs arise, it would be overcome via intergovernmental cooperation, just like the Safe Harbor Agreement.[337] More importantly, the two agreements were believed to work together in the interest of protecting EU data protection by keeping the commercial use of data separate from data-gathering for intelligence purposes.[338] Therefore, the EU was under the impression that the US was appeasing the EU version of data

[335] "Snowden Revelations."
[336] "Agreement between The United States of America and The European Union on the Protection of Personal Information Relating to the Prevention, Investigation, Detection, and Prosecution of Criminal Offenses (Not yet Binding under PIL)," accessed April 15, 2020, https://eclan.eu/en/eu-legislatory/agreement-between-the-united-states-of-america-and-the-european-union-on-the-protection-of-personal-information-relating-to-the-prevention-investigation-detection-and-prosecution-of-criminal-offenses-not-yet-binding-under-pil.
[337] Martin Weiss and Kristin Archick, "U.S.-EU Data Privacy: From Safe Harbor to Privacy Shield" (Congressional Research Service, May 19, 2016).
[338] Farrell and Newman, *Of Privacy and Power*.

protection by ensuring compliance by both private and public entities. While the EU was aware that the US had reorganized arrangements among their intelligence agencies to lead the war on terror, the EU was in the dark with respect to the public-private partnership which was enabled under the Patriot Act. The EU believed that if the US wanted information on one of its citizens for law enforcement, it would reach out to EU institutions to get it. The EU did not expect the conflation of public and private interests, nor did it anticipate that the US would amass the sheer volume of data that it did, in the name of national security. [339]

The Snowden Revelations further shed light on the fact that the US was circumventing data protection commitments to the EU. The EU believed that its authority over the management of EU data by US entities was supported by Safe Harbor and the Umbrella Agreement, by erecting different conditions for data protection under private and public use, respectively, thereby preventing the US from playing one agreement off of the other.[340] As far as the EU was concerned, if the US government needed access to the data profile of an EU citizen for law enforcement, it would confer with the EU under the Umbrella Agreement. Instead, the Snowden Revelations demonstrated that surveillance included not only obstructing the privacy of EU citizens, but also of EU leaders, including the chancellor of Germany Angela Merkel, which was also leading the EU at the time. Besides grossly undermining the terms of their agreement, the Snowden Revelations also signaled a fundamental misunderstanding of European priorities and values. The very origins of European privacy law, as far back as before the advent of processing, are to serve as a protection against government obstruction on personal liberties.[341]

---

[339] David Wright and Reinhard Kreiss, "European Response to Snowden: A Discussion Paper" (Increasing Resilience in Surveillance Societies, December 2013), http://irissproject.eu/wp-content/uploads/2013/12/IRISS_European-responses-to-the-Snowden-revelations_18-Dec-2013_Final.pdf.
[340] Wright and Kreiss.
[341] González-Fuster, *The Emergence of Personal Data Protection as a Fundamental Right of the EU*.

The Snowden Revelations also motivated the emergence of a transnational activist network. While US activist organizations looked to their European peers for guidance on effective advocacy, European activists were focused on taking advantage of revitalized interest in data protection to advocate for stricter regulation.[342] Snowden cooperated with European media organizations like the Guardian, De Spiegel, and Le Monde, increasing public awareness and heightening issue salience for data protection.[343] This had an effect on members of EU Parliament that sought reelection in 2014.[344]

In 2013, Maximilian Schrems, a lawyer turned privacy rights advocate, filed a complaint against Facebook to the Irish DPA, since Facebook has its European headquarters in Ireland.[345] He wanted to prohibit Facebook from transferring his information to the US, where his right to data protection was being violated under Facebook data-sharing practices with the NSA. By 2015, the case reached the ECJ, Schrems' point bolstered by the fact that the EU Charter of Human Rights enshrined data protection as a human right. While it was less surprising that the ECJ decided to support Schrems' claim to data protection, it was shocking that the ECJ went to lengths of repealing US adequacy under Safe Harbor.[346] This decision empowered the ECJ, and not the Commission, to be the final word regarding adequacy. For European negotiators that had been willing to compromise on data protection for the sake of an economic relationship with the US, the decision of the ECJ signaled that there were domestic interests that were being sacrificed in

[342] Zygmunt Bauman et al., "After Snowden: Rethinking the Impact of Surveillance," *International Political Sociology* 8, no. 2 (June 2014): 121–44, https://doi.org/10.1111/ips.12048.
[343] Emily Bell et al., eds., *Journalism after Snowden: The Future of the Free Press in the Surveillance State*, Columbia Journalism Review Books (New York: Columbia University Press, 2017).
[344] Christina Eckes, *EU Powers under External Pressure: How the EU's External Actions Alter Its Internal Structures*, 2019, https://search.ebscohost.com/login.aspx?direct=true&scope=site&db=nlebk&db=nlabk&AN=2003807.
[345] C-362/14 Maximilian Schrems v. Data Protection Commissioner, 2015 E.C.R. 650.
[346] "The Court of Justice Declares That the Commission's US Safe Harbour Decision Is Invalid" (Luxembourg: Court of Justice of the EU, October 6, 2015).

order to achieve this compromise.[347] The ECJ decision also worried American industry leaders that were handling fallout from the Revelations domestically, thereby furthering pressure on American negotiators to draft a new agreement as soon as possible.[348]

With or without the Snowden Revelations, the drafting of the GDPR was already underway, and became the fighting grounds for a variety of different interests. The EU Commission had to demonstrate solidarity with the ECJ decision. Meanwhile, the members of the EU Parliament were doing the political calculus about whether they should succumb to the desires of tech lobby organizations, like Digital Europe which fought to limit the scope of extraterritoriality, minimize the burden of compliance, and the cost of sanctions, or whether the Snowden Revelations would negatively affect their chance at reelection.[349] Advocacy groups were quick to offer commentary in public consultations during drafting with the intension of expanding the GDPR.[350] From their perspective, high sanctions are meant to preclude companies from abusing data protection rights because the cost of doing so would be financially crippling.

Further, the EU had to wrestle with the potential consequences of a stringent regulation on its relationship with the US. If final authority concerning the adequacy of bilateral agreements lies with the ECJ, not the EU Commission, then it would make sense to make a regulation that reflects this reality. Additionally, since the US was already in need of repairing its relationship with the EU, it would make sense for the EU to make a GDPR which was more stringent than the Data Protection Directive. This way, even if the negotiations with the US did not ensure full compliance under the GDPR as it is, the GDPR would at least allow the EU to set the terms of the agreement

---

[347] Farrell and Newman, *Of Privacy and Power*.
[348] "U.S. Government Wants to Step into European Facebook Privacy Legal Challenge," *TechCrunch* (blog), accessed April 30, 2020, https://social.techcrunch.com/2016/06/13/us-government-wants-to-step-into-european-facebook-privacy-legal-challenge/.
[349] Coyne, "The Untold Story of Edward Snowden's Impact on the GDPR."
[350] Coyne.

at a higher bar in comparison to the Data Protection Directive. On April 14th, 2016, the GDPR was approved by the European Parliament,[351] claiming Europe the title of "world's leading tech watchdog."[352]

Shielding Privacy: The Second Bilateral Attempt

With the failure of the Safe Harbor Agreement and the passing of the GDPR, it was time to draft another transatlantic data protection agreement. Still, the US lacked sufficient "rule of law"[353] to govern private entities, or "the existence and effective functioning of one or more independent supervisory authorities,"[354] which would otherwise afford it adequacy under the GDPR. But, the EU used its new leverage to encourage concessions on the part of the US in the drafting of the Privacy Shield. The Commission demanded annual written assurances from their American counterparts to report on how the data of EU citizens was being used by American intelligence agencies.[355] An ombudsman position within the US State Department and independent from the US intelligence community was established to serve as a point of contact for EU citizens that want to file a complaint if they believed that US intelligence agencies were misusing their data.[356] This allowed the EU to prevent the public-private partnership which was previously possible under Safe Harbor.

---

[351] "Data Protection Reform - Parliament Approves New Rules Fit for the Digital Era | News | European Parliament," April 14, 2016, https://www.europarl.europa.eu/news/en/press-room/20160407IPR21776/data-protection-reform-parliament-approves-new-rules-fit-for-the-digital-era.

[352] Satariano, "G.D.P.R., a New Privacy Law, Makes Europe World's Leading Tech Watchdog."

[353] Commission Regulation 16/679, 2016 O.J. (L 119) p 1-88.

[354] Commission Regulation 16/679, 2016 O.J. (L 119) p 1-88.

[355] "EU Commission and United States Agree on New Framework for Transatlantic Data Flows."

[356] "EU-US PRIVACY SHIELD FORM FOR SUBMISSION OF REQUESTS TO THE U.S. OMBUDSPERSON," file:///Users/sasajovanovic/Downloads/20170417_PrivacyShield_RequestformunderOmbudspersonmechanism_enpdf.pdf.

Given the demonstrated inefficiencies of the FTC and the US Chamber of Commerce in enforcing the Safe Harbor agreement, the national DPAs were able to follow up on unresolved EU complaints, implement a dispute settlement mechanism, and set sanctions for noncompliance.[357] The final draft of the EU-US Privacy Shield granted the US adequacy on July 12th, 2016, much to the relief of American private sector which was primarily worried about the risks of noncompliance given the high sanctions. Much like Safe Harbor, the Privacy Shield requires organizations to self-certify to the US Department of Commerce and commit to 23 principles laid out in the agreement.[358] This is a significant expansion in comparison to the 7 principles required under Safe Harbor. There were expectations set out for the US Chamber of Commerce to engage in more rigorous monitoring of those businesses that signed onto the agreement. By 2019, nearly 5,000 businesses had self-certified on the Privacy Shield, and the agreement remains in force.[359]

However, the Privacy Shield has been subject to scrutiny thus far. The ombudsman position was only implemented after the national DPAs expressed their concerns about the fact that there was no oversight regarding the use of EU data for US intelligence purposes.[360] Consensus between the national DPAs the EU Commission was necessary, since the national DPAs were in charge of actually regulating the GDPR.[361] Since the Privacy Shield was passed, the EU had passed three annual reviews of its progress. In 2014, Obama introduced Presidential Policy Directive 28 (PPD-28), intending to "protect the legitimate privacy interests" of foreign nationals, however the first

---

[357] Farrell and Newman, *Of Privacy and Power*.
[358] "EU-U.S. PRIVACY SHIELD FRAMEWORK PRINCIPLES ISSUED BY THE U.S. DEPARTMENT OF COMMERCE" (US Department of Commerce, n.d.), https://www.privacyshield.gov/servlet/servlet.FileDownload?file=015t00000004qAg.
[359] This webpage lists all of the companies which have self-certified onto the Privacy Shield.
[360] "EU-US Privacy Shield Remains Precariously Placed," *TechCrunch* (blog), accessed April 30, 2020, https://social.techcrunch.com/2017/04/06/eu-us-privacy-shield-remains-precariously-placed/.
[361] Samuel Stolton, "95,000 Complaints Issued to EU Data Protection Authorities," *Www.Euractiv.Com* (blog), January 28, 2019, https://www.euractiv.com/section/data-protection/news/95000-complaints-issued-to-eu-data-protection-authorities/.

annual review of the Privacy Shield stated that PPD-28 conflicts with the Foreign Intelligence Surveillance Act (FISA), which allows US authorities to access the personal information of EU citizens via the transatlantic data flow.[362] The first review in 2017 recommended that the US Congress considers extending FISA protections to non-Americans to resolve this issue; this has not yet materialized.[363] The second review released in 2018 was primarily concerned with pressing the US government to appoint a permanent ombudsman, two years after the Privacy Shield had been agreed upon.[364] The EU Parliament pressured the EU Commission to suspend the agreement if the US government did not appoint one by the end of the year. The third review in 2019 was primarily concerned with encouraging ongoing communication between EU and US institutions in order to ensure consistency in enforcement by both sides, as well as outlining recommendations to the FTC and US Chamber of Commerce concerning follow-up of complaints.[365]

Still, the Privacy Shield was considered a success by the negotiators themselves. The EU sees the Privacy Shield as accomplishing what Safe Harbor could not; that is, motivating domestic change regarding privacy practices in the US. The second review of the Privacy Shield included reference to "developments in the US legal system in the area of privacy. These concern, in particular, the consultation initiated by the Federal Trade Commission on a federal approach to

---

[362] "The Privacy and Civil Liberties Oversight Board's Disappointing Report on PPD-28 Implementation," Just Security, October 24, 2018, https://www.justsecurity.org/61199/privacy-civil-liberties-oversight-boards-disappointing-report-ppd-28-implementation/.

[363] "First Annual Review of the EU-U.S. Privacy Shield Brussels" (Brussels, Belgium: European Commission, October 18, 2017).

[364] "REPORT FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL on the Second Annual Review of the Functioning of the EU-U.S. Privacy Shield" (Brussels, Belgium: European Commission, December 12, 2018).

[365] "EU-U.S. Privacy Shield: Third Review," Text, European Commission - European Commission, accessed April 4, 2020, https://ec.europa.eu/commission/presscorner/detail/en/IP_19_6134; "EU–U.S. Privacy Shield: EU Commission Issues Its Third Annual Review Report," Technology Law Dispatch, November 6, 2019, https://www.technologylawdispatch.com/2019/11/regulatory/eu-u-s-privacy-shield-eu-commission-issues-its-third-annual-review-report/; "REPORT FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL on the Third Annual Review of the Functioning of the EU-U.S. Privacy Shield" (European Commission, October 23, 2019).

privacy."[366] After the Commission gave its third review in 2019, Věra Jourová, EU Commissioner for Justice, Consumers and Gender Equality stated "The Privacy Shield is also a dialogue that in the long term should contribute to convergence of our systems, based on strong horizontal rights and independent, vigorous enforcement. Such convergence would ultimately strengthen the foundation on which the Privacy Shield is based."[367]

Of course, the hope is that this convergence of privacy rights shifts in the EU's favor. With the extraterritorial effects of the GDPR, de facto and de jure, there is reason to believe that such convergence is coming to fruition. The Privacy Shield may temporarily lessen the burden of GDPR compliance for US companies by allowing them to circumvent extraterritorial application by signing onto the agreement. However, as other countries adopt GDPR-like legislation, it may just be a matter of time before US companies are forced into full compliance with the GDPR, in order to be globally competitive.

