

Cost-Based California Effects

Jens Frankenreiter[†]

The “California Effect” is a recurring trope in discussions about regulatory interdependence. This effect predicts that businesses active in multiple jurisdictions sometimes adopt the strictest regulatory standards that they face in any jurisdiction globally, even if the jurisdiction’s law does not require global compliance. As the argument goes, California Effects often occur because firms find it less expensive to comply with the most stringent standard everywhere than to provide different products to consumers in different jurisdictions based on the relevant local standards. There is a substantial literature that assumes the existence of such Cost-Based California Effects both at the interstate level in the United States and the international level, where they often appear in connection with the EU’s regulatory activities under the moniker “Brussels Effect.” However, empirical evidence documenting these effects’ existence and strength is scarce.

This Article makes two contributions. On a theoretical level, it argues that Cost-Based California Effects should be treated separately from other forms of cross-jurisdictional influence, as their normative implications differ. On an empirical level, it reports results from a case study investigating the existence of these effects in data privacy law, a field in which they have been said to be particularly influential. The analysis tracks changes in almost 700 webpages’ privacy policies in order to reveal the extent to which EU law (which is usually described as comparably stringent) influences transactions between U.S. online services and consumers. The analysis covers two years starting in November 2017, a period that saw the enactment of a new, sweeping data privacy law in the EU. Contrary to what many assume, the analysis reveals that most U.S. online services treat U.S. consumers and EU consumers differently, with EU consumers enjoying higher levels of protection. This result indicates that the

[†] Visiting Professor, Washington University in St. Louis School of Law. Email: fjens@wustl.edu. I am grateful to participants in the 2021 Annual Meeting of the American Law and Economics Association, the 2022 Conference on Empirical Legal Studies, the 25th Annual ISNIE / SIOE Conference, the 5th Penn-NYU Empirical Contracts Workshop, the Florida-Michigan-Virginia Virtual Law and Economics Workshop, and audience members at UC Berkeley, the University of Chicago, Columbia, ETH Zurich, the Leibniz Institute for Financial Research SAFE, Oxford, the University of Southern California, the University of Toronto, the University of Utah, the University of Virginia, Washington University in St. Louis, and Yale for helpful comments. Particular thanks to Elliott Ash, Jack Balkin, Stefan Bechtold, Omri Ben-Shahar, Bo Bian, Anu Bradford, Ryan Bubb, Meirav Furth-Matzkin, Yoan Hermstrüwer, Cathy Hwang, Nicolas Jabko, Dan Klerman, Mike Livermore, Florencia Marotta-Wurgler, Ruth Mason, Jonathan Masur, Justin McCrary, Tom Nachbar, Anthony Niblett, Julian Nyarko, Sonja Starr, Paul Stephan, Lior Strahilevitz, Eric Talley, Tobias Tröger, Pierre-Hugues Verdier, Mila Versteeg, and Tim Wu. All errors and omissions are solely mine.

impact of EU law on the operations of U.S. online services is limited. Moreover, it suggests that Cost-Based California Effects might be less important than is commonly assumed, at least in data privacy law.

Introduction	1158
I. California and Brussels Effects	1164
A. Cost-Based California Effects	1166
1. Characteristics of Cost-Based California Effects	1166
a. Activities Subject to the Laws of Multiple Jurisdictions	1167
b. Divergent Regulatory Standards	1168
c. Costs of Differentiation and Global Compliance	1169
2. When Do Cost-Based California Effects Occur?.....	1169
3. Distributional and Normative Implications	1171
B. Other Forms of Cross-Jurisdictional Influence	1171
1. Voluntary Compliance	1171
2. Diffusion of Laws	1172
C. Cost-Based California Effects and the Internet	1173
II. Consumer Privacy Law in the United States and in the EU	1174
A. The United States's Market-Based Approach	1175
B. Omnibus Regulation in the EU.....	1176
C. The GDPR's Legal Scope	1177
III. Cost-Based California Effects in Data Privacy Law?	1178
A. General Considerations	1178
B. Existing Empirical Evidence	1180
IV. Empirical Analysis.....	1181
A. Research Design	1182
1. Measuring Changes to Privacy Policies.....	1182
2. Leveraging Variation Over Time.....	1184
3. Illustrations	1184
4. Research Questions.....	1186
B. Data.....	1186
C. Analysis and Results.....	1188
1. Computational Analysis.....	1188
a. Outcome Measures	1188
b. Results	1189
i. The Development of U.S. Privacy Policies	1189
ii. A Quantitative Test of Global Compliance	1194
2. Manual Coding.....	1196
a. Sample Selection and Coding Scheme	1197
b. Results	1198
i. The Legal Significance of Privacy Policy Changes	1198
ii. Protection Levels.....	1199
3. Determinants of Global Compliance	1205

4. Other Potential Explanations	1208
D. Interpretation and Limitations	1209
V. Implications	1210
A. Implications for Data Privacy Law	1210
1. Normative Implications	1210
2. Policy Implications	1214
3. The Role of the EU	1215
B. Implications for Regulatory Interdependence	1215
Conclusion	1216

Introduction

In the spring of 2018, Google, Facebook, and several other leading tech companies announced major changes to their handling of consumer data.¹ These changes were supposed to bring their data practices in line with the General Data Protection Regulation (GDPR),² a new data privacy law in the European Union (EU).³ Yet in practice, the revised policies applied to consumers everywhere, including in the United States.⁴

This global adoption of purportedly GDPR-compliant privacy policies by U.S. online services might seem startling. Compared to the GDPR, data privacy law in the United States generally imposes much less onerous obligations on online services,⁵ and it seems far from clear whether the United States will adopt comprehensive privacy legislation anytime soon. The GDPR itself does not legally apply to interactions between U.S. businesses and U.S. consumers.⁶ Besides, compliance with the GDPR's various requirements is usually considered to be costly.⁷ Why, then, would Google and Facebook decide to extend these expansive protections to consumers in the United States?

Yet the global nature of the changes did not surprise most commentators. Some had for years predicted that stringent data privacy standards could spread between jurisdictions as a result of "California" or "Brussels Effects"—a hypothesized process in which influential jurisdictions cause universal adoption of their comparably stringent regulatory standards through unilateral policymaking.⁸ Proponents of this theory view the reactions by Google,

1. Press Release, Facebook, Complying With New Privacy Laws and Offering New Privacy Protections to Everyone, No Matter Where You Live (Apr. 17, 2018), <https://about.fb.com/news/2018/04/new-privacy-protections> [<https://perma.cc/YP4A-54W3>]; Press Release, Google, Our Preparations for Europe's New Data Protection Law, (May 11, 2018), <https://blog.google/outreach-initiatives/public-policy/our-preparations-europes-new-data-protection-law> [<https://perma.cc/NP6H-9QZH>].

2. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. (L 119) 1 [hereinafter GDPR].

3. See Katie Collins, *Google Makes Privacy Policy Clearer Than Ever to Comply with EU Law*, CNET (May 11, 2018, 5:00 AM PT), <https://www.cnet.com/news/google-makes-privacy-policy-clearer-than-ever-to-comply-with-eu-gdpr-law> [<https://perma.cc/E9ZV-BSNS>].

4. Press Release, Facebook, *supra* note 1; see Michael L. Rustad & Thomas H. Koenig, *Towards a Global Data Privacy Standard*, 71 FLA. L. REV. 365, 391-94 (2019).

5. See *infra* notes 77-103 and accompanying text.

6. See *infra* notes 104-106 and accompanying text.

7. See, e.g., Oliver Smith, *The GDPR Racket: Who's Making Money from This \$9bn Business Shakedown*, FORBES (May 2, 2018, 2:30 AM ET), <https://www.forbes.com/sites/oliversmith/2018/05/02/the-gdpr-racket-whos-making-money-from-this-9bn-business-shakedown> [<https://perma.cc/XBW7-GKD5>].

8. See, e.g., Anu Bradford, *The Brussels Effect*, 107 NW. U. L. REV. 1 (2012); JACK GOLDSMITH & TIM WU, *WHO CONTROLS THE INTERNET? ILLUSIONS OF A BORDERLESS WORLD* 176 (2006).

The use of the term "California Effect" in the literature is somewhat inconsistent. Parts of the literature use it to describe the more general idea that transjurisdictional activity might help spread higher regulatory standards beyond the jurisdiction that initially enacted them. For example, consider David Vogel's book *Trading Up*, which is commonly credited with coining the term "California Effect." Vogel

Facebook, and their ilk as evidence that it is often costly for online services to treat consumers in different jurisdictions differently. Hence, the global adoption of stringent standards imposed by one jurisdiction is seen as a cost-efficient—and rational—reaction for trans-jurisdictional businesses.⁹

The implications of this theory are momentous and reach far beyond data privacy law. In an increasingly interconnected world, we have become used to the fact that business regulation is a global enterprise: many businesses' activities span the globe, and national policymakers' decisions affect outcomes far beyond the borders of their home jurisdiction. Yet the consequences of California/Brussels Effects of the type described above differ from—and are arguably more drastic than—those of other forms of regulatory interdependence. The existence of the former in data privacy law would imply that high-standard jurisdictions like the EU can unilaterally force their regulatory standards on online transactions in other jurisdictions. Consequently, the ability of U.S. policymakers to adopt alternative approaches in regulating transactions between U.S. businesses and their U.S. customers would be severely limited.

This Article challenges the view that California/Brussels Effects driven by costs of differentiation are widespread in data privacy law. It uses a novel dataset of privacy policies and a range of empirical techniques to investigate EU law's influence on U.S. firms' data practices on a larger scale than most existing studies. The analysis shows that the GDPR prompted only few U.S. firms to adopt GDPR-compliant data practices globally. Its results also suggest that existing California/Brussels Effects in data privacy law are not, as many argue, driven by the costs of treating consumers in different jurisdictions differently. Instead, the evidence points to other mechanisms—some of which have so far been largely ignored in the literature—as the main drivers of some companies' decisions to extend GDPR-style privacy protections to consumers in the United States. Consequently, this Article also casts doubt on claims about the power of the EU—or, for that matter, any other jurisdiction—to unilaterally impose rules on online transactions in the United States.

* * *

does not suggest that California's rules prompted car manufacturers with sales in California to change the design of cars sold in other parts of the U.S. even in the absence of similar regulations there. Instead, he describes how higher regulatory standards in some jurisdictions incentivized transjurisdictional actors to lobby for the introduction of similar rules in other jurisdictions, tilting the political landscape in favor of more regulation. DAVID VOGEL, *TRADING UP: CONSUMER AND ENVIRONMENTAL REGULATION IN A GLOBAL ECONOMY* 24, 68-70 (1995).

9. See, e.g., ANU BRADFORD, *THE BRUSSELS EFFECT: HOW THE EUROPEAN UNION RULES THE WORLD* 142-43 (2020); Rustad & Koenig, *supra* note 4, at 391; Nitasha Tiku, *Europe's New Privacy Law Will Change the Web, and More*, WIRED (Mar. 19, 2018, 6:00 AM), <https://www.wired.com/story/europes-new-privacy-law-will-change-the-web-and-more> [<https://perma.cc/26G3-3D6P>].

There are myriad ways in which transactions and the outcomes of legal disputes are influenced by the laws of other jurisdictions.¹⁰ This reality places important constraints on the power of countries and subnational jurisdictions to order their internal affairs. Regulatory interdependence has long been recognized at both the domestic and international levels.¹¹ Domestically, these effects justify the federalization of certain areas of law.¹² Globally, regulatory interdependence is reflected in international trade law,¹³ networks of global banking regulators,¹⁴ and agreements concerning international tax reporting.¹⁵ In recent years, discussions about regulatory interdependence have taken on a new dimension in the United States as the emergence of other influential jurisdictions, most notably the European Union, has challenged the U.S.'s role as the primary exporter of legal rules.¹⁶

California Effects are a recurring trope in discussions about regulatory interdependence. The hypothesis is that businesses active in multiple jurisdictions will sometimes adopt the strictest standards they face in any jurisdiction, even if the law does not mandate global compliance.¹⁷ A common explanation for this effect points to the costs of treating consumers in different jurisdictions differently. As the argument goes, California Effects often occur because firms find it less expensive to comply with the most stringent standard everywhere than to provide different products to consumers in different

10. In U.S. corporate law, scholars have for decades discussed whether permissive venue rules have led to an erosion of shareholder protections or instead, the emergence of more efficient corporate law. See, e.g., William L. Cary, *Federalism and Corporate Law: Reflections Upon Delaware*, 83 YALE L.J. 663 (1974); Roberta Romano, *The State Competition Debate in Corporate Law*, 8 CARDOZO L. REV. 709 (1987); Ralph K. Winter, *State Law, Shareholder Protection, and the Theory of the Corporation*, 6 J. LEGAL STUD. 251 (1977). In environmental law, scholars have argued that emission standards set by Californian law have influenced not only the design of cars sold in all of the United States but in other nations as well. See VOGEL, *supra* note 8, at 68-70. In all these situations, regulatory actions in one jurisdiction shape conduct in other jurisdictions. At the same time, such actions also impair the effectiveness of other jurisdictions' rules and their power to pursue their regulatory goals. See Jack L. Goldsmith, *Against Cyberanarchy*, 65 U. CHI. L. REV. 1199, 1212 (1998).

11. David Lazer, *Regulatory Interdependence and International Governance*, 8 J. EUR. PUB. POL'Y 474 (2001).

12. In environmental law, Congress cited the effects of regulatory interdependence (more precisely, the potential for detrimental competition between states) as a motivation to enact various statutes in this area. See Richard L. Revesz, *Rehabilitating Interstate Competition: Rethinking the "Race-to-the-Bottom" Rationale for Federal Environmental Regulation*, 67 N.Y.U. L. REV. 1210, 1226-27 (1992). Considerations about harmful state competition also played a role in the enactment of New Deal legislation and were cited by the Supreme Court in cases upholding such legislation. See *United States v. Darby*, 312 U.S. 100, 115 (1941); Cass R. Sunstein, *Constitutionalism After the New Deal*, 101 HARV. L. REV. 421, 504-05 (1987). In corporate law, concerns about regulatory interdependence motivated similar calls for federalization. See Cary, *supra* note 10; Lucien Arye Bebbchuk, *Federalism and the Corporation: The Desirable Limits on State Competition in Corporate Law*, 105 HARV. L. REV. 1501 (1992).

13. See, e.g., Agreement on the Application of Sanitary and Phytosanitary Measures, Apr. 15, 1994, 1867 U.N.T.S. 493.

14. See Basel Comm. on Banking Supervision, *The Basel Framework*, BANK FOR INT'L SETTLEMENTS (2020), <https://www.bis.org/publ/bcbs189.pdf> [<https://perma.cc/9FGW-WYR2>].

15. See, e.g., Agreement on Foreign Account Tax Compliance, U.S.-Canada, Feb. 5, 2014, T.I.A.S. No. 14,627.

16. See generally BRADFORD, *supra* note 9 (describing the EU's global influence).

17. See *supra* note 8 and accompanying text.

jurisdictions based on the relevant local standards.¹⁸ In her seminal work on the Brussels Effect, Professor Anu Bradford identifies this mechanism as one of the main pathways through which the EU exerts influence globally.¹⁹ This version of California/Brussels Effects, which I refer to as “Cost-Based California Effects” (CBCEs), is the main focus of this Article.

This Article makes two contributions to discussions about California/Brussels Effects and regulatory interdependence. On a theoretical level, it argues that CBCEs should be treated differently from other forms of cross-jurisdictional influence. Costs of differentiation are far from the only reason why firms opt for global compliance with stringent regulatory standards. For example, firms might also do so to appeal to consumers in other jurisdictions who are willing to pay higher prices for high-quality products or to engage in virtue signaling. However, while most observers treat these different forms of California/Brussels Effect interchangeably,²⁰ the mechanisms giving rise to these effects matter.

Most importantly, CBCEs have different normative implications than other versions of the California/Brussels Effect and other forms of cross-jurisdictional influence. In the presence of CBCEs, transjurisdictional businesses comply with the most stringent standards globally even if—viewed in isolation—both businesses and consumers would profit from the application of local standards in low-protection jurisdictions.²¹ Similar concerns do not arise if the global compliance with the rules of one jurisdiction is motivated by businesses’ belief that they will profit from selling high-quality products in other jurisdictions.²² Consequently, a full assessment of the consequences and implications of California/Brussels Effects requires differentiating between different versions of this phenomenon.

The Article’s second, and main, contribution is empirical in nature. Although there is a substantial literature that assumes the existence of California/Brussels effects, relatively little work has been done to examine whether they are a widespread phenomenon. Most of the evidence that has been cited in support of their existence is anecdotal.²³ Systematic empirical studies are mostly absent from the literature. Also, little work has been done to distinguish the different mechanisms through which the laws of one jurisdiction affect outcomes elsewhere.

This Article contributes to our understanding of California and Brussels Effects by presenting results from a case study of recent developments in data privacy law. With many online services catering to customers in a multitude of

18. See, e.g., GOLDSMITH & WU, *supra* note 8, at 176.

19. BRADFORD, *supra* note 9, at 142; see Bradford, *supra* note 8.

20. See, e.g., BRADFORD, *supra* note 9, at 142-44 (describing how “de-facto Brussels Effects” can either be brought about by costs of differentiation or by consumer demand).

21. See *infra* Sections I.A.3 and V.A.

22. See *infra* Section I.B.1.

23. See, e.g., BRADFORD, *supra* note 9, at 143-46, 161-67; Rustad & Koenig, *supra* note 4, at 391-96.

jurisdictions simultaneously, data privacy law has been hypothesized to be an area where CBCEs are widespread.²⁴ The EU's adoption of the GDPR raises the question of whether the resulting new legal requirements prompted only a few very prominent U.S. companies like Google and Facebook to change their data practices, or whether these changes were more widespread.

Because it is often impossible to observe the data practices of businesses directly,²⁵ this Article employs an empirical strategy that measures changes in publicly available websites' privacy policies. The analysis relies on a longitudinal dataset consisting of the texts of the privacy policies of 693 websites.²⁶ The dataset contains one observation per week for the period between late November 2017 and October 2019. The analysis furthermore relies on a range of quantitative tools, including text analysis and machine learning.²⁷ Additionally, I conducted a series of informal interviews with privacy professionals to contextualize my findings.

The results of this analysis suggest, first, that the impact of EU data privacy law on the relationship between U.S. businesses and their U.S. customers might be more limited than is commonly assumed. While the analysis confirms findings in other studies that a large share of U.S. online services changed their privacy policies in the wake of the GDPR,²⁸ it also demonstrates that only a (small) minority of these services adopted GDPR-compliant data policies globally.²⁹ Instead, most companies that modified their policies to bring them in line with GDPR's requirements took active steps to limit the scope of at least some of the additional protections to consumers in the EU.³⁰ Second, the evidence presented in this Article raises serious doubts about the hypothesis that differentiation costs played a major role in some businesses' decisions to roll out GDPR-style protections on a global basis.³¹

This Article's findings speak to a range of different literatures, including the literatures on data privacy law, consumer contracts, and regulatory interdependence. With regard to data privacy law, this Article challenges the common notion that CBCEs are a widespread phenomenon. Over the past several years, California/Brussels Effects have become an important topic in the global discourse on data privacy.³² One reason for this interest is that the United States and the EU have pursued radically different regulatory approaches. In the United

24. See *infra* Section III.A.

25. But see Christian Peukert, Stefan Bechtold, Michail Batikas & Tobias Kretschmer, *Regulatory Spillovers and Data Governance: Evidence from the GDPR*, *MARKETING SCI.* (forthcoming), <https://ssrn.com/abstract=3560392> [<https://perma.cc/9CKG-Q2H7>] (measuring changes in websites' use of third-party services).

26. The dataset builds on data assembled for another project. See Jens Frankenreiter & Yoan Hermstrüwer, *Privacy's Great Shock: The GDPR and Privacy Policies Around the Globe* (Dec. 8, 2020) (unpublished manuscript) (on file with author).

27. *Infra* Section IV.C.1.a.

28. *Infra* Section IV.C.1.b.i.

29. *Infra* Section IV.C.1.b.ii.

30. *Infra* Section IV.C.2.b.

31. *Infra* Section IV.C.3.

32. See *infra* Section III.A.

States, the scope of consumer privacy protections is largely a matter of contracting.³³ By contrast, particularly since the entry into force of the GDPR in 2018, the EU imposes strict limits on the gathering and processing of personal data.³⁴ Therefore, data privacy law is an area where the presence or absence of CBCEs would lead to quite different policy outcomes. Against this background, the empirical analysis contextualizes the true reach of EU data privacy law. Its results suggest that, if widescale changes in data privacy practices in the United States are warranted, they will likely only come about due to domestic economic and political forces, not actions in other jurisdictions.

A related discussion in data privacy law concerns the role that regulation at the state level can play in protecting consumers' interests across the United States.³⁵ In this context, there was a widespread expectation that California's new data privacy law, the California Consumer Privacy Act (CCPA)³⁶ would have nationwide effects.³⁷ Like predictions about the extraterritorial effects of EU law, these expectations were primarily based on the assumption that it would be too costly for businesses to differentiate among consumers in different states. The results in this Article cast doubt on this assumption.³⁸

With regard to consumer contracts, the analysis suggests that it is often technically feasible and economically viable for online services to tailor their products to individual jurisdictions' regulatory standards. At the same time, this Article also documents how, even in the absence of CBCEs, some companies might still decide to extend stringent standards to consumers in different jurisdictions. Potential explanations for this effect include businesses' desire to create positive public-relations effects or establish themselves as brands that offer high standards of privacy protection.

With regard to the literature on regulatory interdependence, this Article provides one of the first systematic quantitative investigations of California and Brussels Effects in an area in which their existence is often treated as a given. Its findings imply that CBCEs play a much smaller role than is often assumed in the literature. This result reminds us that, even in an age of incessant globalization, it is too early to declare national governance of business activities a relic of a bygone era. Nations remain the primary locus for politics and policymaking, and national borders have significant consequences for the flow of labor, capital, and

33. See *infra* Section II.A.

34. See *infra* Section II.B.

35. See BRADFORD, *supra* note 9, at 146.

36. CAL. CIV. CODE § 1798.100 (West 2020).

37. See, e.g., *Don't Sell My Data! We Finally Have a Law for That*, WASH. POST (Feb. 12, 2020), <https://www.washingtonpost.com/technology/2020/02/06/ccpa-faq> [<https://perma.cc/JVE3-UKTD>]; Aaron Holmes, *Here's Why Facebook, Google, and Every Other Major Tech Company Are Updating Their Privacy Policy in Time for 2020, and What It Means for You*, BUS. INSIDER (Jan. 10, 2020, 8:55 AM), <https://www.businessinsider.com/why-tech-companies-new-privacy-policy-2020-california-2019-12> [<https://perma.cc/W9KJ-PCK7>]; Kashmir Hill, *Want Your Personal Data? Hand Over More Please*, N.Y. TIMES (Oct. 27, 2021), <https://www.nytimes.com/2020/01/15/technology/data-privacy-law-access.html> [<https://perma.cc/9Z48-JHYQ>].

38. Note, however, that it could be easier for businesses to differentiate among consumers in different countries than it is for them to differentiate among consumers in different states.

goods. A more accurate model of business regulation in the contemporary world recognizes that nations can be deeply embedded in a global context while retaining important areas of autonomy in which global influences are constrained.