However, the lifespan of the Privacy Shield is in the hands of the ECJ. In 2018, the ability of the Privacy Shield to safeguard EU data protection was called into question over the Facebook-Cambridge Analytica, since both Facebook and Cambridge Analytica were self-certified to the Privacy Shield.[368] That same year, Schrems filed another complaint against Facebook under the Irish DPA, in this case stating that the use of standard contractual clauses, an approved mechanism for transferring data out of the EU, are inadequate to protecting his right to privacy. Again, his

[366] "REPORT FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL on the Second Annual Review of the Functioning of the EU-U.S. Privacy Shield."
[367] "EU-U.S. Privacy Shield: Second Review Shows Improvements but a Permanent Ombudsperson Should Be Nominated by 28 February 2019," Text, European Commission - European Commission, accessed April 30, 2020, https://ec.europa.eu/commission/presscorner/detail/en/IP_18_6818.
[368] "Privacy Shield," accessed April 30, 2020, https://www.privacyshield.gov/participant?id=a2zt00000008PdqAAE&status=Active; "Pressure Mounts on EU-US Privacy Shield after Facebook-Cambridge Analytica Data Scandal | TechCrunch," accessed April 30, 2020, https://techcrunch.com/2018/06/12/pressure-mounts-on-eu-us-privacy-shield-after-facebook-cambridge-analytica-data-scandal/.

complaint has been referred up to the Irish High Court, and then the ECJ. In its 2018 referral, the Irish Court was particularly concerned on "whether the Privacy Shield was binding under EU law and whether the Privacy Shield's ombudsman system was sufficient."[369] In 2019, Schrems filed GDPR complaints against Facebook, Google, Amazon, Apple Music, DAZN, Filmmit, Netflix, SoundCloud, Spotify and YouTube.[370] While the 2019 cases may not address the credibility of the Privacy Shield directly, they will reflect the extent of enforcement afforded under the GDPR.

Conclusion

This chapter presented two iterations of deal-making between the EU and the US in the interest of keeping an open transatlantic data flow and maintain their economic relationship. The persistent challenge is determining an appropriate level of regulation, and ensuring the continued enforcement of that regulation. While the EU is pro-regulation, stemming from a desire to achieve harmonization of the internal European Market, the US is committed to minimally regulating data protection in the interest of trade liberalization. One 2019 Congressional Research Service report went so far as to claim that the EU's position on data protection restricts international trade and commerce, comparing it to China.[371] This is reflected in the reticence of US institutions to follow through on its commitments, even under a self-regulatory framework which has been critiqued as insufficiently protecting data, by advocacy groups on both sides of the Atlantic. From irregular monitoring of certified companies to stalling on the appointment of an ombudsman, the US has

[369] Farrell and Newman, *Of Privacy and Power,* 157.
[370] Rebecca Hill 18 Jan 2019 at 14:30, "Say GDP-AaaRrrgh, Streamers: Max Schrems Is Coming for You, Netflix and Amazon," accessed April 15, 2020, https://www.theregister.co.uk/2019/01/18/streaming_services_slapped_with_complaints_alleging_failure_to_meet_gdpr_rights/; "Max Schrems Files First Cases under GDPR against Facebook and Google," accessed April 4, 2020, https://www.irishtimes.com/business/technology/max-schrems-files-first-cases-under-gdpr-against-facebook-and-google-1.3508177.
[371] Weiss and Archick, "U.S.-EU Data Privacy: From Safe Harbor to Privacy Shield."

demonstrated reluctance to appease its European counterparts, even after having the Safe Harbor fail as a result of American negligence.

Likewise, there was a mismatch concerning the goals of the states. While the EU approached the deal-making process primarily in the interest of protecting the right to data protection by strategically crafting agreements that maintain this right extraterritorially; meanwhile, the US had multiple priorities. First, was the preservation of an open transatlantic data flow. Second, was minimizing the economic burden of European regulation on US companies, whether it be investing in organizational and technical measures or being subject to a penalty. Third, was maintaining the public-private partnership between US intelligence agencies and US companies in the interest of national security. Despite the fact that safeguards exist within the Privacy Shield agreement, as well as the Umbrella Agreement, to protect EU data from the same abuses that were revealed by Snowden, the US is unlikely to extend the Privacy Act of 1974 to foreign nationals. In fact, during the negotiations for Safe Harbor, the EU suggested that extending applicability of the Privacy Act may suffice for adequacy. While the data-gathering practices of the NSA have since been reformed, the NSA continues to keep those programs active and retains ownership over the data gathered thus far.

A miscalculation on the part of the EU was the tolerance of EU citizens to accept a watered-down version of their rights in order to maintain a transnational strategy.[372] The Snowden Revelations awoke both Europeans and Americans to data protection violations committed against them; however, while Americans lacked institutional or legal means to claim their rights, Europeans were able to turn to their national DPAs, members of European Parliament, and the ECJ to voice complaints. Not only did this provide Schrems with a platform to derail the Safe

[372] Farrell and Newman, *Of Privacy and Power*.

Harbor Agreement, but it also provided an addition check against future abuses, by affording the ECJ with final authority over adequacy. While these actors are not represented in the negotiating process itself, they have been successful at influencing the terms under which the process occurs. At the same time, these domestic actors pose as a challenge to future data protection agreements, if they set a regulatory floor which is beyond that which the US can withstand.

Finally, it is important to note the enduring desire of the EU to export its regulation to other jurisdictions. Not only does the EU intend to protect its right to data protection but also, because of the nature of data and the economic importance of data flows, encourage other countries to adopt similar laws. On the one hand, the extraterritorial effects discussed in Chapter 3 exemplify that domestic attitudes in the US are receptive to the GDPR, even finding agreement among different sectors of the population. However, there is a discrepancy between the domestic attitudes within the US, and the views presented in the intergovernmental negotiations. Further, it is unclear the degree to which these domestic attitudes seek to claim a right to data protection, since there is a competing priority which is national security. As more jurisdictions in the global economy either adopt or have pre-existing laws that achieve adequacy under the GDPR, the US may be at an economic disadvantage to continue to resist enacting a federal data protection law. This strategy can also allow the US to engage in regulatory competition by proposing its own framework, rather than seeking to convince other actors to negotiate down from their own position. With the fate of another data protection agreement in the hands of the ECJ, and the potential of another round of negotiations on the horizon, it is imperative that the US either meet the EU at the bar it has already set twice, or offer an alternative approach.

Chapter 5: The Complex Interdependence of Cyber Westphalia

As of 2019, there are 4.39 billion internet users around the world who have come to rely on the democratization of information and the global reach of the Internet.[373] The advent of the internet has introduced governance challenges which may alter fundamental assumptions of international politics, primarily concerned with the ability of the state to enforce state authority online. Governments have to grapple with an unprecedented degree of interconnectedness and instantaneous communication, which is disassociated from physical boundaries.[374] While the Internet has facilitated economic growth, accounting for 7% of US GDP in 2019 or $1.35 trillion in 2017,[375] governments may no longer be able to adequately handle these challenges on their own. Many governments have acknowledged the need for intergovernmental cooperation in order to handle internet issues.[376]

A study of EU-US relations allows us to contextualize these problems. These two political systems attempt to engage in cooperation over data protection in order to preserve a shared data-flow. The GDPR's success in finding support among different areas of American society, de facto governing a population beyond its borders, speaks to the complexity of governance in the digital age. The GDPR has influenced the awareness of an alternative model for data protection for US

---

[373] Max Roser, Hannah Ritchie, and Esteban Ortiz-Ospina, "Internet," *Our World in Data*, July 14, 2015, https://ourworldindata.org/internet.

[374] Mueller, Mathiason, and Klein, "The Internet and Global Governance: Principles and Norms for a New Regime"; Rolf H. Weber, Mirina Grosz, and Romana Weber, *Shaping Internet Governance: Regulatory Challenges*, Licence ed, Publikationen Aus Dem Zentrum Für Informations- Und Kommunikationsrecht Der Universität Zürich 46 (Heidelberg: Springer, 2009).

[375] "Digital Economy Accounted for 6.9 Percent of GDP in 2017 | U.S. Bureau of Economic Analysis (BEA)," accessed April 19, 2020, https://www.bea.gov/news/blog/2019-04-04/digital-economy-accounted-69-percent-gdp-2017.

[376] MARK T. PETERS, "Interdependence," in *Cashing In on Cyberpower*, How Interdependent Actors Seek Economic Outcomes in a Digital World (University of Nebraska Press, 2018), 13–44, https://doi.org/10.2307/j.ctt22726v0.7; "The Age of Digital Interdependence" (UN Secretary-General's High-level Panel on Digital Cooperation, June 10, 2019).

consumers, changed corporate practices of US firms, and motivated changes to US state-level laws, elaborated in Chapter 3.

While the EU and the US have engaged in iterative institutional dialogue to find a legally-interoperable solution—Safe Harbor, under the Data Protection Directive, and the Privacy Shield, under the GDPR—the inability of the two actors to come to a fundamental agreement during bilateral deal-making called into question whether intergovernmental cooperation on data protection is possible at all. As outlined in Chapter 2 and Chapter 3, each state has a distinct legal framework for data protection, resulting in disparate degrees of institutionalization. The EU has erected a bureaucratic apparatus for the maintenance of data protection, while the US has been unwilling to match the regulatory institutions established by the EU. EU regulators were concerned about whether data would be adequately protected once exported to the US. Even after achieving bilateral agreements with the US, the EU saw persistent problems in commitment, monitoring, enforcement and follow-through by US institutions.[377] The EU's regulatory response was the GDPR. Although the US has resisted adopting data protection regulation itself, and has tried to insulate itself from the influence of the EU through bilateral bargaining, it now finds itself in many ways subject to the EU's visions of data protection regulation. The GDPR is now the de facto global standard for data protection.[378]

As an approach to explain state behavior in cases like these, complex interdependence offers a powerful—yet not completely satisfying—analytical lens to examine the EU and US negotiation over data protection, which has culminated, at least for now, in the GDPR. First,

[377] Connolly, "The US Safe Harbor: Fact or Fiction?"; Kobrin and Kobrin, "Safe Harbours Are Hard to Find: The Trans-Atlantic Data Privacy Dispute, Territorial Jurisdiction and Global Governance."
[378] Dan L. Burk, "Law as a Network Standard," in *The Global Flow of Information*, ed. Ramesh Subramanian and Eddan Katz, Legal, Social, and Cultural Perspectives (NYU Press, 2011), 156–72, www.jstor.org/stable/j.ctt9qfr5n.12; Phillips, "International Data-Sharing Norms."

complex interdependence is particularly suited to explain internet issues because it expects cooperation to arise in situations when states have common goals. The multilateral participation in international organizations like the OECD and the Council of Europe, prior to the formation of the EU, first conformed to expectations of complex interdependence, and set foundational agreements concerning data protection. Later, both the EU and the US had the common goal of maintaining an open data flow between their states. Second, complex interdependence can also help explain why states repeatedly engage in negotiations, despite past failures and different interests, due to economic interdependence. Third, it highlights the role of non-state actors in influencing bilateral outcomes. Multinational corporations, Snowden, and Schrems are just a few that exemplify this feature of complex interdependence.

However, complex interdependence has its limits. The Cyber Westphalian System (CWS), can explain the conditions under which cooperation breaks down, thereby complimenting complex interdependence by capturing the alternative option to states. First, cooperation may fail when one or both actors have competing domestic interests that they prioritize over the issue they are negotiating.[379] The US most clearly illustrates this condition, when it attempted to find ways to maintain its commitment to the EU regarding data protection, at the same as it continued surveillance practices in the interest of national security. Second, cooperation may break down when there is mismatch in institutions or capacity among interdependent states. Without an institution of its own tasked with data protection, the US had to resort to jointly using the FTC and the US Chamber of Commerce to ensure compliance, which were insufficient to match the capacity of the EU's EDPS board and associated national DPAs. Third, cooperation is less likely when definitions of key concepts are not aligned. Fundamental differences in legal attitudes might

[379] Drezner, *All Politics Is Global*.

complicate cooperative action, evidenced by the EU's treatment of data protection as a human right, while the US does not even afford privacy the status of a constitutional right. Finally, CWS assumes jurisdictions are clearly defined, and adjusted in accordance with the territorial limits of the state, a feature of international law.

The challenges of cooperation in light of disparate state interests suggest that the EU may not be able to sustain data protection for its citizens in the EU-US data flow. Complex interdependence creates advantages for some actors over others, which is what the EU employed with the soft power of the GDPR. Despite reciprocity, the EU has achieved its own data protection goals and extend authority into other jurisdictions, thereby enhancing its authority as a global regulatory power. The EU can only uphold data protection as a right if it is able to do so in all data flows globally, with the EU-US data flow being the largest data flow in the world. When this goal was not achieved through bilateral negotiations, i.e., the failure of Safe Harbor, then the EU formulated a regulation that would achieve compliance de facto. The EU has been able to enhance its leverage in cooperation from its own institutional capacity shaped from its internal processes of complex interdependence. This suggests that states which embrace rather than resist complex interdependence can wield it more effectively when negotiating with other states. Soft power tactics may therefore be an extension of the existing literature on complex interdependence. By coupling stringent standards with a bureaucratic apparatus for enforcement, the GDPR effected the behavior of individuals even in jurisdictions insulated by bilateral agreements like the US. Not only do the extraterritorial effects of the GDPR push the boundaries of soft power by questioning who can be governed by a regulation, but it also raises basic concerns about the applicable use of territory and jurisdiction in the digital age.

It is important to note that these claims about soft power may not be generalizable to all internet issues. Data protection is a special case within Internet governance, since there is significant variability amongst actors concerning either its codification in law or overall priority in national interests.[380] However, as the ability of states to assert sovereign views is increasingly threatened by the complex interdependence of the internet, the logic follows that states would adjust strategies to be successful in this new landscape, employing soft power tactics as a means of extending their influence by cultivating new norms and appealing to consumers and other regulators.[381] Therefore, soft power allows states to fulfill domestic interests as predicted by CWS, while engaging in cooperation as predicted by complex interdependence.

The sections that follow will apply the conceptual frameworks to describe EU-US relations as it pertains to data protection, using the material presented in Chapter 2, 3 and 4. The first section analyzes the appropriateness of complex interdependence, highlighting the three conditions of complex interdependence which allowed for bilateral cooperation. The second section uses CWS to explain why bilateral cooperation has been challenged in this case, as domestic state interests compete with intergovernmental commitments. The third section employs soft power to explain how the EU has at least temporarily gained an advantage with the extraterritorial effects of the GDPR.

[380] David Cole and Federico Fabbrini, "Bridging the Transatlantic Divide? The United States, the European Union, and the Protection of Privacy across Borders," *International Journal of Constitutional Law* 14, no. 1 (January 2016): 220–37, https://doi.org/10.1093/icon/mow012.
[381] Anne-Marie Slaughter, *The Chessboard and the Web: Strategies of Connection in a Networked World*, The Henry L. Stimson Lectures Series (New Haven: Yale University Press, 2017).