The remainder of this Article is structured as follows. Part I describes different versions of California/Brussels Effects in more detail and discusses their respective normative implications. Part II provides an overview of the state of data privacy law in the EU and the United States, while Part III summarizes the state of the debate about CBCEs in this area. Part IV offers the main contribution of this Article: an empirical analysis of the conditions under which U.S. online services adjust their privacy policies to the requirements of EU law. Part V discusses the implications of the findings, followed by a brief conclusion.

I. California and Brussels Effects

When California sets new emissions standards for cars, General Motors will build cars to the Californian standard for the entire United States. Its choice to do so depends, of course, on the fact that it is more expensive to create cars customized for California than just build one car for the entire country.

– Jack Goldsmith and Tim Wu³⁹

The exporter has an incentive to adopt a global standard whenever its production or conduct is nondivisible across different markets or when the benefits of a uniform standard due to scale economies exceed the costs of forgoing lower production costs in less regulated markets. Complying with just one regulatory standard allows a corporation to maintain a single production process, which is less costly than tailoring its production to meet divergent regulatory standards. A single standard also facilitates the preservation of a uniform global brand. Thus, unilateral regulatory globalization follows from the nondivisibility of a corporation's production or conduct.

– Anu Bradford⁴⁰

California Effects are a recurring idea in discussions about regulatory interdependence and the regulation of transjurisdictional business activities. As Professors Jack Goldsmith and Tim Wu imply, this idea is often associated with California's role in promoting higher automobile emission standards across the United States.⁴¹ In recent decades, California's laws have often required cars sold in this state to comply with higher emission standards than those set by other U.S. states and the federal government. A common assumption in the literature is that, in response to the introduction of stringent standards in California, carmakers started selling low-emission cars in all of the United States.

In recent years, similar effects have increasingly been described in connection with the EU's regulatory activities. As the story goes, there are many

39. GOLDSMITH & WU, *supra* note 8, at 176.

40. Bradford, *supra* note 8, at 17-18 (footnotes omitted).

41. GOLDSMITH & WU, *supra* note 8, at 176.

regulatory areas in which the EU promulgates more stringent standards than those that apply elsewhere, including in the United States. Major global businesses operating in the EU have to apply these standards in their interactions with consumers there.⁴² With regard to consumers outside of the EU, they face a choice. Businesses can either treat non-EU consumers differently from EU consumers or apply the EU's standards to all. Observers assume that it is often beneficial for businesses to opt for the latter option, resulting in global compliance with the EU's standards. Areas in which California Effects are said to result in a global application of EU law include food safety,⁴³ chemical safety,⁴⁴ environmental law,⁴⁵ online hate speech restrictions,⁴⁶ and data privacy law.⁴⁷

Importantly, many observers assume that the most important driver of these effects is the cost of treating consumers in different jurisdictions differently. This is true in the context of car-emission standards, where many ascribe the extrajurisdictional reach of California's laws to the costs of building two different versions of each car model (one compliant with California law, the other with the law applicable in other states) at the same time.⁴⁸ Work by Bradford and others suggests that this is also true for the EU's regulatory activities.⁴⁹

However, the costs of differentiating between consumers in different jurisdictions are just one of a range of mechanisms by which stringent standards in one jurisdiction can affect outcomes elsewhere. While many in the literature treat California/Brussels Effects caused by different mechanisms interchangeably, their normative implications and consequences for the reality of regulatory interdependence differ substantially. Therefore, this Article distinguishes between what I call Cost-Based California Effects (CBCEs) and other forms of cross-jurisdictional influence.

42. In some areas, EU law requires businesses active in the EU to structure their global operations in accordance with EU law. Perhaps the most important example is antitrust law. For example, mergers and acquisitions involving major business organizations are often subject to antitrust approval in the EU (as well as in other jurisdictions in which at least two of the entities are active) irrespective of where the businesses are headquartered. *See* Council Regulation 139/2004 (2004), art. 1, 2004 O.J. (L 24) 1, 6 (EC). The reason is that the effects of a merger of two businesses based in one jurisdiction will often not be limited to this jurisdiction and thus affect operations elsewhere. At the same time, the scope of laws in many other areas is more limited. For example, in consumer law, EU law usually does not apply if neither the consumer nor the business is based in the EU.

43. *See* Bradford, *supra* note 8, at 179-87.

44. *See id.* at 196-99.

45. *See id.* at 213-21.

46. *See id.* at 160-67.

47. *See id.* at 142-47.

48. *See, e.g.*, GOLDSMITH & WU, *supra* note 8, at 176; *see also* BRADFORD, *supra* note 9, at 64-65 (discussing general conditions for the presence and strength of California Effects in the EU context).

49. BRADFORD, *supra* note 9, at 179-87; *see* Bradford, *supra* note 8, at 17-18; GOLDSMITH & WU, *supra* note 8, at 176; Gregory Shaffer, *Globalization and Social Protection: The Impact of EU and International Rules in the Ratcheting Up of U.S. Privacy Standards*, 25 YALE J. INT'L. L. 1, 78 (2000).

A. Cost-Based California Effects

1. Characteristics of Cost-Based California Effects

I define CBCEs as situations in which the costs of differentiation based on regulatory standards compel transjurisdictional actors to comply with the most stringent standard they face in any jurisdiction globally.

To illustrate this concept, consider the following example: Widget Inc. (*W*) is the only manufacturer of widgets in its home jurisdiction Columbiana and neighboring East Atlantica. Widgets are traditionally made from a plastic compound that some consider to be a health hazard for consumers. Alternatively, widgets can be made from steel, rendering them harmless to health. However, steel widgets are more expensive to manufacture, and they have no other advantages over plastic widgets. To protect its consumers, East Atlantica adopts a law that requires that all widgets sold in East Atlantica are made from steel. Similar legislative initiatives are unsuccessful in Columbiana, where consumers are also unwilling to pay more for steel widgets.

In situations like this, how will *W* respond? The most straightforward response is likely to start manufacturing steel widgets for its customers in East Atlantica while continuing to market plastic widgets to customers in Columbiana. It is also possible that the increased production costs associated with manufacturing steel widgets make it unprofitable to continue serving consumers in East Atlantica. If so, *W* will cease its activities there.

However, there are situations in which *W*'s best response is to offer steel widgets to consumers in both East Atlantica and Columbiana, even though plastic widgets are still legal in Columbiana. This situation can occur if technical or economic reasons make it costly for *W* to market different types of widgets simultaneously. For example, the production costs of all widgets could increase if *W* had to configure its factory to manufacture both plastic and steel widgets. A decision by *W* to shift its global production to steel widgets in order to avoid the costs of differentiation is an example of a CBCE. The definition of CBCEs can be broken down into three elements: First, a business or similar actor is involved in transactions subject to the laws of different jurisdictions. Second, some jurisdictions impose more stringent standards on transactions than others. Third, differentiation costs make it rational for the transjurisdictional actor to apply the same standard to every transaction irrespective of jurisdiction.⁵⁰ In the following Sections, I describe each of these requirements in more detail.

50. In her work on the Brussels effect, Bradford identifies five conditions that have to be met for the EU to exert global power through unilateral regulation: market size, regulatory capacity, stringent standards, inelastic targets, and nondivisibility of standards. BRADFORD, *supra* note 9, at 25. While there might be differences on the margin, this description and my definition of CBCEs largely overlap.

a. Activities Subject to the Laws of Multiple Jurisdictions

CBCEs occur in situations in which more than one jurisdiction can set up and enforce binding rules for (at least some of) a transjurisdictional actor's activities.⁵¹ This requirement is ordinarily met whenever an actor is active in more than one jurisdiction, as jurisdictions are entitled to regulate conduct when it takes place in or affects their territory.⁵² For example, if a business sells goods or services in different jurisdictions, every one of these jurisdictions can usually determine the rules that apply to transactions in their territory. CBCEs ordinarily do not occur in situations where a business is active in only one jurisdiction.

However, there are situations in which jurisdictions are not in a position to effectively regulate conduct taking place or affecting outcomes in their territory. Most importantly, some legal areas have rules that restrict the power of jurisdictions to regulate transjurisdictional actors.⁵³ These situations might result

51. It is not required that all jurisdictions that have the power to regulate exercise this power. For example, in the example above, Columbiana does not impose any limitations on the sale of widgets. Still, *W*'s activities fall under the scope of both Columbiana and East Atlantica's laws, as both jurisdictions could regulate (at least) transactions between *W* and consumers in their respective jurisdictions.

52. See RESTATEMENT (FOURTH) OF THE FOREIGN RELATIONS LAW OF THE UNITED STATES, § 407 (AM. L. INST. 2018) (defining the "specific connection" necessary to exercise jurisdiction).

53. Rules restricting the regulatory reach of jurisdictions are often adopted to save businesses the costs of having to deal with multiple regulatory environments at the same time. In order to achieve this goal, the power to regulate transactions of a transjurisdictional actor is concentrated with one jurisdiction, usually the actor's home jurisdiction.

In principle, such rules can either be rules of the jurisdiction itself or rules adopted at a higher level. Examples of the first type of rules are rules on personal jurisdiction and conflict-of-law such as the internal affairs doctrine in corporate law. See P. John Kozyris, *Corporate Wars and Choice of Law*, 1985 DUKE L.J. 1, 3-4. At least in principle, however, such rules can be changed to extend the reach of a jurisdiction's laws. Cf. Harold W. Horowitz, Comment, *The Commerce Clause as a Limitation on State Choice-of-Law Doctrine*, 84 HARV. L. REV. 806, 807 (1971) (describing implicit Commerce Clause limitations in the multistate context). There are numerous examples of the second type of rule at the interstate level in the United States, where federal law imposes important limitations on the power of states to regulate transjurisdictional conduct. For example, the National Banking Act bars states from regulating certain aspects of credit agreements between their citizens and banks incorporated elsewhere. See *Marquette Nat'l Bank of Minneapolis v. First of Omaha Serv. Corp.*, 439 U.S. 299, 313-19 (1978). Besides federal legislation, such limits can flow from the Fourteenth Amendment's Due Process Clause and the (Dormant) Commerce Clause. See *Int'l Shoe Co. v. Washington*, 326 U.S. 310, 316 (1945); *Pike v. Bruce Church, Inc.*, 397 U.S. 137, 146 (1970) (laying out the test for Commerce Clause-based invalidation of state regulations). At the international level, international law can impose (although usually comparably weak) limits on regulation. See Goldsmith, *supra* note 10, at 1219. Limits applying to states worldwide can flow from customary international law and international treaties, such as the General Agreement on Tariffs and Trade and other trade law instruments. See RESTATEMENT (FOURTH) OF THE FOREIGN RELATIONS LAW OF THE UNITED STATES, § 407 (AM. L. INST. 2018); see also Appellate Body Report, *United States—Measures Affecting the Cross-Border Supply of Gambling and Betting Services*, WTO Doc. WT/DS285/AB/R (adopted Apr. 20, 2005) (finding that the United States violated international trade law in prohibiting providers of online gambling services based in Antigua from offering their services over the internet to customers based in the United States).

in other forms of jurisdictional interdependence,⁵⁴ but they usually do not give rise to CBCEs.⁵⁵

While CBCEs require that a transjurisdictional actor is subject to the regulatory authority of more than one jurisdiction, this does not imply that individual transactions need to fall under the legal scope of multiple laws at the same time. Instead, CBCEs are characterized by “excessive” compliance with the laws that impose the strictest standards on certain types of transactions: technical or economic factors rather than legal obligations compel a business or similar actor to apply stringent standards in its global operations, including in situations in which the law does not require compliance.

b. Divergent Regulatory Standards

Furthermore, CBCEs require that some jurisdictions impose more stringent standards on a certain type of transaction than others—or in other words, that the standards imposed by various jurisdictions diverge.⁵⁶ The standards of jurisdictions diverge whenever there are transactions that are legal under the laws of one jurisdiction but illegal under the laws of other jurisdictions. More precisely, what is required is a hypothetical determination of whether the laws of different jurisdictions would treat the same transaction differently if the transaction were to fall under the scope of all jurisdictions’ laws simultaneously.

To determine which of these different standards constitutes the more stringent one, it makes sense to differentiate between two situations. First, consider the case in which the standards of different jurisdictions have a “nested” relationship. A nested relationship exists between two jurisdictions when a transaction that complies with the first jurisdiction’s laws automatically complies with the laws of the second jurisdiction, while the opposite is not true (that is, compliance with the second jurisdiction’s laws does not always imply

54. As is widely discussed in the corporate law literature, these situations can result in a competition between jurisdictions that can have important ramifications for the standards of protection that apply. *See, e.g.*, Bebhuk, *supra* note 12; Cary, *supra* note 10; Romano, *supra* note 10; Winter, *supra* note 10.

55. Besides, there can also be factual barriers to regulation. Most importantly, jurisdictions might be unable to enforce their laws against a transjurisdictional actor. This situation can arise if a transjurisdictional actor does not have any physical presence or assets located in the respective jurisdiction. *See* Goldsmith, *supra* note 10, at 1217. This obstacle’s importance depends on whether a jurisdiction can rely on other jurisdictions to enforce its judgments. Within the United States, the Constitution’s Full Faith and Credit Clause ensures that individual states’ judgments that satisfy certain minimum requirements can be enforced nationwide. *See id.* In the international context, treaties on mutual judicial assistance allow jurisdictions to overcome some enforcement gaps. However, in most contexts, public policy exceptions allow countries to deny the enforcement of foreign judgments in conflict with their fundamental values. *See id.* at 1219-20.

56. I use the term standard to refer to any requirement that the law imposes on transactions. These requirements can take on various forms. For example, they can relate to the substance of the transaction or its form, such as the imposition of a price ceiling or the stipulation of mandatory product characteristics. Substantive requirements can also confer rights on one party that cannot be bartered away. Formal requirements include using a specific contractual form, disclosure requirements, and similar formalities that have to be fulfilled to make the transaction legal. As described above, jurisdictions can also impose no specific requirements on a transaction type. *See supra* note 51.

compliance with the first jurisdiction's laws). In this case, the standard imposed by the first jurisdiction is the more stringent standard.⁵⁷ Second, there are situations in which multiple jurisdictions' standards are not nested, but in which a subset of transactions could pass under the laws of all jurisdictions. In situations like these, the most stringent standard is not the law of one jurisdiction, but a combination of all jurisdictions' laws.⁵⁸

c. Costs of Differentiation and Global Compliance

CBCEs are situations in which a transjurisdictional actor complies with the most stringent standard globally to realize cost savings associated with treating customers in different jurisdictions alike. Put differently, global compliance must be motivated by a desire to reduce costs of differentiation.

Costs of differentiation are any added production or transaction costs that businesses face if they treat consumers in different jurisdictions differently. These costs can stem from different sources. First, they can concern the production of goods or services. For example, it can be costly to maintain different product lines for consumers in different jurisdictions. The steel and plastic widget example above falls into this first category. Second, differentiation costs can also emerge in the form of increased transaction costs if there are special requirements for contracts in some jurisdictions but not in others. For example, jurisdictions can require different contractual formalities for certain types of transactions, or they can endow consumers with different contractual rights.

2. When Do Cost-Based California Effects Occur?

Not every situation in which businesses face costs of differentiation will give rise to CBCEs. This is because the decision to apply stringent standards globally will usually also result in added compliance costs, which have to be balanced against the benefits of treating all customers alike. Accordingly, CBCEs only occur if the total cost savings from treating consumers across jurisdictions alike exceed the added costs of compliance.

To understand what this balancing of costs entails, consider first the costs of treating consumers everywhere in accordance with the most stringent standard. These costs will usually be a function of the regulatory requirement at hand and the amount of business a firm conducts in low-protection jurisdictions.

57. If there are more than two jurisdictions, a nested relationship need not exist between all of them. Instead, it is sufficient that there is one or more jurisdiction (in the latter case, with both jurisdictions imposing similar standards) that "dominate" all other jurisdictions.

58. At least in theory, there can also be situations in which the standards imposed by different jurisdictions are mutually exclusive, wherein there cannot be any transactions of a particular type that would be considered legal in all jurisdictions. See Michael S. Knoll & Ruth Mason, *Blame Kassel Balancing* 48 (unpublished manuscript) (on file with author) (describing scenarios like these as the "Balkans Effect"). In these situations, transjurisdictional actors cannot offer the same product to customers in different jurisdictions.

All else equal, the total added compliance costs will be higher for firms with a higher share of consumers in these low-protection jurisdictions.⁵⁹

Second, consider the costs of treating consumers in different jurisdictions differently. These costs will likely vary among industries and depending on the legal requirement in question. For example, in the case of a law imposing requirements on physical goods' product design, differentiation costs will often be comparably high. This is because a firm's decision to treat consumers in different jurisdictions differently would imply the simultaneous production of more than one product line. By contrast, firms should find it easier to restrict the application of a law requiring the granting of mandatory product warranties to just one jurisdiction.

Costs of differentiation can be either variable costs, fixed costs, or a combination of both. Importantly, unlike the added costs of compliance, these costs need not be (positively) related to the share of a business's customers in low-standard jurisdictions. This is the case, first, insofar as the costs of differentiation are fixed costs. In the widget example, imagine that the simultaneous manufacturing of steel and plastic widgets requires *W* to build a second production facility. Second, it seems possible that the differential treatment of consumers in different jurisdictions increases the costs of doing business in the high-standard jurisdiction as well. This can happen if product differentiation implies forgone economies of scale that would have decreased per unit production costs everywhere.⁶⁰

These considerations suggest that, all else equal (and assuming that companies continue serving consumers in the high-standard jurisdiction), smaller firms are more likely than bigger ones to comply with more stringent standards across jurisdictions. Among businesses of similar size, CBCEs will most likely influence the decision making of those that derive more of their revenues from transactions in the high-standard jurisdiction.⁶¹ These predictions are based on the amount of added costs of compliance that these firms face when deciding to extend the most stringent standards to consumers in other jurisdictions. These costs will usually be greater for firms with higher sales figures overall and for firms that conduct a larger share of their business in low-protection jurisdictions.

59. This is true whenever some of the compliance costs are variable costs. Insofar as compliance costs consist of fixed costs, these costs do not increase the costs of extending compliance with high standards to other jurisdictions.

60. See Bradford, *supra* note 8, at 17-18.

61. This prediction also suggests that CBCEs are most likely in the context of standards enacted by comparably large jurisdictions (e.g., California at the interstate level in the U.S., the U.S. and the EU at the international level). By contrast, if smaller jurisdictions enact similarly high standards, it is often rational for transjurisdictional actors to limit compliance to the extent required by the law. See Anu Bradford, *Exporting Standards: The Externalization of the EU's Regulatory Power via Markets*, 42 INT'L REV. L. ECON. 158, 161 (2015).

3. Distributional and Normative Implications

CBCEs can have important distributional consequences. In the example above, *W* is not the only actor affected by the decision whether to sell steel widgets in Columbiana; instead, this decision also has implications for consumers in both Columbiana and East Atlantica. An increase in production costs will often result in higher product prices, lower numbers of products sold, and a decrease in consumer welfare.⁶² Under the assumption that the decision to offer different products will increase production costs everywhere, East Atlantica consumers will be better off if *W* sells steel widgets in Columbiana as well. Consumers in Columbiana (who are unwilling to pay a premium to buy steel instead of plastic widgets) will prefer the opposite decision, at least if plastic widgets can still be offered at a cheaper price compared to steel widgets.

More generally, if differentiation is costly, consumers in jurisdictions that impose the most stringent standards will usually benefit from the standard's global application. At the same time, a decision in favor of global compliance can increase product prices in other jurisdictions. If the stringent standards benefit consumers, consumers in these jurisdictions might accept higher price tags.⁶³ However, this need not always be the case. Consumers in different jurisdictions might have different preferences regarding the appropriate level of regulation.⁶⁴ If this is the case, the consequences of CBCEs can be normatively problematic.⁶⁵

B. Other Forms of Cross-Jurisdictional Influence

CBCEs are among several mechanisms by which stringent standards in one jurisdiction can affect outcomes in other jurisdictions. While these mechanisms lead to similar outcomes on their face, their normative implications and influence on regulatory interdependence differ substantially.

1. Voluntary Compliance

First, businesses might comply with stringent standards globally for reasons that are unrelated to costs of differentiation. Most importantly, businesses can offer high-standard products globally to increase their revenues, as consumers might be willing to pay more for such products.⁶⁶ In the widget example above,

62. Whether such consequences occur depends mainly on the competitive structure of a market and the number of companies that change their offerings due to California Effects.

63. See BRADFORD, *supra* note 9, at 239-40.

64. See Richard L. Revesz, *The Race to the Bottom and Federal Environmental Regulation: A Response to Critics*, 82 MINN. L. REV. 535, 536 (1997). Besides, it is also possible that the cost and benefits of certain types of regulation vary across jurisdictions. See *id.* at 536-37.

65. I discuss the normative consequences of California Effects at greater length below. See *infra* Section V.A.

66. Bradford's description of the Brussels effect includes instances in which businesses appear to have acted out of such motivation. See BRADFORD, *supra* note 9, at 144-45.

assume that there is a substantial percentage of Columbiana's population that prefers steel widgets over plastic widgets and is willing to pay a higher price for the latter. In this case, even if there were no costs of differentiation, it would be rational for *W* to start selling steel widgets in Columbiana.⁶⁷

While voluntary compliance and CBCEs might appear to lead to similar outcomes, their consequences differ substantially. First, with voluntary compliance, consumers in low-standard jurisdictions benefit—at least in aggregate—from the introduction of high-standard products. This implies that the distributional consequences described in Section I.A.3 are likely absent in instances of voluntary compliance.⁶⁸ Second, in the case of voluntary compliance, businesses can sell low-standard products alongside high-standard products if there is sufficient demand. Finally, in the absence of differentiation costs that drive CBCEs, businesses will typically be more easily able to revise their decision to adopt global compliance in the face of changing circumstances.

2. Diffusion of Laws

Second, stringent standards can propagate across jurisdictions as a result of a diffusion of laws. In other words, a jurisdiction might decide to copy regulations that implemented a particularly stringent standard elsewhere.⁶⁹ These cases differ from CBCEs along various dimensions. Most importantly, the adoption of stringent laws in one jurisdiction is not on its own sufficient to effect changes to transactions in other jurisdictions. At least in principle, policymakers there retain the option to adopt standards that are better suited to their jurisdiction than the standards in the exporting jurisdiction.⁷⁰

67. At the same time, if consumer demand justifies global compliance with stringent standards, businesses ordinarily have incentives to offer consumers an option to purchase high-standard products even without mandatory laws in any jurisdiction. Why, then, does a legal intervention in one jurisdiction lead to a change in transactions elsewhere? Aside from costs of differentiation, there are at least three mechanisms by which laws of one jurisdiction can bring about such a change. First, laws in one jurisdiction could help overcome market failures in other jurisdictions related to consumers' inability to differentiate between high-standard and low-standard products. See George A. Akerlof, *The Market for "Lemons": Quality Uncertainty and the Market Mechanism*, 84 Q. J. ECON. 488, 488 (1970). In this situation, other jurisdictions' laws and enforcement activities can play a role similar to that of private certification providers. Second, a legal change in one jurisdiction can lead to a shift of consumer preferences in another jurisdiction, for example, because the legal change increases awareness about specific problems. Finally, if most of the costs required to comply with the new standard imposed by one jurisdiction are fixed costs, the expenditure of these costs can unlock more profitable business opportunities in other jurisdictions. Importantly, this is true even if the benefits of selling improved products in all jurisdictions are not high enough to justify the investment absent a legal obligation in at least one jurisdiction.