I'll Have What the EU is Having: Cooperating for Data Protection

This section uses complex interdependence theory to highlight and analyze important factors shaping the EU-US engagement over data protection. This section demonstrates that many of the expectations of complex interdependence were present in this case. First, the multiple channels of communication that arose between the EU and the US, not limited to interstate relations. Second, is the role of non-state actors influencing the circumstances under which bilateral negotiation may occur. And third, is the persistence of common goals between the EU and the US which explains the iterative nature of negotiation, despite bargaining failures and commitment issues. Ultimately, the economic interdependence of the EU-US data flow forces both states into cooperation, regardless of the significant differences in domestic legal attitudes towards data protection.

According to complex interdependence, multiple channels of transnational communication complicate the authority of the state, since intergovernmental discourse is diluted in competition with other channels. Safe Harbor and the Privacy Shield used traditional means of institutional dialogue, drafted, agreed upon, and adopted through the involvement of the EU Commission, FTC, and the US Chamber of Commerce. Connections across the Atlantic applied indirect pressure and heightened the issue salience of data protection within both jurisdictions. A transnational activist network motivated collaboration between European groups like Privacy International and American non-profits like Electronic Frontier Foundation. Because Snowden employed American and European media to make his revelations, citizens in the US were paying attention to European news outlets as leaks occurred, and vice versa.

While EU citizens had valued their right to data protection prior to the Snowden Revelations, these multiple channels of communication allowed sectors of the US to adopt

European sentiments about data protection, so much so that Americans have been claiming their rights in European courts. This also prepared them to welcome the extraterritorial effects of the GDPR. Multinational firms, like Microsoft, subject to global pressures, opted to standardize company practices across jurisdictions to the highest global standard, such as to lower compliance costs and transaction costs.[382] In response to heightened consumer expectations for data protection, data protection was marketed as a service to the user exemplified by ad campaigns like Facebook's in 2018, or Apple's in 2019. This cultural shift has culminated with the passing of US state laws that emulate the GDPR, although to a lesser scope, and Americans await a federal law to fix the current patchwork system for data protection.

These multiple channels of communication allow non-state actors to directly and indirectly influence the success of these agreements. Snowden is the obvious and prime example. His whistleblowing revealed the insufficiencies of Safe Harbor to adequately protect EU data from collaboration between US private firms and intelligence agencies. Snowden triggered Schrems, another non-state actor, to pursue his case against Facebook in the EU, ultimately spelling the end of Safe Harbor when the ECJ removed adequacy for the US. Further, the leaks introduced imbalance in the negotiations for the Privacy Shield in favor of the EU, since the US had to conceded to demands like the ombudsman position to assure Europeans that their data was being adequately protected. The private sector was also an important non-state actor.[383] Intergovernmental cooperation arose in the first place in order to preserve data protection for EU citizens while safeguarding their economic relationship. However, because the major tech

[382] Bradford, *The Brussels Effect*, 2020.
[383] George W. Coombe and Susan L. Kirk, "Privacy, Data Protection, and Transborder Data Flow: A Corporate Response to International Expectations," *The Business Lawyer* 39, no. 1 (1983): 33–66.

companies were primarily in the US, the private sector was able to compel US institutions to develop arrangements that would serve in their best interest.

As evidenced by the pursuit of bilateral agreements even after their failure, both the EU and the US share a common goal. Prior to engaging with negotiations with the US, the EU had benefitted from the pursuit of regulatory coordination in the organizing of its internal market. Concerns regarding cross-border data flows were first addressed in international organizations like the OECD and the Council of Europe, providing the forums for multilateral discourse on data protection. Conceptual linkage amongst the member states established fundamental principles for data protection, which contributed to the shaping of the EU Data Protection Directive in 1995. Legal harmonization was furthered by a bureaucratic apparatus, the EDPS, which ensured consistency in enforcement across member states. Therefore, the GDPR may be considered a result of extensive conceptual linkage over time.[384]

Given this track record of success with regulatory coordination, it made sense that the EU expected that negotiations with the US would similarly result in a mutually beneficial outcome. Because of the degree of economic interdependence between the two actors, the existence of a common goal should have been sufficient enough to ensure successful regulatory coordination, from the perspective of the EU. Further, the interdependence of the EU and the US is undeniable; in 2017, the digital economy accounted for 7 percent of US GDP alone.[385] Negotiations reflected that both actors were willing to make sacrifices on their part to try to make an agreement work. The US was willing to reconcile with the EU despite having other priorities. However, the US failed to materialize those promises by falling short on monitoring the self-regulating companies,

[384] von Grafenstein, "Conceptual Definitions as a Link for Regulation"; González-Fuster, *The Emergence of Personal Data Protection as a Fundamental Right of the EU*; Burk, "Law as a Network Standard."
[385] "Digital Economy Accounted for 6.9 Percent of GDP in 2017 | U.S. Bureau of Economic Analysis (BEA)."

and enforcing compliance. The EU understood this as adjustment costs associated with accommodating a regulatory framework which US institutions and companies were not used to. This seemed to be the case, with American performance improving in response to the findings of the EU's annual review of Safe Harbor. Neither did the Snowden Revelations cause the EU to abandon bargaining, even after the Snowden Revelations threw doubt into the extent of US commitment. Therefore, the degree to which both states mutually rely on cooperation, highlights the applicability of complex interdependence in this case.

Complex interdependence sheds light on the ways in which the digital age shows that governance is no longer dictated by hierarchy amongst states in competition with each other. Many actors at many levels are able to influence outcomes, and states have to cooperate in order to achieve the best outcome. The breadth of extraterritorial effects of the GDPR, as well as the instrumental role Snowden and Schrems played with respect to the negotiating of bilateral agreements, speak to this fact. While states have turned to intergovernmental cooperation primarily to ensure that their own regulatory frameworks are protected in other jurisdictions, states will also employ soft power tactics, should they have the capacity to do so, in order to shape these channels in their own favor. The third section in this chapter will elaborate upon the ways the EU has primarily employed soft power in the transatlantic struggle over data protection.

CWS Complicates Bilateral Cooperation

Complex interdependence defines the conditions which make cooperation desirable; but, why do states choose to not cooperate, if cooperation is considered advantageous? After all, if the US had not neglected Safe Harbor, then the EU would not have been encouraged to make the GDPR so stringent as a response. This section will employ CWS in order to understand the reasons

behind American non-compliance as a means of understanding the conditions under which the expectations of complex interdependence are unlikely to realized. Based on a realist approach to state behavior, CWS suggests that the expectations of complex interdependence break down under the following conditions: 1) when there are competing domestic priorities, 2) when there is a mismatch in institutions or capacity among the interdependent states; 3) when definitions of key concepts are not aligned; and 4) when jurisdictions are not clearly defined.[386] I explore each of these issues in the case of the GDPR, and engagement on data protection more broadly by the EU and the US.

CWS posits that states are driven by domestic interests, and may have competing priorities when cooperating with other states, that results in preference divergence.[387] Drezner suggests that "whether regulatory coordination takes place is a function of the adjustment costs actors face in altering their preexisting rules and regulations. When the adjustment costs are sufficiently high, [states will not cooperate]."[388] Safe Harbor was only drafted because the EU passed the Directive, which safeguarded the data protection rights of EU citizens. As Chapter 3 highlighted, the US does not have a legal framework for the regulation of consumer data comparable to that of the EU, therefore adjustment costs were high in order to fulfill the expectations of the EU in negotiations.

Furthermore, the US had competing priorities. The FTC attempted to limit its responsibilities to the EU in order to protect the US tech industry from regulation that it believed would impede laissez-faire economic growth. Additionally, national security was another competing priority. The US arranged commitments to the EU under Safe Harbor and the Umbrella Agreement to preserve its intelligence practices which relied on public-private coordination. As a

[386] Demchak and U.S. Naval War College, "Three Futures for a Post-Western Cybered World"; Drezner, *All Politics Is Global*.
[387] Ibid.
[388] Drezner, *All Politics Is Global,* 5.

result, the US limited its dedication to the EU, since this would mean detracting from national security. Preference divergence can also lead to bargaining failures and commitment problems.[389] The Snowden revelations led to the catastrophic bargaining failure of Safe Harbor after it became obvious that the US was taking advantage of EU data transferred in good faith through in its bulk data collection practices. Commitment problems on the part of the US are reflected in the persistent challenge of ensuring compliance by the FTC and Chamber of Commerce, that culminated in the establishment of an ombudsman position in the US State Department.[390]

While complex interdependence emphasizes the role of multiple channels of communication, CWS privileges institutional dialogue by raising it above other channels as the manner by which agreements are negotiated. However, this does not imply that institutional dialogue will always reach the desired outcome. Drezner states that "regulatory coordination is more likely to take place when preexisting institutions are in place and possess the necessary monitoring and enforcement capabilities."[391] While the EU has the national DPAs and the EDPS board that have the technical expertise to manage data protection issues, the US did not have institutions of its own to match the institutional capacity of the EU.[392] Although the US saddled the FTC and the US Chamber of Commerce with this new responsibility, they repeatedly fell short of achieving the stringent standard of compliance the Europeans desired.

However, commitment problems also were an issue in the EU. While the EU was able to institutionalize data protection and achieve regulatory coordination within the EU, this was more challenging when it attempted to cooperate with the US. After the Schrems case, which afforded

[389] Drezner.
[390] Farrell and Newman, *Of Privacy and Power*.
[391] Drezner, 23.
[392] "Confronting A Data Privacy Crisis, Gillibrand Announces Landmark Legislation To Create A Data Protection Agency | Kirsten Gillibrand | U.S. Senator for New York."

the ECJ the power to determine adequacy in addition to the EU Commission and ruled Safe Harbor inadequate under EU primary law, it was difficult to determine whether European institutions had aligned preferences. Since the ECJ cannot be involved in negotiations, it is disorienting for the US to be entering in negotiations with the EU Commission without knowing whether the agreement will be thrown out in a few years. This is the current fear concerning the Privacy Shield, as Schrems attempts to use EU primary law again, in order to destabilize another bilateral agreement.

Furthermore, definitions of key concepts were not aligned. Conceptual mismatch persisted throughout negotiations and later maintenance due to fundamental incompatibilities in legal attitudes about privacy.[393] According to Drezner, "ideational pressures in combination with structure-based approaches lead to regulatory coordination."[394] Regulatory coordination was achievable in the EU because it coupled conceptual linkage with an institutional framework that made legal harmonization possible. This built upon a decades-long, multilateral discussion about the appropriate ways to handle privacy, whether it be by the OECD or the Council of Europe, which served to align norms inside the EU.[395] On the other hand, the US right to privacy is chiefly from the government, while the European right to privacy is from both public and private entities. While the average American agrees with the major provision of the GDPR, their assessment changes when given the option of choosing data protection or national security. If the US is unable to solidify a constitutional right to privacy after 243 years, it is unlikely to undermine its own legal attitude for the EU's, which has had over 60 years to formulate a consensus on privacy and data protection amongst member states.

[393] Hurrell, "Power, Institutions, and the Production of Inequality."
[394] Drezner, *All Politics Is Global,* 14.
[395] González-Fuster, *The Emergence of Personal Data Protection as a Fundamental Right of the EU.*

Finally, CWS implies that jurisdictions are clearly defined since hierarchy amongst states must be distinct in order to assign authority. Because the CWS framework highlights the role of the state in regulating the Internet, it requires distinct delineation such as to separate one state from another so that authority is unambiguous. The current international legal framework prioritizes territory as the basis for state authority, which would otherwise support the CWS framework.[396] However, the Internet does not conform to past understanding of territory.

States have tried to overcome this problem. The GDPR is an example of such a regulation, first using the territorial scope of the EU to constitute applicability, and then also employing extraterritoriality in order to attach authority over all data flows that involve the EU. The GDPR further achieves territorialization by moving past the citizenship requirement that the EU Data Protection used. Since the GDPR applies to all data subjects on the territory of the EU, it deemphasizes the role of citizenship thereby becoming truly "general." while, the GDPR minimizes the authority of other states to claim authority over their own citizens, it also accentuates the authority over the EU to dictate rules on its own territory, thereby featuring its own sovereignty as a result. However, although this is legally practical, it may be increasingly technically challenging to enforce. As complex interdependence suggests, as the number of internet users increases and the volume of the data flow rises, it may become extremely challenging for the EU to continue to enforce the GDPR. This inherent tension between complex interdependence and the CWS system is covered in the next section.

[396] Buxbaum, "Territory, Territoriality, and the Resolution of Jurisdictional Conflict."

It Happened When You Weren't Looking: The Soft Power of the GDPR

Finally, this paper argued that the EU is uniquely positioned to employ soft power to gain control over the EU-US data flows through the extraterritorial effects of the GDPR. While complex interdependence suggests that cooperative behavior results in mutual reliance thereby weakening the ability of a government to regulate its domestic affairs in exchange for benefits from cooperation, this section will show how soft power provides a way for the state to protect its own regulatory framework and extend it to other jurisdictions. The digital age is especially advantageous to states that can to employ soft power since the Internet affords multiple channels of communication that exchange information at an unprecedented volume and speed.

The EU did have to use cooperation in order to ensure that the data flow remained open. Without a bilateral agreement in place, the US would not reach adequacy and the EU Commission would be forced to suspend the flow until an arrangement was agreed upon. Therefore, the EU approached cooperation with the intention of achieving its own goals. But, more importantly, the EU employed soft power as a strategic choice, echoed in statements from EU officials and negotiators alike, with the explicit intention of exporting EU regulation to other jurisdictions, including that of the US. In the wake of the Snowden Revelations, the GDPR was drafted with this dual purpose in mind, setting a stringent standard for domestic purposes while using extraterritoriality to motivate compliance abroad.

Second, Europe had engaged in a deliberative, multilateral process in order to safeguard this right, long before engaging with the US on this issue, and even before the formation of the EU. This put the EU in a far better position to advance its model against the fragmented approach of the US. The regulatory capacity of the EU to handle data protection issues in the form of national DPAs and the EDPS assured that stringent standards like the GDPR were going to be enforced,

both domestically and abroad. The EU is also consistent in its strategy to enforce data protection via institutional instruments rather than relying on the private sector to self-regulation. The response of the EU following the dramatic collapse of Safe Harbor exemplifies this preference for institutionalization. Since monitoring failed, the EU insisted on further institutionalizing US compliance with the appointment of an ombudsman in order to ensure that the US was delivering on its promises.

The stringency of the GDPR is unquestionable. Not only does it afford the data subject with the most extensive rights in the world, but it also has high sanctions which if enforced come to a significant financial blow to corporations. In this case, the Snowden Revelations partly motivated the political preference for stringency since MPAs in EU Parliament were expected to strengthen the draft of the GDPR in order to secure reelection in 2014. However, since it was succeeding a directive as a regulation, the GDPR was anticipated to be stringent anyways, necessarily raising the regulatory floor for data protection compliance in the EU. As a regulation, the GDPR also ensured consistent application across the jurisdictions of the EU member states as well.