68. This is because companies have incentives to offer the product that maximizes the total surplus, which is divided between the company and its customers. Under normal circumstances, a business's voluntary decision to switch to high-standard products will maximize not only the business's profits, but also aggregate consumer welfare.

69. Some of the literature on regulatory interdependence describes this effect as an instance of the California Effect. See *supra* note 41.

70. Of course, the adoption of stringent standards in one jurisdiction can tilt the political landscape in other jurisdictions in favor of similar policy initiatives. For example, the former jurisdiction

C. Cost-Based California Effects and the Internet

This Article focuses on transactions between businesses and consumers that take place on the internet. Unlike in traditional contexts, actors' physical locations generally do not constrain interactions on the internet. At least in principle, content and services made available on websites and similar devices can be accessed everywhere. Also, the internet's architecture implies that it can be costly, and sometimes even impossible, for actors to ascertain the identity and physical location of a party with whom they interact.

Against this background, a naïve view might hold that differentiation costs are substantially higher for online service providers than for other businesses. If this were the case, CBCEs would likely be more prevalent in the context of transactions on the internet than they are in traditional transactions. Taken to the extreme, if online services were generally unable to distinguish between customers in different jurisdictions,⁷¹ CBCEs would be ubiquitous on the internet.⁷²

If this was ever an adequate description of online activities, it has been rendered obsolete by two parallel developments. The first development is the emergence of ever-better geo-identification technology.⁷³ This technology allows providers of online services to distinguish—with some degree of certainty—between customers located in different jurisdictions and to offer different versions of their services to these customers.⁷⁴

The second development concerns the scope of laws regulating interactions between online service providers and their customers. Jurisdictions mostly refrain from applying their laws to transactions between online service providers

might attempt to exert pressure on other jurisdictions to adopt similar standards. Also, businesses active in multiple jurisdictions might also lobby for the introduction of stringent standards everywhere, particularly because it might afford them advantages over local competitors. *See, e.g.*, VOGEL, *supra* note 8, at 68-70.

71. This is equivalent to assuming infinite differentiation costs.

72. There are several examples of cases before courts of various jurisdictions in which online service providers unsuccessfully argued for exemptions from regulation based on the argument that it would require them to change their operations in other jurisdictions as well. This argument also played a significant role in early academic debates about the regulation of online activities. Proponents of the cyberlibertarian movement in the 1990s in particular argued that the regulation of online activity would result in the simultaneous application of the laws of all jurisdictions simultaneously. *See, e.g.*, David R. Johnson & David Post, *Law and Borders—The Rise of Law in Cyberspace*, 48 STAN. L. REV. 1374, 1375-76 (1996). As Jack Goldsmith argued, advocates of this view overstated the extent of the ensuing problem because of limits in jurisdictions' power to enforce their laws against foreign actors. *See* Goldsmith, *supra* note 10, at 1220.

73. GOLDSMITH & WU, *supra* note 8, at 60-62; DAN JERKER B. SVANTESSON, PRIVATE INTERNATIONAL LAW AND THE INTERNET 525-36 (3d ed. 2016).

74. Differentiating between customers is even more straightforward if there are elements of a transaction that take place in the real world. For example, shopping websites, food delivery services, and similar businesses can limit deliveries to specific jurisdictions or areas. Paid online content can be restricted to customers whose residence in a particular jurisdiction has been confirmed by a provider of payment services such as a bank or credit card company.

and consumers if the service provider has taken appropriate measures to prevent consumers in this jurisdiction from accessing a website or service.⁷⁵

Together, these developments imply that it is generally feasible for online service providers to ascertain the laws that apply to a given transaction and modify their handling of the transaction according to these laws. As a result, there is little reason to assume that CBCEs are inherently more common in online transactions than they are in traditional transactions.⁷⁶

II. Consumer Privacy Law in the United States and in the EU

While data privacy laws in the United States and the EU have common intellectual roots⁷⁷ and early on developed in a similar direction,⁷⁸ they have diverged strikingly over the past several decades.⁷⁹ Today, the United States and the EU occupy what can be seen as opposite poles of the spectrum of liberal democracies' regulatory approaches to data privacy.⁸⁰ The EU has emerged as a forerunner in implementing so-called "omnibus" privacy laws which establish comprehensive, mandatory standards of protection that limit the collection and use of personal data by both public and private actors.⁸¹ In the United States, no such comprehensive set of rules exist. Federal (and until very recently, state) legislation targeting business is limited to narrow subfields such as education and credit reporting.⁸² In most areas, it is therefore left to the market to determine the scope of privacy protections for customers vis-à-vis businesses.⁸³

75. See, e.g., County Court of Paris, Interim Court Order, League Against Racism & Anti-Semitism & French Union of Jewish Students v. Yahoo! Inc., No. RG 00/05308 (Nov. 20, 2000).

76. See Goldsmith, *supra* note 10, at 1200-01.

77. See Paul M. Schwartz, *The EU-U.S. Privacy Collision: A Turn to Institutions and Procedures*, 126 HARV. L. REV. 1966, 1970-71 (2013) (describing how the data privacy discourse in Germany had been influenced by early work on privacy law in the United States).

78. See *id.* at 1975 (describing how international harmonization even led some observers to hypothesize about a convergence of regulation).

79. See generally Paul M. Schwartz & Karl-Nikolaus Pfeifer, *Transatlantic Data Privacy Law*, 106 GEO. L.J. 115 (2017) (identifying differences between EU and U.S. perspectives on individual legal interests within data privacy laws).

80. See, e.g., Franz-Stefan Gady, *EU/U.S. Approaches to Data Privacy and the "Brussels Effect": A Comparative Analysis*, 2014 GEO. J. INT'L AFFS. 12, 15; Kimberly A. Houser & W. Gregory Voss, *GDPR: The End of Google and Facebook or a New Paradigm in Data Privacy?*, 25 RICH. J.L. & TECH. 1, 9 (2018).

81. Schwartz, *supra* note 77, at 1973-74 ("[T]he Directive has encouraged the rise of omnibus legislation throughout the EU and most of the world."); Paul M. Schwartz, *Global Data Privacy: The EU Way*, 94 N.Y.U. L. REV. 771, 777-78 (2019) (describing how EU data privacy law has inspired similar legislation elsewhere).

82. E.g., Schwartz, *supra* note 77, at 1974-75.

83. See Schwartz & Pfeifer, *supra* note 79, at 132 ("Unlike the EU's data subject, U.S. law does not equip the privacy consumer with fundamental constitutional rights; rather, she participates in a series of free exchanges involving her personal information. In this legal universe, the rhetoric of bilateral self-interest holds sway."); Shaffer, *supra* note 49, at 13 ("[T]he United States . . . relies more on private ordering through market processes.").

A. The United States's Market-Based Approach

One of the defining features of consumer privacy law in the United States is that businesses are by default free to gather, process, and share information that they obtain from their customers. Consumers enjoy legal protection only under a rather narrow set of circumstances. Various legal sources can promulgate limits on permissible data practices. First, “sectoral” federal and state legislation restricts the gathering and use of information by specific businesses and concerning specific types of data.⁸⁴ Second, data practices can run afoul of applicable legal rules beyond data privacy law.⁸⁵ These rules include common-law institutions, such as contract law, as well as statutory law. From a practical perspective, the most important rule in this category is section 5 of the Federal Trade Commission Act, which has served as the basis for several enforcement actions brought by the Federal Trade Commission (FTC) against data practices perceived as deceptive or unfair.⁸⁶ Finally, California and a few other states adopted laws imposing a range of obligations on most businesses that gather data on consumers in these states.

In practice, whenever sectoral legislation does not apply, data privacy is mostly a matter of contract between customers and businesses.⁸⁷ Businesses face no substantial constraints on their data practices as long as they provide consumers with an accurate and transparent description of these practices.⁸⁸ This is different only for residents of the above-mentioned states who, since the entry into force of the CCPA and similar laws in other states, enjoy certain rights vis-à-vis businesses that collect information on them.

84. *E.g.*, Fair Credit Reporting Act (FCRA), 15 U.S.C. § 1681(a)-(x) (2018); Family Educational Rights and Privacy Act (FERPA), 20 U.S.C. § 1232(g) (2018).

85. *See* DANIEL J. SOLOVE & PAUL M. SCHWARTZ, *PRIVACY LAW FUNDAMENTALS* 134-44 (2019).

86. Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 *COLUM. L. REV.* 583 (2014). These enforcement actions have focused on broken promises in privacy policies and other deceptive and unfair practices. *Id.* at 627-43; SOLOVE & SCHWARTZ, *supra* note 85, at 143. The most important substantive constraints following from the FTC’s interpretation of section 5 of the FTC Act concern the implementation of adequate security practices to guard against data security breaches. Solove & Hartzog, *supra*, at 636-38, 643. Some in the literature have raised doubts about the effectiveness of this regime. *See, e.g.*, Florencia Marotta-Wurgler & Dan Svirsky, *Do FTC Privacy Enforcement Actions Matter? Compliance Before and After US-EU Safe Harbor Agreement Actions* (NYU L. & Econ., Working Paper No. 16-18) (on file with the author).

87. Kevin E. Davis & Florencia Marotta-Wurgler, *Contracting for Personal Data*, 94 *N.Y.U. L. REV.* 662, 663 (2019) (“To a large extent, the relationship between the business and user with regards to information privacy is contractual.”). It is subject to dispute whether privacy notices outlining a business’s data practice should be treated as contracts in the legal sense. *Compare* SOLOVE & SCHWARTZ, *supra* note 85, at 136, *with* Omri Ben-Shahar & Lior Jacob Strahilevitz, *Contracting over Privacy: Introduction*, 45 *J. LEGAL STUD.* S1, S7 (2016).

88. *See* Davis & Marotta-Wurgler, *supra* note 87, at 663 (“The protection of consumer information in the United States has followed a ‘Notice and Choice’ approach, where businesses outline their information privacy practices . . . which are typically incorporated by references in general Terms of Service contracts, to which users must agree.”).

B. Omnibus Regulation in the EU

Since the late 1990s, EU law has offered consumers a uniform set of comprehensive protections against the collection and use of personal data by both public and private actors.⁸⁹ By default, businesses require a legal justification to gather, process, and share personal information about consumers in the EU. One important avenue for businesses to obtain authorization is to demonstrate that the “processing [of data] is necessary for the purposes of the[ir] legitimate interests,”⁹⁰ which essentially delegates the decision about the scope of permissible data practices to the agencies and courts tasked with enforcing data privacy law. Authorization can also be obtained by securing the consumer’s consent.⁹¹ Notably, however, EU law establishes both formal requirements for obtaining consent⁹² and mandatory rights for consumers that cannot be contracted away.⁹³ Moreover, EU law provides for the establishment of specialized enforcement agencies tasked with prosecuting data privacy violations.

While EU law has followed this general approach since the entry into force of the Data Protection Directive in 1995,⁹⁴ the GDPR substantially tightened the restrictions for businesses handling consumer data along multiple dimensions.⁹⁵ First, it scaled up the requirements for legally handling consumer data in the first place. In particular, to obtain a consumer’s consent, businesses now need to provide them with a clear description of every intended use of their data.⁹⁶ If information is not needed to provide a good or service, businesses are generally not permitted to make interactions with consumers conditional on their consent with a business’s data practices.⁹⁷ Also, consumers can withdraw their consent at any time, rendering future processing of the data illegal.⁹⁸ Second, the GDPR extended the number and scope of rights that consumers enjoy vis-à-vis

89. Before the EU started regulating privacy law, it had been a domain of the EU member states, some of which had enacted comparably strong privacy protections even in the absence of EU law. *See* Schwartz, *supra* note 77, at 1969-71.

90. GDPR, *supra* note 2, art. 6(1)(f); *cf.* Council Directive 95/46, art. 7(f), 1995 O.J. (L 281) 31 (EC) [hereinafter Data Protection Directive] (“[Personal data may be processed if] processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party . . .”).

91. GDPR, *supra* note 2, art. 6(1)(a); *cf.* Data Protection Directive, *supra* note 90, art. 7(a) (“[Personal data may be processed if] the data subject has unambiguously given his consent . . .”).

92. Such formal requirements include restrictions on blanket provisions and certain forms of click-wrap contracts. *See* Case C-673/17, *Bundesverband der Verbraucherzentralen und Verbraucherverbände v. Planet49 GmbH*, ECLI:EU:C:2019:801, ¶¶ 44-65 (Oct. 1, 2019) (failing to deselect prechecked checkboxes does not imply consent).

93. *See* Schwartz & Pfeifer, *supra* note 79, at 139 (“EU data protection law establishes important areas of inalienable privacy, setting out bedrock data protection principles that are not subject to individual waiver and cannot be traded away in bargained-for exchanges.”).

94. *See* Data Protection Directive, *supra* note 89. Because rulemaking was done through an EU Directive, the EU Member States had to adopt national laws for the Data Protection Directive to become fully effective. By contrast, the GDPR is directly applicable to the EU Member States because it takes the form of an EU Regulation.

95. *E.g.*, Rustad & Koenig, *supra* note 4, at 376-79.

96. GDPR, *supra* note 2, arts. 7(2), 13(1).

97. *Id.* art. 7(4).

98. *Id.* art. 7(3).

businesses that obtained information on them in the past. Consumers can, *inter alia*, request information about the usage of their data,⁹⁹ demand correction of any false information¹⁰⁰ as well as deletion of information that is no longer needed,¹⁰¹ and ask for a copy of the information obtained by the business in order to supply this information to a competing service.¹⁰² Finally, the GDPR substantially expanded the scope of potential monetary fines for violations of data privacy rules.¹⁰³

In sum, EU law imposes substantial restrictions on businesses' handling of consumer information that cannot be overridden by contractual agreement. Rather than trusting market mechanisms to determine the ideal scope of permissible data practices, the EU approach relies heavily on public actors such as enforcement agencies and courts.

C. The GDPR's Legal Scope

While the territorial scope of the GDPR is broad, it is not unlimited. Most importantly for the purposes of this Article, EU privacy law is generally not applicable to transactions in which neither the business nor the consumers are physically present in the EU.

The application of the GDPR is triggered whenever one of two conditions is met. First, the GDPR covers all handling of personal data that is done by businesses or business units operating out of the EU.¹⁰⁴ Second, it also covers other businesses' or business units' data practices insofar as they target consumers in the EU.¹⁰⁵ As a consequence, EU privacy law usually does not apply to interactions between businesses and consumers if none of them are located in the EU.¹⁰⁶

99. *Id.* art. 15.

100. *Id.* art. 16.

101. *Id.* art. 17.

102. *Id.* art. 20.

103. Meg Leta Jones & Margot Kaminski, *An American's Guide to the GDPR*, DENV. L. REV. 98, 106 (2021). Fines for violations of the GDPR can amount to up to 4% of an undertaking's annual worldwide turnover.

104. GDPR, *supra* note 2, art. 3(1). This norm establishes that all handling of consumer data that takes place "in the context of the activities of an establishment" in the EU is subject to the GDPR, even though the data processing itself might take place elsewhere. According to the case law of the Court of Justice, this requirement is met whenever a business has a "branch or subsidiary" in one of the member states, and the use of consumer data is connected to the activities of this business unit. Case C-507/17, *Google LLC v. CNIL*, ECLI:EU:C:2019:772, ¶¶ 48-52 (Sept. 24, 2019) (deciding that Google's use of information about consumers to build its products together with the general "commercial and advertising activities" of Google's French subsidiary was sufficient to fulfill this condition).

105. GDPR, *supra* note 2, art. 3(2); GUIDELINES 3/2018 ON THE TERRITORIAL SCOPE OF THE GDPR (ARTICLE 3), EUR. DATA PROT. BD. (Nov. 12, 2019), https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_3_2018_territorial_scope_after_public_consultation_en_1.pdf [<https://perma.cc/B4TP-K5TX>].

106. Given the scarcity of case law on Article 3 of the GDPR, the precise territorial scope of the regulation is still unclear. In particular, it is unclear whether the Court of Justice's broad interpretation of Article 3(1) can result in a situation in which businesses that operate mostly outside the EU have to

III. Cost-Based California Effects in Data Privacy Law?

A. General Considerations

The de facto Brussels Effect is particularly strong in the domain of data privacy. . . . Various examples suggest that, for today's global digital companies, maintaining different data practices across global markets is often both difficult (due to technical non-divisibility) and costly (due to economic non-divisibility).

– Anu Bradford¹⁰⁷

As Bradford's argument demonstrates, CBCEs are assumed to play an important role in data privacy law.¹⁰⁸ Commentators have, for decades, speculated about the existence of these effects. An early proponent of this idea was Professor Gregory Shaffer, who predicted in a 2000 article that it would “be pragmatically difficult for businesses to employ two sets of data privacy practices, one for EU residents (providing for greater privacy protection) and one for U.S. residents (providing for less).”¹⁰⁹ In a 2006 book, Goldsmith and Wu described a similar concept as an example of “global laws.”¹¹⁰ Finally, in her work on the “Brussels Effect,” Bradford regularly describes data privacy law as one of the fields in which the EU extends its regulatory reach through CBCEs.¹¹¹

As these examples show, claims about CBCEs in data privacy law precede the GDPR. However, when several prominent online services, such as Google and Facebook, announced in 2018 the adoption of what they described as GDPR-

extend GDPR-style protections to consumers in non-EU countries. However, it seems unlikely that the Court of Justice will interpret the GDPR to cover situations in which the consumer, the business's headquarters, and the business units involved in the transaction are located outside the EU. For example, in its decision in *Google LLC v. CNIL*, the Court of Justice showed reluctance to extend the scope of rights established in the GDPR to situations that mostly involved actors in other jurisdictions. *Google LLC*, C:2019:772 at ¶¶ 53-72.

107. BRADFORD, *supra* note 9, at 142-43.

108. CBCEs are not the only channel through which the EU is said to have changed data practices beyond the territorial scope of the GDPR. According to some, the EU also exerts pressure on other jurisdictions to adopt data privacy laws similar to its own. In particular, the EU reportedly uses the “adequacy procedure” required for non-EU countries to receive general clearance that allows companies to transfer data gathered in the EU into these countries. See BRADFORD, *supra* note 9, at 149-50; Christina Lam, *Unsafe Harbor: The European Union's Demand for Heightened Data Privacy Standards in Schrems v. Irish Data Protection Commissioner*, 40 B.C. INT'L & COMP. L. REV. 10 (2017). But see Schwartz, *supra* note 81 (describing the negotiations between the EU and other countries in adequacy procedures as “collaborative” rather than as an exercise in unilateral power). Besides, the obligation to implement strict data privacy standards in the EU could have provided transjurisdictional businesses with an incentive to lobby for the introduction of similar standards elsewhere. See BRADFORD, *supra* note 9, at 148.

109. Shaffer, *supra* note 49, at 78.

110. GOLDSMITH & WU, *supra* note 8, at 173-77.

111. Bradford, *supra* note 8, at 25 (“Internet companies find it difficult to create different programs for different markets and therefore tend to apply the strictest international standards across the board. At times, it is technologically difficult or impossible to separate data involving European and non-European citizens. Other times it may be feasible but too costly to create special websites or data-processing practices just for the EU.”); Bradford, *supra* note 61, at 164 (“Technical non-divisibility often applies for the regulation of privacy. For example, the EU forces companies like Google to amend their data storage and other business practices to conform to European privacy standards. Facing a technical difficulty to isolate its data collection for the EU, Google is forced to adjust its global operations to the most demanding EU standard.”).

compliant privacy policies on a global level, proponents of this theory viewed it as additional evidence in favor of CBCEs.¹¹² Proponents of this view conjecture that these effects caused many firms to adopt GDPR-compliant privacy standards globally,¹¹³ which also implies that EU data privacy standards governs the relationship between many U.S. businesses and their customers in the United States. Today, even commentators who are otherwise skeptical about the EU's power to impose its data privacy laws on other jurisdictions sometimes concede the possibility of CBCEs.¹¹⁴

At the same time, there are reasons to doubt the pervasiveness of CBCEs in data privacy law. As others have documented, websites now routinely adjust the content they show to visitors based on their location.¹¹⁵ This observation suggests that online services might also be able to tailor their offerings to the legal requirements of the jurisdiction in which the consumer is based. This is particularly true because, as I argue above, not every situation in which it is costly to treat consumers in different jurisdictions differently gives rise to CBCEs. Instead, CBCEs require that costs of differentiation outweigh the added costs of compliance related to treating consumers in low-standard jurisdictions in accordance with the more stringent standards established in a high-standard jurisdiction.¹¹⁶

Furthermore, much of the discussion of CBCEs in data privacy law ignores the fact that the question whether CBCEs exist is likely not a simple yes-or-no question.¹¹⁷ Rather, it seems possible that service providers reserve some of the protections envisioned by the GDPR to EU consumers, while other GDPR-induced changes benefit consumers from other countries as well. The latter might be particularly relevant in the context of GDPR provisions that require service providers to establish internal compliance mechanisms¹¹⁸ or for rules that affect the fundamental structure of digital products.¹¹⁹

112. BRADFORD, *supra* note 9, at 142-45; Rustad & Koenig, *supra* note 4, at 389-96.

113. BRADFORD, *supra* note 9, at 142-43.

114. Anupam Chander, Margot E. Kaminski & William McGeeveran, *Catalyzing Privacy Law*, MINN. L. REV. (forthcoming 2022) (manuscript at 42), <https://papers.ssrn.com/abstract=3433922> (“For the most part the GDPR has not had a (de jure) ‘California Effect’ on the U.S. federal government or U.S. states, but it has had a (de facto) ‘Brussels Effect’ on companies operating in U.S. jurisdictions.”); Schwartz, *supra* note 81, at 780 (“Under Bradford’s factors, there is indeed much evidence that suggests a de facto unilateral Brussels Effect for privacy.”).

115. *See, e.g.*, GOLDSMITH & WU, *supra* note 8, at 60-62

116. *See supra* Section I.A.2.

117. *But see* Leta Jones & Kaminski, *supra* note 103, at 110 (“While companies might not provide for individual data protection rights to individuals in non-EU countries around the world, they may be more likely to extend internal compliance patterns to non-EU data.”).

118. *Id.* One example of an internal compliance mechanism is the appointment of Data Protection Officers. GDPR, *supra* note 2, art. 37.

119. One example is the use of third-party service providers in websites. *See* Peukert et al., *supra* note 25.

B. Existing Empirical Evidence

While many in the literature seem to treat the existence of CBCEs in data privacy law as a given, there is only limited empirical evidence to prove their existence and scope. Most observers who assume the existence of CBCEs base their claims on anecdotes of major online services professing to align their global operations with EU privacy law either at the entry into force of the GDPR or when confronted with EU regulators in other instances.¹²⁰ At the same time, even proponents of California Effects like Bradford acknowledge that these effects are not ubiquitous.¹²¹ Furthermore, in line with the observation that compliance with the GDPR might not be a simple yes-or-no decision, even some companies whose reactions to the GDPR are often cited as examples of CBCEs did not treat customers from non-EU countries similarly to EU consumers across every dimension.¹²²

Some additional support for the existence of (Cost-Based) California Effects comes from a series of quantitative studies that investigate changes to privacy policies and other privacy-related website features over the course of the GDPR's entry into force. In line with the hypothesis that CBCEs are a major factor in data privacy law, several studies find that even websites that are likely not subject to the GDPR have responded to its entry into force in a way that leads to better privacy protections for their visitors. Nevertheless, these studies do not provide conclusive evidence either for or against the widespread existence of CBCEs in data privacy law.