Fourth, the EU had a predisposition to regulate inelastic targets which made it difficult for actors to escape compliance by shifting operations to a different jurisdiction. The GDPR was able to regulate inelastic targets by territorializing its scope to be applicable to all data subjects within the EU, and become more "general" since the GDPR dropped the citizenship requirement formerly used under the Data Protection Directive. However, the nature of data requires the EU to also assure its citizens that its data was being protected in data transfers to third countries as well. As Dutch politician and member of EU Parliament Gijs De Vrijes put it: "if you exchange information

internationally, you must strengthen data protection. Those are two sides of the same coin."[397] Therefore, the EU had to extend its reach through extraterritoriality in order to secure the right to data protection. However, in doing so, the EU is able to extend its territorial reach[398] into other jurisdictions in order to secure the right to data protection of data subjects that may not even be its own citizens.

Further, the non-divisibility of standards is the most significant feature that persuades corporations to globalize their operations to comply with the most stringent standard in jurisdictions other than the EU. Because of the nature of data, it is often technically not feasible or too costly for a corporation to segment corporate practices according to jurisdictional limits. Therefore, the ability of the EU to harness soft power boils down to this condition. The extraterritorial effects of the GDPR suggest that corporations have been making investments towards globalizing their operations to align with EU regulation. Corporations have adopted data protection into their corporate practices, even marketing it as an added benefit of their products.

The multiple channels of communication between the two jurisdictions have likewise allowed for other extraterritorial effects to materialize too. Transnational activist networks have heightened the appeal of data protection for the average American consumer, reflecting the ideational power of the GDPR. Corporations have indirectly motivated a de jure effect, pressuring lawmakers to pass laws that embody provisions of the GDPR in order to clarify their legal responsibilities in the US jurisdiction. While this has mainly manifested itself in the form of state laws, there is anticipation of a federal law on the horizon. Even American institutions have begun to imitate their EU counterparts, with the FTC giving its largest fine to date to Facebook at five

[397] "Gijs de Vries: EU Counter-Terrorism Coordinator," NATO Review, September 1, 2005, https://www.nato.int/docu/review/articles/2005/09/01/gijs-de-vries-eu-counter-terrorism-coordinator/index.html.
[398] SCOTT, "Extraterritoriality and Territorial Extension in EU Law."

billion dollars citing data protection as the main reason behind the fine. This even trumps the biggest GDPR fine ever given out, which was to Google at fifty-seven million dollars.

While advantageous for the EU, this holds significant consequences for sovereignty which centers on the ability of a state to express authority over its jurisdictional limits, which is intrinsically related to territory. In an interdependent world with soft power, jurisdictional limits based on territory do not match up with the extent of the state's authority.[399] To be clear, this does not mean that the significance of the state will wither in light of soft power. Rather, soft power will become the preferred method of state competition since it is able to circumvent the formal authority of the other state altogether while achieving the outcome it wants. And the EU provides a prime example for other states to follow. While international law affords sovereignty according to distinct delineations such as to separate one state from another, this system may prove difficult to maintain as the ability to dictate conditions of data flows becomes a means of extending authority into another jurisdiction. Therefore, the EU's use of the GDPR may encourage scholars to theorize new interpretations of the means of territory, jurisdiction, and who can be governed by a regulation.

Conclusion

Weighing the analytical frameworks of complex interdependence and CWS against one another, it is clear that neither entirely satisfy. Complex interdependence does offer a powerful lens to explain why regulatory cooperation arises in the first place. The development of data protection law in the EU exemplifies complex interdependence at its best, with the OECD and the Council of Europe using multilateral coordination which set a foundation for later EU policies.

[399] Mueller, *Will the Internet Fragment?*

Complex interdependence still remains relevant when explaining why the EU and the US would engage in cooperation despite extensive differences in their legal attitudes towards data protection. Their intention to find a workable solution, even after the failure of the first bilateral agreement, further speaks in favor of complex interdependence.

However, complex interdependence does have its shortcomings. While both the US and the EU were invested in maintaining bilateral agreements, the persistence of national interests and disparate institutional arrangements led to American non-compliance under Safe Harbor. Different legal attitudes meant that data protection was codified to different degrees in each domestic context. The US was expected to incur more adjustment costs in comparison to the EU, since any agreement was going to result in obligations that were new to US institutions. Moreover, the US had competing priorities. While the US lacked the necessary bureaucratic scaffolding for data protection, it had invested extensively in its national security apparatus, from decreasing barriers for data-sharing among intelligence agencies to passing laws like the Patriot Act which expanded the powers of the CIA, FBI and NSA. Therefore, while the US needed to cooperate with the EU in order to secure an adequacy decision and maintain the EU-US data flow, the US was also subject to domestic constraints that limited the extent to which the US was able to commit to its negotiating partner.

Although CWS complicates the feasibility of cooperation, soft power provided a way for the EU to maintain its bilateral agreement the US while achieving their own goals de facto with the extraterritorial effects of the GDPR. Despite the fact that the Privacy Shield is in place to provide US corporations with alternative means of achieving GDPR compliance, the stringency of the regulation, coupled with its extraterritorial reach, has led to corporations globalizing the GDPR regardless of jurisdictional limits. Further, the high sanctions of the GDPR are reinforced by the

EU institutions that are willing and capable to administer the fines. While the de facto adoption of the GDPR by multinational corporations are a direct result of the GDPR, the other extraterritorial effects are mainly an indirect result of multiple channels of communication between jurisdictions that aided in raising the issue salience of data protection among the US population. Networked advocacy and transnational media coverage provided Americans with knowledge of the associated risks of foregoing data protection. In response to demands from citizens and corporations alike, American lawmakers have been pressured to adopt data protection laws at the state level, with expectations of a federal law in the near future.

Therefore, the soft power of the EU relies on continued bilateral cooperation in order to sustain the extraterritorial effects of the GDPR. In this way, complex interdependence can serve a national interest if it provides the ability for a state to heighten the appeal of its own regulation in another jurisdiction. However, appeal does not come cheap. A state must cultivate appeal, whether it be from consistency in internal regulation, adherence to stringent rules, or reinforcement by institutional mechanisms. The endurance of data protection as a right in Europe, later codified in the GDPR, led to the persistent rationale of the EU to uphold data protection through bureaucratic means. As a result, the EU was in a better position to employ soft power over the EU-US data flow because the US could not compete with a framework of its own. Until the US does adopt its own framework, the dominance of the GDPR via its extraterritorial effects is likely to continue.

Conclusion: A Future of Contentious Cooperation for the Internet of Tomorrow

In 2017, the Global Commission on Internet Governance wrote a report that noted the "emergence of contention in Global Internet Governance."[400] Contention could threaten the feasibility of inter-state cooperation that is requisite to maintain Internet connectivity via the openness of data flows. Coordination problems amongst states offers clear evidence of this contention, but states themselves also struggle to balance domestic priorities with transnational commitments. No longer is the Internet "just a technical administrative issue"[401]; maintaining the Internet requires states intervention "for a number of public interest concerns, such as infrastructure availability, security, and individual civil liberties."[402] As Internet governance is inherently multifaceted, involving many actors that are concerned with particular applications of the Internet, such as trade, development or national security, rather than its technical underpinning.[403] As a result, identifying shared governance solutions through cooperation will become more challenging at both the domestic and international levels. States unique approaches to their priorities and policies governing the Internet will further complicate inter-state relations; coordination among states will require tailored approaches to meet the specific needs of the negotiating states.

The findings of this paper provide valuable insights concerning the feasibility of state cooperation for Internet governance. While data protection is only one of many state concerns related to the Internet, it is a central issue that may facilitate or impede data flows. The transatlantic data protection debate between the EU and the US illustrates that while cooperation is desirable,

[400] Bradshaw et al., "THE EMERGENCE OF CONTENTION IN GLOBAL INTERNET GOVERNANCE."
[401] Bradshaw et al, 46.
[402] Bradshaw et al, 46.
[403] Nye, "The Regime Complex for Managing Global Cyber Activities."

it may be unexpectedly challenging to execute in reality, even amongst political and economic allies. Differences in the relative priorities of the US and the EU led to persistent challenges in the maintenance of data protection agreements, a problem exacerbated by insufficient institutional competence on the part of the US, as the US attempted to maintain a focus on national security, even as it conflicted with its bilateral commitments on data protection. At the same time, states had to consider with the interests of non-state actors, such as multinational corporations and activists, who attempted to influence or resist state regulations. Therefore, contention arises not only internationally, but also domestically, as states must wrestle with multiple priorities in combination with demands from many actors.

Moreover, this paper highlights the fact that longstanding legal approaches are applied to Internet governance in each case, and not designed from scratch to address the challenges of the digital realm. While one might expect that technological innovation prompt novel legal instruments, in fact fundamental ideas about civil liberties like privacy dictate how states respond to new technological pressures. The multilateral agreement amongst EU member states, a consensus facilitated by the OECD and the Council of Europe that was fifty years in the making, upheld data protection as a human right. Without this legal history, the EU likely would not have had the political will to create the stringent rules it did under the GDPR. In turn, the EU was able to pass the GDPR, codify data protection as a human right in pre-existing institutions like the ECJ, and also create new institutions like the EDPB that were tasked with the primary responsibility of safeguarding this right.

As contention rises amongst states, making cooperation more difficult, states may employ soft power as a means of reconciling the tensions between internal priorities and bilateral commitments. Soft power can be used to persuade non-state actors and subnational actors about

the merits of the state's desired regulatory model. Asymmetries in institutional capacity provide states like the EU the ability to forward its data protection agenda indirectly through the extraterritorial effects of regulation. The EU derives a competitive advantage from that fact that it had unified 28-member states on a single regulatory approach to data protection, a model that in turn exerts influence through non-state actors within the US jurisdiction. While this competitive advantage can be especially effective in the highly fragmented nature of US federalism, it holds true for every other state that hopes to negotiate with the EU due to the stringency of the GDPR which applies globally. As a result, the EU may be willing to tolerate cooperative interstate agreements which may formally protect data at a de jure lower standard than the GDPR, since it is able to achieve de facto extraterritorial compliance through the use of other channels.

The EU-US transatlantic data protection debate confirms that cooperation is increasingly contentious, as states like the EU capitalize on their institutional capacities to extend their influence extraterritorially with legislation like the GDPR. As the complexities associated with interdependent governance of data grows, it is anticipated that more states adopt soft power tactics in order to resolve the tension between internal and external responsibilities. The distinction among states will wane as states extend authority beyond jurisdictional limits, further obscuring sovereign boundaries. Therefore, the use of technical infrastructure as a proxy for territory offers an incomplete legal framework to account for the disassociation of state power from territorial constraints with respect to Internet issues. In light of this conclusion, I encourage scholars to theorize new ways of applying jurisdiction to cyberspace, such that state sovereignty is defined in terms other than territory, thereby accounting for the nature of data.

Finally, states that uphold data protection as a human right have another barrier to the maintenance of this right, beyond their bureaucratic duty to engage in cooperation with third

countries: time. While states like the EU incur an initial competitive advantage from accumulated knowledge in its institutions, the sustainability of its right to data protection can only be tested by its endurance over time. Moore's law states that every 18 months computer processing capabilities double.[404] As technologies like artificial intelligence, blockchain, and the Internet of Things (IoT) enter the homes of average citizens, the right to data protection is further endangered, as the question is no longer if it *should* be enforced, but if it *could* be practically enforced at all.[405]Although institutions can marginally adapt legal interpretations to account for shifts in short-run, the durability of the right to data protection in the long-run ultimately comes down to the time lost between now and catch up.

[404] Michael F. Wolff, "Chase Moore's Law, Inventors Urged," *Research Technology Management* 47, no. 1 (2004): 6–6.
[405] Cameron F. Kerry, "Why Protecting Privacy Is a Losing Game Today—and How to Change the Game," *Brookings* (blog), July 12, 2018, https://www.brookings.edu/research/why-protecting-privacy-is-a-losing-game-today-and-how-to-change-the-game/.

Bibliography

"- THE EU DATA PROTECTION DIRECTIVE: IMPLICATIONS FOR THE U.S. PRIVACY DEBATE." Accessed April 30, 2020. https://www.govinfo.gov/content/pkg/CHRG-107hhrg71497/html/CHRG-107hhrg71497.htm.

Pew Research Center. "10 Tech-Related Trends That Shaped the Decade." Accessed April 13, 2020. https://www.pewresearch.org/fact-tank/2019/12/20/10-tech-related-trends-that-shaped-the-decade/.

14:30, Rebecca Hill 18 Jan 2019 at. "Say GDP-AaaRrrgh, Streamers: Max Schrems Is Coming for You, Netflix and Amazon." Accessed April 15, 2020. https://www.theregister.co.uk/2019/01/18/streaming_services_slapped_with_complaints_alleging_failure_to_meet_gdpr_rights/.

"2019 Data Breaches: 4 Billion Records Breached So Far." Accessed April 13, 2020. https://us.norton.com/internetsecurity-emerging-threats-2019-data-breaches.html.

TechCrunch. "A Senate Bill Would Create a New US Data Protection Agency." Accessed April 14, 2020. https://social.techcrunch.com/2020/02/13/gilliband-law-data-agency/.

"About the OECD - OECD." Accessed April 30, 2020. https://www.oecd.org/about/.

"About Us." Accessed April 30, 2020. https://www.nsa.gov/about/.

"Agreement between The United States of America and The European Union on the Protection of Personal Information Relating to the Prevention, Investigation, Detection, and Prosecution of Criminal Offenses (Not yet Binding under PIL)." Accessed April 15, 2020. https://eclan.eu/en/eu-legislatory/agreement-between-the-united-states-of-america-and-the-european-union-on-the-protection-of-personal-information-relating-to-the-prevention-investigation-detection-and-prosecution-of-criminal-offenses-not-yet-binding-under-pil.

"Alastair Mactaggart: First CCPA, Tackles CPRA Next." Accessed April 13, 2020. https://www.natlawreview.com/article/next-act-architect-california-consumer-privacy-act-california-privacy-rights-act.

Allen, Chris, Michael Gasiorek, Alasdair Smith, Harry Flam, and Peter Birch Sørensen. "The Competition Effects of the Single Market in Europe." *Economic Policy* 13, no. 27 (1998): 441–86.

"Anu Bradford, The Brussels Effect, 107 NW. U. L. REV. 1 (2012). Available at: Https://Scholarship.Law.Columbia.Edu/Faculty_scholarship/271," n.d.