It is possible to distinguish between two lines of work: studies that focus on changes to privacy policies and those that focus on changes to other privacy-related features. One example from the first group is a recent paper by Thomas Linden and coauthors, who document substantial changes to the text of privacy policies obtained from websites they describe as “Global” websites (as opposed

120. BRADFORD, *supra* note 9, at 142-45; Rustad & Koenig, *supra* note 4, at 389-96; *see also* GOLDSMITH & WU, *supra* note 8, at 175-76.

121. BRADFORD, *supra* note 9, at 145.

122. One example of a disparate treatment of consumers despite a pledge to harmonize data practices across jurisdictions is Facebook's handling of consent for facial recognition technology. When Facebook introduced its new global data privacy in April 2018, it issued a statement providing that it would use facial recognition technology only if users “turned on” this feature. Complaint ¶ 153, *United States v. Facebook*, 456 F. Supp. 3d 115 (D.D.C. 2019) (No. 19-2184). However, while users in the EU had to opt in to activate this feature, it was automatically turned on for many users in the United States. *Id.* ¶¶ 144-56; *see* Leo Kelion, *Facebook Seeks Facial Recognition Consent in EU and Canada*, BBC NEWS (Apr. 18, 2018), <https://www.bbc.com/news/technology> [<https://perma.cc/H542-CP35>].

In a similar vein, even if companies in principle treat customers in different jurisdictions alike, customers outside the EU will regularly not be able to rely on the GDPR's enforcement mechanisms to protect their interests. In this context, it is interesting to note that Facebook restructured its legal relationship with customers in Africa, Asia, Australia, and the Middle East before the entry into force of the GDPR, replacing its European subsidiary with a U.S. entity as the provider of services for customers in these jurisdictions. Some commentators have described the elimination of potential enforcement actions related to the treatment of these customers outside the EU as the main reason for this move. *See* BRADFORD, *supra* note 9, at 145-46.

to “EU” websites).¹²³ However, the study does not examine the nature of these changes. Therefore, on its own, its findings are insufficient to show that websites extended GDPR-style privacy protections to consumers outside the EU. The study also does not attempt to show that online services located outside the EU treated consumers everywhere the same, as CBCEs would predict. In another recent paper, Kevin Davis and Florencia Marotta-Wurgler investigate changes in privacy policies in various industries between 2014 and 2018.¹²⁴ While they document that terms covered by the GDPR became more protective during that period, they also report relatively low absolute rates of compliance and variation across industries, which suggests that market forces drive the adoption of more protective standards.¹²⁵

The second group of studies analyzes changes in other privacy-relevant website features, with mixed results. Perhaps the strongest evidence for the existence of CBCEs comes from a recent paper by Professor Christian Peukert and coauthors.¹²⁶ Analyzing changes in websites’ use of third-party services following the GDPR’s entry into force, they document that those changes extended to situations that were not covered by the GDPR.¹²⁷ By contrast, Adrian Dabrowski and coauthors show that many websites differentiate between consumers in the EU and elsewhere when it comes to the use of cookies.¹²⁸

IV. Empirical Analysis

This Part presents novel evidence on the existence of CBCEs in data privacy law in the United States. In particular, it sheds light on the question whether and to what extent U.S. online services changed their privacy policies in an attempt to offer GDPR-style protections to consumers in the United States. Contrary to the hypothesis that CBCEs prompted most U.S. online services with exposure to the GDPR to adopt GDPR-compliant privacy policies on a global level, it shows that these services adopted a range of strategies to treat EU consumers and U.S. consumers differently. For one, the analysis shows that several services feature separate privacy policies that apply to EU citizens, and that they changed these EU privacy policies at a substantially higher rate than their U.S. privacy policies around the entry into force of the GDPR. For another,

123. Thomas Linden, Rishabh Khandelwal, Hamza Harkous & Kassem Fawaz, *The Privacy Policy Landscape After the GDPR* (2019), <https://arxiv.org/abs/1809.08396> [<https://perma.cc/FX9U-TUVB>].

124. Davis & Marotta-Wurgler, *supra* note 87, at 695-700.

125. *Id.* at 702-03. Other studies focus on changes to privacy policies in the EU. *See, e.g.*, Martin Degeling, Christine Utz, Christopher Lentzsch, Henry Hosseini, Florian Schaub & Thorsten Holz, *We Value Your Privacy . . . Now Take Some Cookies: Measuring the GDPR’s Impact on Web Privacy* (2019), <https://arxiv.org/abs/1808.05096> [<https://perma.cc/FW9T-E894>]. Because these studies provide little insight into the existence of CBCEs, I do not describe them further.

126. Peukert et al., *supra* note 25.

127. *Id.* at 11-13.

128. Adrian Dabrowski, Georg Merzdovnik, Johanna Ullrich, Gerald Sendera & Edgar Weipp, *Measuring Cookies and Web Privacy in a Post-GDPR World*, in *PASSIVE AND ACTIVE MEASUREMENT* 258, 264-66 (David Choffnes & Marinho Barcellos eds., 2019).

it shows that many services that did not have separate privacy policies for consumers in different jurisdictions responded to the GDPR by updating their privacy policies in line with the requirements in the GDPR, but explicitly limited the rights flowing from the GDPR to EU citizens.

A. Research Design

1. Measuring Changes to Privacy Policies

There are various ways in which CBCEs could have influenced the handling of information on U.S. consumers by businesses in the United States. At one end of the spectrum of possible responses are decisions to treat all consumers worldwide in line with the rules established in the GDPR. Such decisions entail, among other things, allowing all consumers to exercise the GDPR's various data-subject rights—for example, the right to erasure. The decisions by companies like Google and Facebook to adopt purportedly GDPR-compliant privacy policies on a global level fall into this category. But even absent such a wholesale adoption of GDPR-compliant privacy practices, the GDPR could still have influenced individual aspects of businesses' global data practices. For example, as Meg Leta Jones and Margot Kaminski argue, the GDPR required companies to adopt privacy compliance mechanisms that might have rendered companies more aware of privacy concerns in general.¹²⁹

The analysis presented in this Article focuses on the first type of reaction. It asks whether U.S. businesses, in reaction to the GDPR's entry into force, changed their treatment of U.S. consumers as if they had been legally required to treat those consumers pursuant to the protections established in the GDPR. The most important reason for the decision is a pragmatic one: in a quantitative study like the one presented here, one cannot possibly capture all the ways in which privacy practices changed in response to the GDPR's entry into force. Against this background, the decision to focus on reactions like those observed for Google and Facebook reflects the fact that observers often describe these reactions as paradigmatic examples of California Effects in data privacy law.

In order to measure online service providers' reactions to the entry into force of the GDPR, the analysis focuses on their privacy policies. Privacy policies are the focus of this analysis because there are limited opportunities to obtain direct information about businesses' handling of consumer data. Most of these activities are hidden from public view. As a result, any attempt to construct a dataset with comprehensive information on the actual data practices of large numbers of online service providers would be futile. By contrast, privacy policies are available for the public to inspect on almost all major websites on the

129. Leta Jones & Kaminski, *supra* note 103, at 110.

internet.¹³⁰ Privacy policies describe—in varying degrees of detail—what information is stored, when and how it is processed, and when and how it is transferred to servers in other jurisdictions and/or third parties.

Of course, it can be argued that privacy policies are but a crude measure for companies' privacy practices. After all, who knows whether online services practice what they preach? However, there are reasons to assume that privacy policies are a relatively good proxy for businesses' actual handling of consumer data. First, a company that treats consumer data less favorably than stipulated in its privacy policy risks legal consequences. This is true in the EU, where such a deviation between policy and practice would render the data processing illegal, as well as in other jurisdictions. Although privacy policies are not generally mandated by federal law in the United States, a failure to comply with a privacy policy can result in enforcement actions by the FTC based on section 5 of the FTC Act.¹³¹ Second, while it cannot be ruled out that companies treat consumers more favorably than described in their privacy policies, my conversations with privacy professionals suggest that such deviations are marginal at best.¹³²

Besides, the structure and content of a privacy policy on their own can provide some insights into whether businesses attempt to be GDPR-compliant. For online services that fall under the scope of EU privacy law, the GDPR imposes an extensive set of requirements regarding the contents of privacy policies.¹³³ These requirements differ markedly from the requirements set up in the GDPR's predecessor, the Data Protection Directive.¹³⁴ It seems reasonable to assume that almost all businesses that wanted to comply with the GDPR's requirements had to change their privacy policies before the regulation's entry into force.

At the same time, this study's approach also means that the analysis presented here might miss some ways in which the GDPR increased the privacy protection levels enjoyed by U.S. consumers. For example, as Peukert and coauthors have shown, websites everywhere reduced their reliance on third-party

130. In the EU, privacy policies have long been mandatory for all websites that collect their visitors' information. GDPR, *supra* note 2, art. 13; Data Protection Directive, *supra* note 90, art. 10. In the United States, while federal law does not mandate the universal use of privacy policies, most websites feature a privacy notice either to comply with state law (for example, the California Online Privacy Protection Act of 2003), or because it is required by third-party services whose tools are implemented on a website. See Ari Ezra Waldman, *Privacy, Notice, and Design*, 21 STAN. TECH. L. REV. 74, 90-93 (2018).

131. See *supra* Section II.A. One example of an instance in which a failure to comply with a GDPR-inspired privacy policy in the United States led to FTC enforcement actions is Facebook's handling of consent for its face recognition feature. See *supra* note 122. These actions were part of the alleged misconduct that resulted in a \$5 billion settlement between the FTC and Facebook in 2019. See Press Release, Fed. Trade Comm'n, *FTC Imposes \$5 Billion Penalty and Sweeping New Privacy Restrictions on Facebook*, FTC (July 24, 2019), <https://www.ftc.gov/news-events/press-releases/2019/07/ftc-imposes-5-billion-penalty-sweeping-new-privacy-restrictions> [<https://perma.cc/T436-G6JC>]. Some in the literature have raised doubts about the effectiveness of the FTC's enforcement actions in the field of data privacy. Marotta-Wurgler & Svirsky, *supra* note 86.

132. In particular, all interview partners dismissed the idea that online services whose privacy policies included special rights for consumers from the EU would extend these rights to consumers from other jurisdictions.

133. GDPR, *supra* note 2, art. 13.

134. Data Protection Directive, *supra* note 90, art. 10.

providers after the GDPR took effect.¹³⁵ Insofar as the text of privacy policies did not reflect these changes, the empirical approach pursued here would have been unable to detect them.

2. Leveraging Variation Over Time

As a matter of principle, it is challenging to measure the effects of laws without observing variation over time. This is because, without such variation, it is usually impossible to obtain an estimate for how the same actors observed in the study would behave in the absence of the law. For this reason, I focus on changes to privacy policies around the entry into force of the GDPR. This allows me to compare the state of the world before and after that point in time. Changes in privacy policies that can be attributed to the GDPR's entry into force suggest that these businesses are—at least de facto—under the influence of EU law.

While this study can, therefore, exploit changes over time, it lacks a second feature that is usually considered an essential prerequisite for measuring causal effects: because the potential reach of EU privacy law extends to websites worldwide, there is no clearly identifiable group of untreated privacy policies (that is, a group of policies that could not possibly have been affected by the GDPR). Thus, it is challenging to attribute any observed changes in privacy policies to the entry into force of the GDPR. After all, other factors might have effected similar changes even in the absence of the GDPR.

My response to this challenge is twofold. First, the dataset's structure allows me to compare the changes observed while the GDPR took effect to changes during other periods. Therefore, I can determine whether changes similar to the ones observed around the entry into force of the GDPR also occurred in other periods. While such tests cannot completely rule out the possibility that some other factor caused changes observed during the entry into force of the GDPR, they have the potential to render such an alternative explanation unlikely. Second, I investigate the quality of the changes in detail, measuring whether they implement the specific requirements introduced by the GDPR.¹³⁶ While this is no perfect remedy for the lack of a control group either, a finding that privacy policies conform closely with Article 13 of the GDPR renders alternative explanations rather unlikely.