AppleInsider. "Apple Urges Customers to Keep Data Safe in New 'Privacy on IPhone' Ad." Accessed April 13, 2020. https://appleinsider.com/articles/19/10/25/apple-shares-new-privacy-on-iphone-ad-urges-users-to-protect-personal-data.

Arnull, Anthony. *The European Union and Its Court of Justice*. 2nd ed. Oxford EC Law Library. Oxford ; New York: Oxford University Press, 2006.

Azzi, Adèle. "The Challenges Faced by the Extraterritorial Scope of the General Data Protection Regulation." *JIPITEC* 9, no. 2 (2018): 126–37.

Baldwin, David A. "Realism." In *Power and International Relations*, 123–38. A Conceptual Approach. Princeton University Press, 2016. https://doi.org/10.2307/j.ctt1q1xsp6.8.

Baliga, B. R., and Alfred M. Jaeger. "Multinational Corporations: Control Systems and Delegation Issues." *Journal of International Business Studies* 15, no. 2 (1984): 25–40.

Bamford, James. "Edward Snowden: The Untold Story." *Wired*, August 13, 2014. https://www.wired.com/2014/08/edward-snowden/.

Bauman, Zygmunt, Didier Bigo, Paulo Esteves, Elspeth Guild, Vivienne Jabri, David Lyon, and R. B. J. Walker. "After Snowden: Rethinking the Impact of Surveillance." *International Political Sociology* 8, no. 2 (June 2014): 121–44. https://doi.org/10.1111/ips.12048.

Bell, Emily, Taylor Owen, Smitha Khorana, Jennifer R. Henrichsen, and Lee C. Bollinger, eds. *Journalism after Snowden: The Future of the Free Press in the Surveillance State*. Columbia Journalism Review Books. New York: Columbia University Press, 2017.

Bendiek, Annegret, and Magnus Römer. "Externalizing Europe: The Global Effects of European Data Protection." *Digital Policy, Regulation and Governance* 21, no. 1 (January 1, 2019): 32–43. https://doi.org/10.1108/DPRG-07-2018-0038.

"Betzel, Margaret, 'Privacy Law Developments In California,' I/S: A Journal of Law and Policy for the Information Society, Vol. 2, No. 3 (2006), 831-877.," n.d.

Bildt, H.E. Carl, William E. Kennard, Frances G. Burwell, and Tyson Barker. "A Transatlantic Digital Marketplace:" Building a Transatlantic Digital Marketplace: Atlantic Council, 2016. JSTOR. www.jstor.org/stable/resrep03652.7.

Birnbaum, Emily. "GOP Senator Introduces Privacy Legislation after Bipartisan Talks Break Down." Text. TheHill, March 12, 2020. https://thehill.com/policy/technology/487157-gop-senator-introduces-privacy-legislation-after-bipartisan-talks-break.

Blair, Alasdair, and Steven Curtis. "European Integration." In *International Politics*, 265–93. An Introductory Guide. Edinburgh University Press, 2009. www.jstor.org/stable/10.3366/j.ctt1g0b1tz.18.

Bowie, Norman E., and Karim Jamal. "Privacy Rights on the Internet: Self-Regulation or Government Regulation?" *Business Ethics Quarterly* 16, no. 3 (2006): 323–42.

Bradford, Anu. "The Brussels Effect." In *The Brussels Effect*, by Anu Bradford, 25–66. Oxford University Press, 2020. https://doi.org/10.1093/oso/9780190088583.003.0003.

———. *The Brussels Effect: How the European Union Rules the World*. New York: Oxford University Press, 2020.

———. "The EU as a Regulatory Power." CONNECTIVITY WARS. European Council on Foreign Relations, 2016. JSTOR. https://doi.org/10.2307/resrep21667.20.

Bradshaw, Samantha, Laura DeNardis, Fen Osler Hampson, Eric Jardine, Mark Raymond, and GLOBAL COMMISSION ON INTERNET GOVERNANCE. "THE EMERGENCE OF CONTENTION IN GLOBAL INTERNET GOVERNANCE." Who Runs the Internet? Centre for International Governance Innovation, 2017. JSTOR. www.jstor.org/stable/resrep05243.8.

Brandom, Russell. "The FBI Has Asked Apple to Unlock Another Shooter's IPhone." The Verge, January 7, 2020. https://www.theverge.com/2020/1/7/21054836/fbi-iphone-unlock-apple-encryption-debate-pensacola-ios-security.

BrasseurTue, Kyle, Sep 10, and 2019 2:43 Pm. "Amazon's Bezos among 51 CEOs Calling for National Data Privacy Law." Compliance Week. Accessed April 14, 2020. https://www.complianceweek.com/data-privacy/amazons-bezos-among-51-ceos-calling-for-national-data-privacy-law/27678.article.

Bu-Pasha, Shakila. "Cross-Border Issues under EU Data Protection Law with Regards to Personal Data Protection." *Information & Communications Technology Law* 26, no. 3 (September 2, 2017): 213–28. https://doi.org/10.1080/13600834.2017.1330740.

Burk, Dan L. "Law as a Network Standard." In *The Global Flow of Information*, edited by Ramesh Subramanian and Eddan Katz, 156–72. Legal, Social, and Cultural Perspectives. NYU Press, 2011. www.jstor.org/stable/j.ctt9qfr5n.12.

Buxbaum, Hannah L. "Territory, Territoriality, and the Resolution of Jurisdictional Conflict." *The American Journal of Comparative Law* 57, no. 3 (July 1, 2009): 631–76. https://doi.org/10.5131/ajcl.2008.0018.

Byers, Alex. "USA Freedom Act vs. USA PATRIOT Act." POLITICO. Accessed April 30, 2020. https://www.politico.com/story/2015/05/usa-freedom-act-vs-usa-patriot-act-118469.html.

C-131/12 Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González, 2014 E.C.R. 317.

C-362/14 Maximilian Schrems v. Data Protection Commissioner, 2015 E.C.R. 650.

Carrière-Swallow, Yan, and Vikram Haksar. "The Economics and Implications of Data: An Integrated Perspective." International Monetary Fund, September 2019. file:///Users/sasajovanovic/Downloads/TEIDEA.pdf.

Carruthers, Bruce G., and Naomi R. Lamoreaux. "Regulatory Races: The Effects of Jurisdictional Competition on Regulatory Standards." *Journal of Economic Literature* 54, no. 1 (2016): 52–97.

Cavoukian, Ann, and Fred Carter. "Privacy by Design: The 7 Foundational Principles – Implementation and Mapping of Fair Information Practices." Internet Architecture Board, December 2010. https://www.iab.org/wp-content/IAB-uploads/2011/03/fred_carter.pdf.

"CCPA and GDPR Comparison Chart." Accessed April 14, 2020. https://iapp.org/resources/article/ccpa-and-gdpr-comparison-chart/.

Chin, Caitlin. "Highlights: The GDPR and CCPA as Benchmarks for Federal Privacy Legislation." *Brookings* (blog), December 19, 2019. https://www.brookings.edu/blog/techtank/2019/12/19/highlights-the-gdpr-and-ccpa-as-benchmarks-for-federal-privacy-legislation/.

Clark, R H. "Constitutional Sources of the Penumbral Right to Privacy." *Villanova Law Review* 19 (n.d.): 53.

Claudio M. Radaelli. "The Puzzle of Regulatory Competition." *Journal of Public Policy* 24, no. 1 (2004): 1–23.

Cochran, Charles L. "De Facto and De Jure Recognition: Is There a Difference?" *The American Journal of International Law* 62, no. 2 (1968): 457–60.

Cole, David, and Federico Fabbrini. "Bridging the Transatlantic Divide? The United States, the European Union, and the Protection of Privacy across Borders." *International Journal of Constitutional Law* 14, no. 1 (January 2016): 220–37. https://doi.org/10.1093/icon/mow012.

COMELLA, VÍCTOR FERRERES. "The Impact of the European Court of Human Rights." In *Constitutional Courts and Democratic Values*, 139–54. A European Perspective. Yale University Press, 2009. www.jstor.org/stable/j.ctt1np70w.16.

"Commission Proposes a Comprehensive Reform of Data Protection Rules to Increase Users' Control of Their Data and to Cut Costs for Businesses," January 25, 2012. https://ec.europa.eu/commission/presscorner/detail/en/IP_12_46.

Commission Regulation 16/679, 2016 O.J. (L 119) p 1-88.

"Confronting A Data Privacy Crisis, Gillibrand Announces Landmark Legislation To Create A Data Protection Agency | Kirsten Gillibrand | U.S. Senator for New York." Accessed April 14, 2020. https://www.gillibrand.senate.gov/news/press/release/confronting-a-data-privacy-crisis-gillibrand-announces-landmark-legislation-to-create-a-data-protection-agency.

"Congressional Record, V. 148, PT. 7, May 23, 2002 to June 12, 2002," n.d.

Connolly, Chris. "The US Safe Harbor: Fact or Fiction?" Galexia, 2008.
Coombe, George W., and Susan L. Kirk. "Privacy, Data Protection, and Transborder Data Flow: A Corporate Response to International Expectations." *The Business Lawyer* 39, no. 1 (1983): 33–66.
"'Copycat CCPA' Bills Introduced in States Across Country | Privacy & Security Law Blog | Davis Wright Tremaine." Accessed April 30, 2020. https://www.dwt.com/blogs/privacy--security-law-blog/2019/02/copycat-ccpa-bills-introduced-in-states-across-cou.
Council Directive 95/46, 1995 O.J. (L 281) pg 31-50.
Coyne, Hallie. "The Untold Story of Edward Snowden's Impact on the GDPR." *The Cyber Defense Review* 4, no. 2 (2019): 65–80. https://doi.org/10.2307/26843893.
Culnan, Mary J. "Protecting Privacy Online: Is Self-Regulation Working?" *Journal of Public Policy & Marketing* 19, no. 1 (2000): 20–26.
cycles, This text provides general information Statista assumes no liability for the information given being complete or correct Due to varying update, and Statistics Can Display More up-to-Date Data Than Referenced in the Text. "Topic: Internet Usage Worldwide." www.statista.com. Accessed April 30, 2020. https://www.statista.com/topics/1145/internet-usage-worldwide/.
"Data Is Power: Profiling and Automated Decision-Making in GDPR Report." Privacy International, April 9, 2018. https://privacyinternational.org/report/1718/data-power-profiling-and-automated-decision-making-gdpr.
GDPR.eu. "Data Protection Impact Assessment (DPIA)," August 9, 2018. https://gdpr.eu/data-protection-impact-assessment-template/.
"Data Protection Reform - Parliament Approves New Rules Fit for the Digital Era | News | European Parliament," April 14, 2016. https://www.europarl.europa.eu/news/en/press-room/20160407IPR21776/data-protection-reform-parliament-approves-new-rules-fit-for-the-digital-era.
Demchak, Chris C. "Uncivil and Post-Western Cyber Westphalia." *The Cyber Defense Review* 1, no. 1 (2016): 49–74.
Demchak, Chris C., and Peter J. Dombrowski. "Rise of a Cybered Westphalian Age: The Coming Decades." In *The Global Politics of Science and Technology - Vol. 1: Concepts from International Relations and Other Disciplines*, edited by Maximilian Mayer, Mariana Carpes, and Ruth Knoblich, 91–113. Berlin, Heidelberg: Springer Berlin Heidelberg, 2014. https://doi.org/10.1007/978-3-642-55007-2_5.
Demchak, Chris, and Peter Dombrowski. "Cyber Westphalia: Asserting State Prerogatives in Cyberspace." *Georgetown Journal of International Affairs*, 2013, 29–38.
Demchak, Chris, and U.S. Naval War College. "Three Futures for a Post-Western Cybered World." *Military Cyber Affairs* 3, no. 1 (June 2018). https://doi.org/10.5038/2378-0789.3.1.1044.
DeNardis, Laura. "Internet Points of Control as Global Governance." Internet Governance Papers. Waterloo, Canada: The Centre for International Governance Innovation, August 2013. https://www.cigionline.org/sites/default/files/no2_3.pdf.
DeNardis, Laura, and GLOBAL COMMISSION ON INTERNET GOVERNANCE. "INTRODUCTION:" A Universal Internet in a Bordered World. Centre for International Governance Innovation, 2016. JSTOR. www.jstor.org/stable/resrep05249.5.

"Digital Economy Accounted for 6.9 Percent of GDP in 2017 | U.S. Bureau of Economic Analysis (BEA)." Accessed April 19, 2020. https://www.bea.gov/news/blog/2019-04-04/digital-economy-accounted-69-percent-gdp-2017.

"Digital Economy Report 2019: Value Creation and Capture Implications for Developing Countries." New York, New York: United Nations Conference on Trade and Development, 2019. https://unctad.org/en/PublicationsLibrary/der2019_overview_en.pdf.

Donohue, Laura K. *The Future of Foreign Intelligence: Privacy and Surveillance in a Digital Age*, 2016. http://public.ebookcentral.proquest.com/choice/publicfullrecord.aspx?p=4717489.

Dougherty, Conor. "Jay Edelson, the Class-Action Lawyer Who May Be Tech's Least Friended Man." *The New York Times*, April 4, 2015, sec. Technology. https://www.nytimes.com/2015/04/05/technology/unpopular-in-silicon-valley.html.

Drezner, Daniel W. *All Politics Is Global: Explaining International Regulatory Regimes*, 2008. https://doi.org/10.1515/9781400828630.

Drezner, Daniel W. "Globalization and Policy Convergence." *International Studies Review* 3, no. 1 (2001): 53–78.

Durkee, Alison. "Zoom Gets Federal Government's Attention As Privacy Concerns Mount." Vanity Fair. Accessed April 30, 2020. https://www.vanityfair.com/news/2020/04/zoom-privacy-concerns-ftc-investigation.

Eckes, Christina. *EU Powers under External Pressure: How the EU's External Actions Alter Its Internal Structures*, 2019. https://search.ebscohost.com/login.aspx?direct=true&scope=site&db=nlebk&db=nlabk&AN=2003807.

Egan, Michelle P., ed. *Creating a Transatlantic Marketplace: Government Policies and Business Strategies*. European Policy Research Unit Series. Manchester ; New York: Manchester University Press, 2005.

Elliott, Francis. "Cameron Hints at Action to Stop Security Leaks." *The Times*, October 28, 2013, sec. unknown section. https://www.thetimes.co.uk/article/cameron-hints-at-action-to-stop-security-leaks-krg6tl9w80c.

European Commission - European Commission. "EU Commission and United States Agree on New Framework for Transatlantic Data Flows: EU-US Privacy Shield." Text. Accessed April 4, 2020. https://ec.europa.eu/commission/presscorner/detail/en/IP_16_216.

"EU Position in World Trade - Trade - European Commission." Accessed April 25, 2020. https://ec.europa.eu/trade/policy/eu-position-in-world-trade/.

Europäische Union, and Europarat, eds. *Handbook on European Data Protection Law*. 2018 edition. Handbook / FRA, European Union Agency for Fundamental Rights. Luxembourg: Publications Office of the European Union, 2018.

"Europe, Not the U.S., Is Now the Most Powerful Regulator of Silicon Valley - The Washington Post." Accessed April 30, 2020. https://www.washingtonpost.com/.

European Commission - European Commission. "European Commission Launches EU-U.S. Privacy Shield." Text. Accessed April 15, 2020. https://ec.europa.eu/commission/presscorner/detail/en/IP_16_2461.

"EU-US Data Transfers Won't Be Blocked While Privacy Shield Details Are Hammered Out, Says WP29 | TechCrunch." Accessed April 4, 2020. https://techcrunch.com/2016/02/03/eu-us-data-transfers-wont-be-blocked-while-privacy-shield-details-are-hammered-out-says-wp29/?guccounter=1&guce_referrer=aHR0cHM6Ly9lbi53aWtpcGVkaWEub3JnLw&gu

ce_referrer_sig=AQAAAMmVFFYWXYECAg_HghpkMSRRZZZH9-1fIiVuM0kjJxMQtk7WwjN46LuBTiy3aeIHv2MDPuQ_n226LUnTard9K5Y1H_q8FOzkyL-4uAJm0QazCoWdYlVDKc5lSp_2mXwNZvuobkg52FNoWeO0yrRk49QlAQ8lcWsKPxXj__oHrmi3.

"EU-U.S. Joint Statement on Data Protection by European Commission Vice-President Viviane Reding and U.S. Secretary of Commerce John Bryson," March 19, 2012. https://ec.europa.eu/commission/presscorner/detail/en/MEMO_12_192.

Technology Law Dispatch. "EU–U.S. Privacy Shield: EU Commission Issues Its Third Annual Review Report," November 6, 2019. https://www.technologylawdispatch.com/2019/11/regulatory/eu-u-s-privacy-shield-eu-commission-issues-its-third-annual-review-report/.

"EU-US PRIVACY SHIELD FORM FOR SUBMISSION OF REQUESTS TO THE U.S. OMBUDSPERSON," n.d. file:///Users/sasajovanovic/Downloads/20170417_PrivacyShield_RequestformunderOmbudspersonmechanism_enpdf.pdf.

"EU-U.S. PRIVACY SHIELD FRAMEWORK PRINCIPLES ISSUED BY THE U.S. DEPARTMENT OF COMMERCE." US Department of Commerce, n.d. https://www.privacyshield.gov/servlet/servlet.FileDownload?file=015t00000004qAg.

TechCrunch. "EU-US Privacy Shield Remains Precariously Placed." Accessed April 30, 2020. https://social.techcrunch.com/2017/04/06/eu-us-privacy-shield-remains-precariously-placed/.

European Commission - European Commission. "EU-U.S. Privacy Shield: Second Review Shows Improvements but a Permanent Ombudsperson Should Be Nominated by 28 February 2019." Text. Accessed April 30, 2020. https://ec.europa.eu/commission/presscorner/detail/en/IP_18_6818.

European Commission - European Commission. "EU-U.S. Privacy Shield: Third Review." Text. Accessed April 4, 2020. https://ec.europa.eu/commission/presscorner/detail/en/IP_19_6134.

Evans, A. C. "European Data Protection Law." *The American Journal of Comparative Law* 29, no. 4 (1981): 571–82. https://doi.org/10.2307/839754.

"Explanatory Report to the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data." Strasbourg: Council of Europe, 1981.

"Facebook Launches a New Ad Campaign With an Old Message." *Wired*. Accessed April 13, 2020. https://www.wired.com/story/facebook-launches-a-new-ad-campaign-with-an-old-message/.

Fan, Ziyang, and Anil Gupta. "The Dangers of Digital Protectionism." *Harvard Business Review*, August 30, 2018. https://hbr.org/2018/08/the-dangers-of-digital-protectionism.

Farer, Tom J. "Political and Economic Coercion in Contemporary International Law." *American Journal of International Law* 79, no. 2 (1985): 405–13. https://doi.org/10.2307/2201710.

Farrell, Henry. "Constructing the International Foundations of E-Commerce—The EU-U.S. Safe Harbor Arrangement." *International Organization* 57, no. 2 (2003): 277–306. https://doi.org/10.1017/S0020818303572022.

Farrell, Henry, and Abraham Newman. *Of Privacy and Power: The Transatlantic Struggle over Freedom and Security*, 2019. https://doi.org/10.1515/9780691189956.

Farrier, Jasmine. “The Patriot Act’s Institutional Story: More Evidence of Congressional Ambivalence.” *PS: Political Science and Politics* 40, no. 1 (2007): 93–97.

“First Annual Review of the EU-U.S. Privacy Shield Brussels.” Brussels, Belgium: European Commission, October 18, 2017.

“Forget the Techlash. The Lawlash Is Long Overdue | WIRED.” Accessed April 30, 2020. https://www.wired.com/story/opinion-forget-the-techlash-the-lawlash-is-long-overdue/.

“French Data Protection Watchdog Fines Google $57 Million under the GDPR | TechCrunch.” Accessed April 30, 2020. https://techcrunch.com/2019/01/21/french-data-protection-watchdog-fines-google-57-million-under-the-gdpr/.

Federal Trade Commission. “FTC Imposes $5 Billion Penalty and Sweeping New Privacy Restrictions on Facebook,” July 24, 2019. https://www.ftc.gov/news-events/press-releases/2019/07/ftc-imposes-5-billion-penalty-sweeping-new-privacy-restrictions.

“Full Text of Letter Containing Comments of ‘Safe-Harbor’ Pact.” *Wall Street Journal*, April 6, 2000, sec. Front Section. https://www.wsj.com/articles/SB954961643812226656.

Gabbatt, Adam. “Edward Snowden a ‘hero’ for NSA Disclosures, Wikipedia Founder Says.” *The Guardian*, November 25, 2013, sec. World news. https://www.theguardian.com/world/2013/nov/25/edward-snowden-nsa-wikipedia-founder.

Gady, Franz-Stefan. “EU/U.S. Approaches to Data Privacy and the ‘Brussels Effect’: A Comparative Analysis.” *Georgetown Journal of International Affairs*, 2014, 12–23.

Gearty, C. A. “The European Court of Human Rights and the Protection of Civil Liberties: An Overview.” *The Cambridge Law Journal* 52, no. 1 (1993): 89–127.

NATO Review. “Gijs de Vries: EU Counter-Terrorism Coordinator,” September 1, 2005. https://www.nato.int/docu/review/articles/2005/09/01/gijs-de-vries-eu-counter-terrorism-coordinator/index.html.

Gilardi, Fabrizio. “Transnational Diffusion: Norms, Ideas, and Policies.” In *Handbook of International Relations*, 453–77. 1 Oliver’s Yard, 55 City Road, London EC1Y 1SP United Kingdom: SAGE Publications Ltd, 2013. https://doi.org/10.4135/9781446247587.n18.

Gilbert, Ben. “Clearview AI Scraped Billions of Photos from Social Media to Build a Facial Recognition App That Can ID Anyone — Here’s Everything You Need to Know about the Mysterious Company.” Business Insider. Accessed April 30, 2020. https://www.businessinsider.com/what-is-clearview-ai-controversial-facial-recognition-startup-2020-3.

“Global Flows in a Digital Age | McKinsey.” Accessed April 4, 2020. https://www.mckinsey.com/business-functions/strategy-and-corporate-finance/our-insights/global-flows-in-a-digital-age.

González-Fuster, Gloria. *The Emergence of Personal Data Protection as a Fundamental Right of the EU*. Law, Governance and Technology Series, volume 16. Cham ; New York: Springer, 2014.

“Google and Yahoo Win Appeal in Argentine Case - The New York Times.” Accessed April 29, 2020. https://www.nytimes.com/2010/08/20/technology/internet/20google.html?_r=0.

NPR.org. “Google Has Received 650,000 ‘Right To Be Forgotten’ Requests Since 2014.” Accessed April 12, 2020. https://www.npr.org/sections/thetwo-way/2018/02/28/589411543/google-received-650-000-right-to-be-forgotten-requests-since-2014.

"Google's AMP Project Announces New Consent Component Ahead of GDPR Compliance Deadline - Search Engine Land." Accessed April 15, 2020. https://searchengineland.com/googles-amp-project-announces-new-consent-component-ahead-of-gdpr-compliance-deadline-295633.

Grafenstein, Maximilian von. "Conceptual Definitions as a Link for Regulation." In *The Principle of Purpose Limitation in Data Protection Laws*, 1st ed., 61–108. The Risk-Based Approach, Principles, and Private Standards as Elements for Regulating Innovation. Nomos Verlagsgesellschaft mbH, 2018. www.jstor.org/stable/j.ctv941v5w.4.

Greenstein, Shane. *How the Internet Became Commercial*. Princeton University Press, 2015. https://doi.org/10.2307/j.ctvc777gg.

Greer, Damon. "The US EU Safe Harbor Framework: Cross Border Data Flows, Data Protection, and Privacy." Presented at the International Trade Association, October 15, 2007.

Greze, Benjamin. "The Extra-Territorial Enforcement of the GDPR: A Genuine Issue and the Quest for Alternatives." *International Data Privacy Law*, April 21, 2019. https://doi.org/10.1093/idpl/ipz003.

Gunasekara, G. "The 'Final' Privacy Frontier? Regulating Trans-Border Data Flows." *International Journal of Law and Information Technology* 17, no. 2 (June 1, 2009): 147–79. https://doi.org/10.1093/ijlit/eam004.

Hamilton, Daniel S., Frances G. Burwell, Jeff Bialos, Megan Chabalowski, Heather Conley, Christine Fisher, Paul Isbell, et al. "Forging a Strategic U.S.-EU Partnership." Shoulder to Shoulder: Atlantic Council, 2009. JSTOR. www.jstor.org/stable/resrep03552.6.

Hanrieder, Wolfram F. "Compatibility and Consensus: A Proposal for the Conceptual Linkage of External and Internal Dimensions of Foreign Policy." *The American Political Science Review* 61, no. 4 (1967): 971–82. https://doi.org/10.2307/1953399.

Harknett, Richard J., and James A. Stever. "The Struggle to Reform Intelligence after 9/11." *Public Administration Review* 71, no. 5 (2011): 700–706.

Haunss, Sebastian. "Privacy Activism after Snowden: Advocacy Networks or Protest?," n.d., 19.

Henderson, Nathan C. "The Patriot Act's Impact on the Government's Ability to Conduct Electronic Surveillance of Ongoing Domestic Communications." *Duke Law Journal* 52, no. 1 (2002): 179–209. https://doi.org/10.2307/1373134.

Hern, Alex. "Facebook Agrees to Pay Fine over Cambridge Analytica Scandal." *The Guardian*, October 30, 2019, sec. Technology. https://www.theguardian.com/technology/2019/oct/30/facebook-agrees-to-pay-fine-over-cambridge-analytica-scandal.

Hoofnagle, Chris Jay, Bart van der Sloot, and Frederik Zuiderveen Borgesius. "The European Union General Data Protection Regulation: What It Is and What It Means." *Information & Communications Technology Law* 28, no. 1 (January 2, 2019): 65–98. https://doi.org/10.1080/13600834.2019.1573501.

GovTrack.us. "H.R. 3162 (107th): Uniting and Strengthening America by Providing Appropriate ... -- Senate Vote #313 -- Oct 25, 2001." Accessed April 30, 2020. https://www.govtrack.us/congress/votes/107-2001/s313.

Hurrell, Andrew. "Power, Institutions, and the Production of Inequality." In *Power in Global Governance*, edited by Michael Barnett and Raymond Duvall, 33–58. Cambridge Studies in International Relations. Cambridge: Cambridge University Press, 2004. https://doi.org/10.1017/CBO9780511491207.002.

"ICO Issues Maximum £500,000 Fine to Facebook for Failing to Protect Users' Personal Information." ICO, October 25, 2018. https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2018/10/facebook-issued-with-maximum-500-000-fine/.

"In Privacy Laws, an Incomplete American Quilt - The New York Times." Accessed April 30, 2020. https://www.nytimes.com/2013/03/31/technology/in-privacy-laws-an-incomplete-american-quilt.html.

Jennings, Rebecca. "What's Going on with TikTok, China, and the US Government?" Vox, December 16, 2019. https://www.vox.com/open-sourced/2019/12/16/21013048/tiktok-china-national-security-investigation.

Johnson, David R., and David Post. "Law and Borders: The Rise of Law in Cyberspace." *Stanford Law Review* 48, no. 5 (1996): 1367–1402. https://doi.org/10.2307/1229390.

Jr, Joseph S. Nye. "Multinationals: The Game and the Rules: Multinational Corporations in World Politics," August 31, 2017. https://www.foreignaffairs.com/articles/1974-10-01/multinationals-game-and-rules-multinational-corporations-world-politics.

Keohane, Robert O. "Reciprocity in International Relations." *International Organization* 40, no. 1 (1986): 1–27.

Keohane, Robert O., and Joseph S. Nye Jr. "Power and Interdependence in the Information Age," February 15, 2019. https://www.foreignaffairs.com/articles/1998-09-01/power-and-interdependence-information-age.

Keohane, Robert O., and Joseph S. Nye. *Power and Interdependence*. 2nd ed. Scott, Foresman/Little, Brown Series in Political Science. Glenview, Ill: Scott, Foresman, 1989.

Kerry, Cameron F. "Why Protecting Privacy Is a Losing Game Today—and How to Change the Game." *Brookings* (blog), July 12, 2018. https://www.brookings.edu/research/why-protecting-privacy-is-a-losing-game-today-and-how-to-change-the-game/.

Kirby, Michael. "The History, Achievement and Future of the 1980 OECD Guidelines on Privacy." *International Data Privacy Law* 1, no. 1 (October 5, 2010): 6–14. https://doi.org/10.1093/idpl/ipq002.

Kobrin, Stephen J., and Steve Kobrin. "Safe Harbours Are Hard to Find: The Trans-Atlantic Data Privacy Dispute, Territorial Jurisdiction and Global Governance." *Review of International Studies* 30, no. 1 (2004): 111–31.

Kogan, Lawrence A. "Exporting Europe's Protectionism." *The National Interest*, no. 77 (2004): 91–99.

KRASNER, STEPHEN D. "Problematic Sovereignty." In *Problematic Sovereignty*, edited by STEPHEN D. KRASNER, 1–23. Contested Rules and Political Possibilities. Columbia University Press, 2001. https://doi.org/10.7312/kras12178.5.

La Chapelle, Bertrand de, Paul Fehlinger, and GLOBAL COMMISSION ON INTERNET GOVERNANCE. "JURISDICTION ON THE INTERNET: FROM LEGAL ARMS RACE TO TRANSNATIONAL COOPERATION." A Universal Internet in a Bordered World. Centre for International Governance Innovation, 2016. JSTOR. www.jstor.org/stable/resrep05249.10.

Liaropoulos, A. "An International Cyber-Order under Construction?" *Journal of Information Warfare* 12, no. 2 (2013): 19–26.

Lillich, Richard B. "Economic Coercion and the International Legal Order." *International Affairs (Royal Institute of International Affairs 1944-)* 51, no. 3 (1975): 358–71. https://doi.org/10.2307/2616620.

Lind, Dara. “Everyone’s Heard of the Patriot Act. Here’s What It Actually Does.” Vox, June 2, 2015. https://www.vox.com/2015/6/2/8701499/patriot-act-explain.

Maher, Imelda. “The Networked (Agency) Regulation of Competition.” In *Regulatory Theory*, edited by PETER DRAHOS, 693–710. Foundations and Applications. ANU Press, 2017. www.jstor.org/stable/j.ctt1q1crtm.52.

Mantelero, Alessandro. “Regulating Big Data. The Guidelines of the Council of Europe in the Context of the European Data Protection Framework.” *Computer Law & Security Review* 33, no. 5 (October 2017): 584–602. https://doi.org/10.1016/j.clsr.2017.05.011.

———. “The EU Proposal for a General Data Protection Regulation and the Roots of the ‘Right to Be Forgotten.’” *Computer Law & Security Review* 29, no. 3 (June 2013): 229–35. https://doi.org/10.1016/j.clsr.2013.03.010.

Marcus, J Scott. “Contribution to Growth:The European Digital Single Market Delivering Economic Benefits for Citizens and Businesses,” n.d., 88.

Marmor, Davis Wright Tremaine LLP-Rachel R., Maryam Casbarro, Monder “Mike” Khoury, Nancy Libin, and Helen Goff Foster. “‘Copycat CCPA’ Bills Introduced in States Across Country | Lexology.” Accessed April 30, 2020. https://www.lexology.com/library/detail.aspx?g=163d5d78-e738-4ca1-a803-88f19db6b1ad.

“Max Schrems Files First Cases under GDPR against Facebook and Google.” Accessed April 4, 2020. https://www.irishtimes.com/business/technology/max-schrems-files-first-cases-under-gdpr-against-facebook-and-google-1.3508177.

Mayes, Tessa. “We Have No Right to Be Forgotten Online | Tessa Mayes.” *The Guardian*, March 18, 2011, sec. Opinion. https://www.theguardian.com/commentisfree/libertycentral/2011/mar/18/forgotten-online-european-union-law-internet.

Meltzer, Joshua P. “Cross-Border Data Flows, the Internet and What It Means for U.S. and EU Trade and Investment.” *Brookings* (blog), October 21, 2014. https://www.brookings.edu/blog/up-front/2014/10/21/cross-border-data-flows-the-internet-and-what-it-means-for-u-s-and-eu-trade-and-investment/.

Mendez, Fernando, and Mario Mendez. “Comparing Privacy Regimes: Federal Theory and the Politics of Privacy Regulation in the European Union and the United States.” *Publius* 40, no. 4 (2010): 617–45.

“Moran Tees Up Data Privacy Bill As Senate Effort Splinters.” Accessed April 30, 2020. https://news.bloomberglaw.com/privacy-and-data-security/moran-tees-up-data-privacy-bill-as-senate-effort-splinters.

“More Americans See Man Who Leaked NSA Secrets as ‘patriot’ than Traitor: Poll.” *Reuters*, June 12, 2013. https://www.reuters.com/article/us-usa-security-poll-idUSBRE95B1AF20130612.

Morrison, Sara. “Zoom Responds to Its Privacy (and Porn) Problems.” Vox, March 31, 2020. https://www.vox.com/recode/2020/3/31/21201019/zoom-coronavirus-privacy-hacks.

Mueller, Milton. *Will the Internet Fragment? Sovereignty, Globalization and Cyberspace*. Digital Futures. Cambridge, UK ; Malden, MA: Polity Press, 2017.

Mueller, Milton, John Mathiason, and Hans Klein. “The Internet and Global Governance: Principles and Norms for a New Regime.” *Global Governance* 13, no. 2 (2007): 237–54.

“National Security Agency Central Security Service > What We Do > Understanding the Threat.” Accessed April 30, 2020. https://www.nsa.gov/what-we-do/understanding-the-threat/.

American Civil Liberties Union. “National Security Letters.” Accessed April 30, 2020. https://www.aclu.org/other/national-security-letters.

“New York Times Launches ‘The Privacy Project.’” Accessed April 13, 2020. https://iapp.org/news/a/new-york-times-launches-the-privacy-project/.

Nicas, Jack, and Katie Benner. “F.B.I. Asks Apple to Help Unlock Two IPhones.” *The New York Times*, January 7, 2020, sec. Technology. https://www.nytimes.com/2020/01/07/technology/apple-fbi-iphone-encryption.html.

“NPR: The Patriot Act: Key Controversies.” Accessed April 30, 2020. https://www.npr.org/news/specials/patriotact/patriotactdeal.html.

Nye, Joseph. “The Regime Complex for Managing Global Cyber Activities.” Global Commission on Internet Governance. Centre for International Governance Innovation, May 2014. https://www.cigionline.org/sites/default/files/gcig_paper_no1.pdf.

Nye, Joseph S. “Public Diplomacy and Soft Power.” *The Annals of the American Academy of Political and Social Science* 616 (2008): 94–109.

———. “Soft Power.” *Foreign Policy*, no. 80 (1990): 153–71. https://doi.org/10.2307/1148580.

O’Malley, Tom, and Clive Soley. “Privacy and Self-Regulation.” In *Regulating the Press*, 165–74. Pluto Press, 2000. https://doi.org/10.2307/j.ctt183q680.13.

“Only ‘1% of Snowden Files Published.’” *BBC News*, December 3, 2013, sec. UK. https://www.bbc.com/news/uk-25205846.

Organisation for Economic Co-operation and Development. *Regulatory Co-Operation for an Interdependent World*. Paris: OECD Pub., 1994. https://doi.org/10.1787/9789264062436-en.

Palfrey, John Gorham, and Urs Gasser. *Interop the Promise and Perils of Highly Interconnected Systems*. New York: Basic Books, 2012. http://proquestcombo.safaribooksonline.com/9780465021970.

Patrick, P. Howard. “PRIVACY RESTRICTIONS ON TRANSNATIONAL DATA FLOWS: A COMPARISON OF THE COUNCIL OF EUROPE DRAFT CONVENTION AND OECD GUIDELINES.” *Jurimetrics* 21, no. 4 (1981): 405–20.

Payne, David. “Google, Doctors, and the ‘Right to Be Forgotten.’” *BMJ: British Medical Journal* 350 (2015). www.jstor.org/stable/26517819.

“Pentagon Says Snowden Took Most U.S. Secrets Ever: Rogers - Bloomberg.” Accessed April 12, 2020. https://web.archive.org/web/20140110092104/http://www.bloomberg.com/news/2014-01-09/pentagon-finds-snowden-took-1-7-million-files-rogers-says.html.

PETERS, MARK T. “Interdependence.” In *Cashing In on Cyberpower*, 13–44. How Interdependent Actors Seek Economic Outcomes in a Digital World. University of Nebraska Press, 2018. https://doi.org/10.2307/j.ctt22726v0.7.

———. “Interdependence.” In *Cashing In on Cyberpower*, 13–44. How Interdependent Actors Seek Economic Outcomes in a Digital World. University of Nebraska Press, 2018. https://doi.org/10.2307/j.ctt22726v0.7.

Phillips, Mark. “International Data-Sharing Norms: From the OECD to the General Data Protection Regulation (GDPR).” *Human Genetics* 137, no. 8 (August 2018): 575–82. https://doi.org/10.1007/s00439-018-1919-7.

Piodi, Franco, Iolanda Mombelli, European Parliament, and EPRS. *The ECHELON Affair: The European Parliament and the Global Interception System*. Luxembourg: Publications Office, 2014.

Plante, Chris. “A Short, Crucial Explanation of the USA Patriot Act and USA Freedom Act.” The Verge, October 20, 2015. https://www.theverge.com/2015/10/20/9573619/usa-patriot-act-freedom-explainer.

Poll, Finn Partners; Harris. “Harris Poll And Finn Partners Unveil New Metric For The Return On Investment For Social Good.” Accessed April 13, 2020. https://www.prnewswire.com/news-releases/harris-poll-and-finn-partners-unveil-new-metric-for-the-return-on-investment-for-social-good-300747201.html.

Porter, Jon. “Clearview AI’s Source Code and App Data Exposed in Cybersecurity Lapse.” The Verge, April 17, 2020. https://www.theverge.com/2020/4/17/21224718/clearview-ai-exposed-server-source-code-windows-ios-android-mac-apps-cloud-storage.

“Pressure Mounts on EU-US Privacy Shield after Facebook-Cambridge Analytica Data Scandal | TechCrunch.” Accessed April 30, 2020. https://techcrunch.com/2018/06/12/pressure-mounts-on-eu-us-privacy-shield-after-facebook-cambridge-analytica-data-scandal/.

Presuel, Rodrigo Cetina, and Sebastián Zárate Rojas. “Introduction to the Special Issue: The Right to the Protection of One’s Own Image in Ibero-America and Its Relevance for the Right of Publicity in Common Law Countries.” *Journal of Information Policy* 8 (2018): 338–45. https://doi.org/10.5325/jinfopoli.8.2018.0338.

World Economic Forum. “Privacy Is a Human Right, We Need a GDPR for the World: Microsoft CEO.” Accessed April 4, 2020. https://www.weforum.org/agenda/2019/01/privacy-is-a-human-right-we-need-a-gdpr-for-the-world-microsoft-ceo/.

“Privacy Shield.” Accessed April 30, 2020. https://www.privacyshield.gov/participant?id=a2zt00000008PdqAAE&status=Active.

AppleInsider. “‘Privacy. That’s IPhone’ Ad Campaign Launches, Highlights Apple’s Stance on User Protection.” Accessed April 13, 2020. https://appleinsider.com/articles/19/03/14/privacy-thats-iphone-ad-campaign-launches-highlights-apples-stance-on-user-protection.

Rana, Waheeda. “Theory of Complex Interdependence: A Comparative Analysis of Realist and Neoliberal Thoughts” 6, no. 2 (2015): 8.

Raymond, Mark. “Puncturing the Myth of the Internet as a Commons.” *Georgetown Journal of International Affairs*, 2013, 53–64.

Council on Foreign Relations. “Reforming the U.S. Approach to Data Protection and Privacy.” Accessed April 30, 2020. https://www.cfr.org/report/reforming-us-approach-data-protection.

Regan, Priscilla M. “Privacy as a Philosophical and Legal Concept.” In *Legislating Privacy*, 24–41. Technology, Social Values, and Public Policy. University of North Carolina Press, 1995. www.jstor.org/stable/10.5149/9780807864050_regan.6.

Release, Press. “Human Rights and Privacy Groups Launch Global Action to Oppose Mass Surveillance.” Electronic Frontier Foundation, November 26, 2013. https://www.eff.org/press/releases/human-rights-and-privacy-groups-launch-global-action-oppose-mass-surveillance.

“REPORT FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL on the Second Annual Review of the Functioning of the EU-U.S. Privacy Shield.” Brussels, Belgium: European Commission, December 12, 2018.

“REPORT FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL on the Third Annual Review of the Functioning of the EU-U.S. Privacy Shield.” European Commission, October 23, 2019.

"Report to the European Council On the Year 2000 (Y2K) Computer Problem Experience." Brussels, Belgium: European Commission, June 16, 2000.

TechCrunch. "Researchers Spotlight the Lie of 'Anonymous' Data." Accessed April 12, 2020. https://social.techcrunch.com/2019/07/24/researchers-spotlight-the-lie-of-anonymous-data/.

Richards, Neil M., and Daniel J. Solove. "Prosser's Privacy Law: A Mixed Legacy." *California Law Review* 98, no. 6 (2010): 1887–1924.

Riebling, Mark. *Wedge: From Pearl Harbor to 9/11: How the Secret War between the FBI and CIA Has Endangered National Security*. 1st Touchstone ed., Updated with a new epilogue. New York: Simon & Schuster, 2002, 2002.

Lawfare. "Road to Adequacy: Can California Apply Under the GDPR?," April 22, 2019. https://www.lawfareblog.com/road-adequacy-can-california-apply-under-gdpr.

Rodriguez, Daniel B. "Turning Federalism Inside out: Intrastate Aspects of Interstate Regulatory Competition." *Yale Law & Policy Review* 14, no. 2 (1996): 149–76.

Rogerson, Kenneth S. "INFORMATION INTERDEPENDENCE: Keohane and Nye's Complex Interdependence in the Information Age." *Information, Communication & Society* 3, no. 3 (January 2000): 415–36. https://doi.org/10.1080/13691180051033379.

Roser, Max, Hannah Ritchie, and Esteban Ortiz-Ospina. "Internet." *Our World in Data*, July 14, 2015. https://ourworldindata.org/internet.

Roth, Alexander D. "DOCUMENTS ON DATA PROTECTION." *International Legal Materials* 19, no. 2 (1980): 282–324.

Russell, Annelise, and Maxwell McCombs. "The Media." In *Policy Analysis in the United States*, edited by John A. Hird, 1st ed., 265–80. Bristol University Press, 2018. https://doi.org/10.2307/j.ctt22h6q1x.20.

Santosuosso, Amedeo, and Alessandra Malerba. "Legal Interoperability as a Comprehensive Concept in Transnational Law." *Law, Innovation and Technology* 6, no. 1 (May 27, 2014): 51–73. https://doi.org/10.5235/17579961.6.1.51.

Satariano, Adam. "G.D.P.R., a New Privacy Law, Makes Europe World's Leading Tech Watchdog." *The New York Times*, May 24, 2018, sec. Technology. https://www.nytimes.com/2018/05/24/technology/europe-gdpr-privacy.html.

Schmitt, Michael N., and NATO Cooperative Cyber Defence Centre of Excellence, eds. *Tallinn Manual on the International Law Applicable to Cyber Warfare: Prepared by the International Group of Experts at the Invitation of the NATO Cooperative Cyber Defence Centre of Excellence*. Cambridge ; New York: Cambridge University Press, 2013.

Schultz, Kenneth A. "What's in a Claim? De Jure versus De Facto Borders in Interstate Territorial Disputes." *The Journal of Conflict Resolution* 58, no. 6 (2014): 1059–84.

Schulze, Elizabeth. "Mark Zuckerberg Says He Wants Stricter European-Style Privacy Laws — but Some Experts Are Questioning His Motives." CNBC, April 1, 2019. https://www.cnbc.com/2019/04/01/facebook-ceo-zuckerbergs-call-for-gdpr-privacy-laws-raises-questions.html.

SCOTT, JOANNE. "Extraterritoriality and Territorial Extension in EU Law." *The American Journal of Comparative Law* 62, no. 1 (2014): 87–125.

Scott, Mark. "U.S. and Europe in 'Safe Harbor' Data Deal, but Legal Fight May Await." *The New York Times*, February 2, 2016, sec. Technology. https://www.nytimes.com/2016/02/03/technology/us-europe-safe-harbor-data-deal.html.

Seamon, R, and W Gardner. “The Patriot Act and the Wall between Foreign Intelligence and Law Enforcement.” *Harvard Journal of Law & Public Policy* 28, no. 2 (2005): 319–464.

U.S. Senator for Kansas, Jerry Moran. “Sen. Moran Introduces Landmark Federal Data Privacy Legislation.” Accessed April 30, 2020. https://www.moran.senate.gov/public/index.cfm/2020/3/sen-moran-introduces-landmark-federal-data-privacy-legislation.

NPR.org. “Senate Approves USA Freedom Act, Obama Signs It, After Amendments Fail.” Accessed April 12, 2020. https://www.npr.org/sections/thetwo-way/2015/06/02/411534447/senateis-poised-to-vote-on-house-approved-usa-freedom-act.

Seyfried, Pia Philippa. “A European Intelligence Service?” Federal Academy for Security Policy, 2017. JSTOR. https://doi.org/10.2307/resrep22196.

Shackelford, Scott J. *Governing New Frontiers in the Information Age: Toward Cyber Peace*. New York, NY: Cambridge University Press, 2019.

Shaping Europe’s digital future - European Commission. “Shaping Europe’s Digital Future.” Text. Accessed April 30, 2020. https://ec.europa.eu/digital-single-market/en.

Sheffield, Matthew. “Americans Overwhelmingly Want Congress to Restrict Sharing of Personal Data, Poll Finds.” Text. TheHill, December 14, 2018. https://thehill.com/hilltv/what-americas-thinking/421384-opting-out-of-data-sharing-is-what-americans-want-most-from-a.

Sherwood-Randall, Elizabeth. “ALLIANCES AND AMERICAN NATIONAL SECURITY.” Strategic Studies Institute, US Army War College, 2006. JSTOR. www.jstor.org/stable/resrep11189.

Singer, Natasha, Nicole Perlroth, and Aaron Krolik. “Zoom Rushes to Improve Privacy for Consumers Flooding Its Service.” *The New York Times*, April 8, 2020, sec. Business. https://www.nytimes.com/2020/04/08/business/zoom-video-privacy-security-coronavirus.html.

Slaughter, Anne-Marie. “How to Succeed in the Networked World: A Grand Strategy for the Digital Age.” *Foreign Affairs* 95, no. 6 (2016): 76–89.

———. “Leading through Law.” *The Wilson Quarterly (1976-)* 27, no. 4 (2003): 37–44.

———. “The Accountability of Government Networks.” *Indiana Journal of Global Legal Studies* 8, no. 2 (2001): 347–67.

———. *The Chessboard and the Web: Strategies of Connection in a Networked World*. The Henry L. Stimson Lectures Series. New Haven: Yale University Press, 2017.

Sloot, Bart van der. “Privacy from a Legal Perspective.” In *The Handbook of Privacy Studies*, edited by Bart van der Sloot and Aviva de Groot, 63–136. An Interdisciplinary Introduction. Amsterdam University Press, 2018. https://doi.org/10.2307/j.ctvcmxpmp.6.

Smith, John. “About.” Text. European Data Protection Supervisor - European Data Protection Supervisor, November 11, 2016. https://edps.europa.eu/about-edps_en.

———. “About EDPB.” Text. European Data Protection Board - European Data Protection Board, January 10, 2018. https://edpb.europa.eu/about-edpb/about-edpb_en.

Lawfare. “Snowden Revelations,” July 15, 2015. https://www.lawfareblog.com/snowden-revelations.

Solove, Daniel J. “Conceptualizing Privacy.” *Calif. L. Rev.. California Law Review*, no. IR (n.d.). http://lawcat.berkeley.edu/record/1118238.

Solove, Daniel J., and Paul M. Schwartz. *Information Privacy Law*. Fifth edition. Aspen Casebook Series. New York: Wolters Kluwer Law & Business, 2015.

SPIEGEL, Christian Grothoff, Michael Sontheimer, Marcel Rosenbach, Laura Poitras, Andy Müller-Maguhn, DER. "Snowden Documents Indicate NSA Has Breached Deutsche Telekom - DER SPIEGEL - International." Accessed April 12, 2020. https://www.spiegel.de/international/world/snowden-documents-indicate-nsa-has-breached-deutsche-telekom-a-991503.html.

Stang, Gerald. "Global Commons:" European Union Institute for Security Studies (EUISS), 2013. JSTOR. www.jstor.org/stable/resrep06840.

Statt, Nick. "Facebook Says It Will Not Extend GDPR Privacy Protections beyond EU." The Verge, April 3, 2018. https://www.theverge.com/2018/4/3/17194504/facebook-mark-zuckerberg-gdpr-privacy-protections-europe.

Stolton, Samuel. "95,000 Complaints Issued to EU Data Protection Authorities." *Www.Euractiv.Com* (blog), January 28, 2019. https://www.euractiv.com/section/data-protection/news/95000-complaints-issued-to-eu-data-protection-authorities/.

Strahilevitz, Lior Jacob. "Reunifying Privacy Law." *California Law Review* 98, no. 6 (2010): 2007–48.

Suuberg, Alessandra. "The View from the Crossroads: The European Union's New Data Rules and the Future of U.S. Privacy Law." *Tulane Journal of Technology and Intellectual Property* 16 (2013): 267.

Switzer, Stephanie. "THE EUROPEAN INSTITUTIONS." In *European Law Essentials*, 19–34. Edinburgh University Press, 2009. www.jstor.org/stable/10.3366/j.ctt1g09xcb.8.

———. "THE 'MAKING' OF THE EUROPEAN UNION." In *European Law Essentials*, 1–12. Edinburgh University Press, 2009. www.jstor.org/stable/10.3366/j.ctt1g09xcb.6.

Sykes, Alan O. "Regulatory Protectionism and the Law of International Trade." *University of Chicago Law Review* 66, no. 1 (1999).

Taylor, Veronica L. "Regulatory Rule of Law." In *Regulatory Theory*, edited by PETER DRAHOS, 393–414. Foundations and Applications. ANU Press, 2017. www.jstor.org/stable/j.ctt1q1crtm.33.

Terwangne, Cécile de. "The Work of Revision of the Council of Europe Convention 108 for the Protection of Individuals as Regards the Automatic Processing of Personal Data." *International Review of Law, Computers & Technology* 28, no. 2 (May 4, 2014): 118–30. https://doi.org/10.1080/13600869.2013.801588.

"The Age of Digital Interdependence." UN Secretary-General's High-level Panel on Digital Cooperation, June 10, 2019.

"The Application of Commission Decision 520/2000/EC of 26 July 2000 Pursuant to Directive 95/46 of the European Parliament and of the Council on the Adequate Protection of Personal Data Provided by the Safe Harbour Privacy Principles and Related Frequently Asked Questions Issued by the US Department of Commerce." European Commission, February 13, 2002.

"The Court of Justice Declares That the Commission's US Safe Harbour Decision Is Invalid." Luxembourg: Court of Justice of the EU, October 6, 2015.

Bloomberg Law. "The Far-Reaching Implications of the California Consumer Privacy Act (CCPA)." Accessed April 30, 2020. https://pro.bloomberglaw.com/the-far-reaching-implications-of-the-california-consumer-privacy-act-ccpa/.

"The Framework for Global Electronic Commerce." Accessed April 30, 2020. https://clintonwhitehouse4.archives.gov/WH/New/Commerce/.

"The Historical Development of European Integration," n.d., 24.

"The Implementation of Commission Decision 520/2000/EC on the Adequate Protection of Personal Data Provided by the Safe Harbour Privacy Principles and Related Frequently Asked Questions Issued by the US Department of Commerce." Brussels, Belgium: European Commission, October 20, 2004.

Just Security. "The Privacy and Civil Liberties Oversight Board's Disappointing Report on PPD-28 Implementation," October 24, 2018. https://www.justsecurity.org/61199/privacy-civil-liberties-oversight-boards-disappointing-report-ppd-28-implementation/.

"TikTok Said to Be Under National Security Review - The New York Times." Accessed April 30, 2020. https://www.nytimes.com/2019/11/01/technology/tiktok-national-security-review.html.

TITLE 1.81.5. California Consumer Privacy Act of 2018 [1798.100 - 1798.199] (Title 1.81.5 added by Stats. 2018, Ch. 55, Sec. 3.) (n.d.).

European Commission - European Commission. "Types of EU Law." Text. Accessed April 30, 2020. https://ec.europa.eu/info/law/law-making-process/types-eu-law_en.

TechCrunch. "U.S. Government Wants to Step into European Facebook Privacy Legal Challenge." Accessed April 30, 2020. https://social.techcrunch.com/2016/06/13/us-government-wants-to-step-into-european-facebook-privacy-legal-challenge/.

Vermeulen, Gert, and Eva Lievens. *Data Protection and Privacy under Pressure. Transatlantic Tensions, EU Surveillance, and Big Data.* Antwerpen: Maklu, 2018.

VICTOR, JACOB M. "The EU General Data Protection Regulation: Toward a Property Regime for Protecting Data Privacy." *The Yale Law Journal* 123, no. 2 (2013): 513–28.

Vinocur, Nicholas. "How One Country Blocks the World on Data Privacy." POLITICO. Accessed April 29, 2020. https://politi.co/2PqFc42.

Vogel, David. *Trading up: Consumer and Environmental Regulation in a Global Economy*. Cambridge, Mass: Harvard University Press, 1995.

Voigt, Paul, and Axel von dem Bussche. *The EU General Data Protection Regulation (GDPR): A Practical Guide*. Cham, Switzerland: Springer, 2017.

Volokh, Eugene. "TORT LAW VS. PRIVACY." *Columbia Law Review* 114, no. 4 (2014): 879–948.

WARREN, SAMUEL D. BRANDEIS LOUIS D. *RIGHT TO PRIVACY.* Place of publication not identified: OUTLOOK Verlag, 2018.

Warren, Tom. "Zoom Grows to 300 Million Meeting Participants despite Security Backlash." The Verge, April 23, 2020. https://www.theverge.com/2020/4/23/21232401/zoom-300-million-users-growth-coronavirus-pandemic-security-privacy-concerns-response.

The National Law Review. "Washington State Takes The Lead In CCPA Copycat Legislation Race, Trends Emerge." Accessed April 30, 2020. https://www.natlawreview.com/article/washington-state-takes-lead-ccpa-copycat-legislation-race-trends-emerge.

The Daily Wire. "WATCH: Congressman Reveals How Many Data Points Facebook Has On You." Accessed April 22, 2020. https://www.dailywire.com/news/watch-congressman-reveals-how-many-data-points-ryan-saavedra.

Watts, Sean, and Theodore Richard. "BASELINE TERRITORIAL SOVEREIGNTY AND CYBERSPACE." *Lewis & Clark Law Review* 22, no. 3 (September 2018): 771–840.

whitehouse.gov. "We Can't Wait: Obama Administration Unveils Blueprint for a 'Privacy Bill of Rights' to Protect Consumers Online," February 23, 2012.

https://obamawhitehouse.archives.gov/the-press-office/2012/02/23/we-can-t-wait-obama-administration-unveils-blueprint-privacy-bill-rights.
Weber, Rolf H., Mirina Grosz, and Romana Weber. *Shaping Internet Governance: Regulatory Challenges*. Licence ed. Publikationen Aus Dem Zentrum Für Informations- Und Kommunikationsrecht Der Universität Zürich 46. Heidelberg: Springer, 2009.
Weiss, Martin, and Kristin Archick. "U.S.-EU Data Privacy: From Safe Harbor to Privacy Shield." Congressional Research Service, May 19, 2016.
Westin, Alan F. "Science, Privacy, and Freedom: Issues and Proposals for the 1970's. Part I--The Current Impact of Surveillance on Privacy." *Columbia Law Review* 66, no. 6 (1966): 1003–50. https://doi.org/10.2307/1120997.
"What Is the USA Patriot Web." Accessed April 30, 2020. https://www.justice.gov/archive/ll/highlights.htm.
European Commission - European Commission. "What Rules Apply If My Organisation Transfers Data Outside the EU?" Text. Accessed April 13, 2020. https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/what-rules-apply-if-my-organisation-transfers-data-outside-eu_en.
"White House Unveils E-Commerce Plans." Accessed April 30, 2020. https://archive.nytimes.com/www.nytimes.com/library/tech/98/11/cyber/articles/30magaziner.html.
Wilson, Ernest J. "Hard Power, Soft Power, Smart Power." *The Annals of the American Academy of Political and Social Science* 616 (2008): 110–24.
Wolf, Christopher. "Delusions of Adequacy? Examining the Case for Finding the United States Adequate for Cross-Border EU-U.S. Data Transfers." *Washington University Journal of Law and Policy* 43, no. 1 (2014): 227–58.
Wolff, Michael F. "Chase Moore's Law, Inventors Urged." *Research Technology Management* 47, no. 1 (2004): 6–6.
Wong, Julia Carrie. "The FBI and Apple Are Facing off over an IPhone Again. What's Going On?" *The Guardian*, January 15, 2020, sec. US news. https://www.theguardian.com/us-news/2020/jan/14/fbi-apple-faceoff-iphone-florida-shooting.
Wright, David, and Reinhard Kreiss. "European Response to Snowden: A Discussion Paper." Increasing Resilience in Surveillance Societies, December 2013. http://irissproject.eu/wp-content/uploads/2013/12/IRISS_European-responses-to-the-Snowden-revelations_18-Dec-2013_Final.pdf.
Young, Alasdair R. "The European Union as a Global Regulator? Context and Comparison." *Journal of European Public Policy* 22, no. 9 (October 21, 2015): 1233–52. https://doi.org/10.1080/13501763.2015.1046902.
"Zoom Goes From Conferencing App to the Pandemic's Social Network." *Bloomberg.Com*, April 9, 2020. https://www.bloomberg.com/news/features/2020-04-09/zoom-goes-from-conferencing-app-to-the-pandemic-s-social-network.
Zuboff, Shoshana. *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. First Trade Paperback Edition. New York: PublicAffairs, 2020.