3. Illustrations

To illustrate the approach taken in this study, consider the following examples. As discussed above, both Google and Facebook are often cited as examples of companies that offer GDPR-style protections to consumers

135. Peukert et al., *supra* note 25.

136. See generally Marion Dumas & Jens Frankenreiter, *Text as Observational Data*, in *LAW AS DATA: COMPUTATION, TEXT, AND THE FUTURE OF LEGAL ANALYSIS* 59 (Daniel Rockmore & Michael A. Livermore eds., 2019) (discussing new opportunities offered by textual data in the exploration of causal processes).

worldwide.¹³⁷ Even before the GDPR, Google’s and Facebook’s websites displayed essentially the same privacy policy to users accessing their websites from the EU and the United States (including to those customers who accessed country-specific versions of Google). On or shortly before the GDPR’s enactment, both Google and Facebook changed the content of their privacy policies for users everywhere, again offering essentially the same privacy protections to all users. While not offering definitive proof that EU law *de facto* governs the handling of all personal data by Facebook and Google, this observation seems to support the claim that European data privacy law affects the relationship between these two companies and their U.S. customers.¹³⁸

However, not all services are like Google and Facebook. One important counterexample is Amazon. Until May 2018, customers accessing *amazon.com* from the United States, *amazon.co.uk* from the UK, and *amazon.de* from Germany were shown privacy policies that contained essentially the same information. On May 22, 2018, Amazon changed the privacy policies on its EU websites but not the privacy policy on its U.S. website. Subsequently, the EU website’s privacy policy differed markedly from the one Amazon used in the United States. Among other things, the revised privacy policy in the EU suggests that Amazon stopped using email tracking in the EU and location-based services if a consumer accessed the website using a mobile device. If Amazon adopted these changes to conform with what it perceived as requirements imposed by the GDPR, then the fact that it did not change its U.S. privacy policy suggests that EU law did not influence its relations with consumers based in the United States.¹³⁹

Amazon is not the only service that “forked” its privacy policy. WhatsApp, a Facebook subsidiary since 2014, acted similarly. In late April of 2018, it posted a new privacy policy on the German version of its website. In this privacy policy, it addressed at length the rights users enjoyed under the GDPR. By contrast, the U.S. version of WhatsApp’s website did not change its privacy policy between August 2016 and January 2020. As a result, WhatsApp’s U.S. privacy policy did not contain comparable protections.

Other services changed the privacy policy’s text for all users but explicitly limited the rights flowing from the GDPR to EU citizens. One example of this approach is Pinterest’s U.S. privacy policy adopted around the entry into force

137. *See supra* Section III.A.

138. Along the lines of the challenges described in Sections IV.A.1 and IV.A.2, there are several reasons why this observation does not offer full proof of the proposition that EU law governs the relationship between Google or Facebook and their U.S. customers. First, as we do not know whether Google and Facebook would have adopted similar changes in the absence of the GDPR, we cannot exclude the possibility that the entry into force of the GDPR did not cause the observed change in privacy policies. Second, it seems at least possible that Google and Facebook changed only their privacy policies, but not their handling of personal data.

139. Of course, the fact that Amazon did not change the privacy policy on its U.S. website offers no proof that it did not start handling data concerning U.S. customers differently in reaction to the GDPR’s enactment, either. However, there is no apparent reason why Amazon would not change its U.S. privacy policy as well.

of the GDPR. This policy states that certain rights mandated by the GDPR would only be available to European consumers. The text of the provision is as follows:

You have options in relation to the information that we have about you described below. To exercise these options, please contact us. If you're an EEA user, you can:

- Access the information we hold about you. . .
- Have your information corrected or deleted. . .
- Object to us processing your information. . .
- Have the information you provided to us sent to another organization. . .
- Complain to a regulator. . .

Importantly, when websites adopt this type of provision, consumers in the EU and consumers in the United States enjoy different protection levels despite being shown identical privacy policies. Furthermore, the existence of this type of provision points to a fundamental limitation of studies that seek to measure the effect of the GDPR on privacy protections in the United States solely by documenting changes in the text of privacy policies of U.S. websites. Even if these changes implement requirements of EU law, they might leave the level of protection for U.S. consumers untouched.

4. Research Questions

The examples in the preceding Section illustrate that the question of whether the owners of U.S. websites extend EU-style privacy protections to U.S. customers cannot be answered with a simple “Yes” or “No.” Some do, others don't. Against this background, this empirical investigation has three main goals: It seeks to determine, first, how widespread the adoption of GDPR-style protections is among U.S. online services. Put very simply, do most U.S. websites resemble Google, Facebook, and other GDPR-compliant websites in their reactions to the entry into force of the GDPR, or do they look more like the U.S. version of Amazon? Second, for those websites that adopt GDPR-style privacy protections, it examines whether these rights are limited to EU consumers. Finally, it explores whether the observed patterns of responses allow for insights into businesses' motivations to extend GDPR-style privacy protections to consumers in other jurisdictions. The overall goal is to obtain evidence about the existence of CBCEs.

B. Data

In the analysis, I use a longitudinal dataset consisting of the texts of the privacy policies of 693 websites, with one observation per week between late November 2017 and October 2019.¹⁴⁰ The dataset was assembled in two steps.

140. More details on the dataset can be found in the Online Appendix. Jens Frankenreiter, *The Missing “California Effect” in Data Privacy Law: Online Appendix*, https://www.jensfrankenreiter.com/_files/ugd/de5252_664c855b29574770b9f04d771f58a72a.pdf [<https://perma.cc/7YEN-KZV4>] [hereinafter *Online Appendix*]; see also Frankenreiter & Hermstrüwer, *supra* note 26 (describing the dataset).

The core of the dataset (covering 271 websites, with a majority of websites in the EU) consists of privacy policies that were downloaded weekly during that period.¹⁴¹ The dataset was amended in January 2020 using snapshots¹⁴² of other websites' privacy policies obtained from archive.org.

The dataset consists of two parts. The first part contains most of the most frequented websites in the United States (here referred to as *U.S. websites* and *U.S. privacy policies*), including most websites that appear in the Top 500 ranking in Alexa's Top Sites service.¹⁴³ For various reasons, I exclude some of the websites that appear in this ranking, including all websites operated by online services located in the EU.¹⁴⁴ As a result, this dataset consists of privacy policies for 357 websites. In assembling this part of the dataset, I used additional measures to ensure that the dataset does not mistakenly contain a privacy policy exclusively shown to EU consumers visiting the website.¹⁴⁵ For this, these websites' privacy policies were either downloaded from locations within the United States or using a VPN client.¹⁴⁶

The second part of the dataset, which serves mostly as a control group, consists of some of the most important websites in the EU (*EU websites* and *EU privacy policies*). The dataset contains all websites among the Alexa Top 500 for the U.K. and Germany that meet one of three conditions: (1) they are operated by services located in the EU, (2) they use a European top-level domain (.de, .uk), or (3) they feature a separate version of the website that is explicitly directed at consumers in the EU—for example, a German version (in the last case, I use the version directed at EU consumers).¹⁴⁷ For EU privacy policies, I took similar steps to the ones described above to ensure that the dataset contains the version of the privacy policy displayed to EU consumers. Overall, the second part of the dataset consists of 277 websites from Germany and 59 websites from the U.K.

The final dataset contains almost 70,000 privacy policies, with a structure similar to that of a (balanced) panel dataset with $N = 693$ and $T \sim 100$. To make these privacy policies amenable to further analysis, I removed those that were

141. Websites were downloaded using a Python script.

142. When available, I obtained weekly snapshots. For some websites, the intervals at which privacy policies are available are considerably longer than that.

143. *The Top 500 Sites on the Web*, ALEXA, <https://www.alexa.com/topsites> [<https://perma.cc/8WAP-NTCA>].

144. The reason for this last decision is that services located in the EU are under a legal obligation to treat all consumers in line with the provisions in the GDPR. *Supra* Section II.C. Therefore, the incentives that these sites face in their treatment of U.S. customers are different from those of service providers based in the United States. In addition, I limited the dataset to websites with privacy policies that are available in English and excluded websites that use the same privacy policy as another website in the sample.

145. In principle, it is possible that consumers in different jurisdictions are being shown different versions of a website. *See supra* Part III. It is unclear whether online service providers have in turn displayed country-specific privacy policies to different customers. *See* Peukert et al., *supra* note 25, at A-3.

146. NordVPN.

147. I also excluded websites that made no privacy policy available in either English or German.

duplicates of the same website's privacy policy at *T-I*¹⁴⁸ and used an array of tools to extract the text of the actual privacy policy.¹⁴⁹ I then manually inspected all nonduplicate texts to ensure that they contained the privacy policy's actual text.¹⁵⁰

In addition to the texts of the privacy policies, I obtained a range of background variables for all U.S. websites. On the basis of information collected from alexa.com, I obtained a measure for the relative share of users visiting a website from an EU member country (*Pct_EU_Users*). From similarweb.com, I obtained the average number of users per month (in the analysis, I use the logarithmic version of this measure, *Log_Total_Users*) as well as the type of service provided by the website.

Additionally, I determine whether a website explicitly targets EU consumers alongside consumers in the United States (*EU_target*), or whether there is a separate version of the website available that is directed at EU consumers (*EU_twin*).¹⁵¹ In the latter case, I also check whether the privacy policy of the EU version of the website is featured among the EU privacy policies in my sample.

C. Analysis and Results

1. Computational Analysis

In this Section, I analyze the development of privacy policies around the time of the entry into force of the GDPR using measures obtained by way of automated text analysis.

a. Outcome Measures

Automated text analysis comprises a range of techniques that make text amenable to quantitative research.¹⁵² Put very simply, these tools convert text into numerical representations without the need for human coders. Because these measures are calculated automatically, I can obtain measures for every privacy policy in the sample.

148. For this, I used a Python script that compared the occurrence of the most frequent words with more than three letters in the text of different privacy policies.

149. Because custom methods for boilerplate removal such as boiler pipe produced unsatisfying results, I used a custom-made algorithm trained to "predict" the beginning and end of the text of a privacy policy.

150. The resulting corpus consists of 3,889 texts.

151. One example of a website targeting EU consumers alongside U.S. consumers is Facebook.com, which is available in German. Amazon is an example of a service offering different versions of its website to consumers in the United States and in the EU. For most websites, I obtained information on the service provider from Wikipedia.

152. See generally Jens Frankenreiter & Michael A. Livermore, *Computational Methods in Legal Analysis*, 16 ANN. REV. L. SOC. SCI. 39 (2020) (explaining the use of computational methods in legal scholarship).

In the analysis, I use three different measures.¹⁵³ First, I calculate the length of each policy by number of words (*num_words*). The second measure captures the amount of text added between two versions of the same privacy policy (*compare_docs*). The measure is based on the distribution of tri-grams in both documents. This measure resembles a simple plagiarism detector, with the difference that I am mostly interested in the parts of the text that were not copied from another source.¹⁵⁴

Finally, I also include a measure of the use of GDPR-specific vocabulary (*GDPR_vocab*) obtained through topic modeling. Topic modeling is a machine-learning technique that can be used to measure the semantic content of documents. In order to do so, topic modeling identifies groups of co-occurring words and groups them into topics. Topic modeling is an unsupervised technique: contrary to other text analysis tools, it does not require training data. In other words, topic modeling can discern the structure of a corpus of documents without any input that guides its decisions.¹⁵⁵ To obtain *GDPR_vocab*, I estimate a structural topic model with $K = 39$ topics and calculate the sum of all topics whose average prevalence increased by at least 100% during the entry into force of the GDPR.¹⁵⁶ The measure ranges from 0 to 1, with 0 indicating no use of GDPR-specific language.

b. Results

i. The Development of U.S. Privacy Policies

As a first step, I use the measures described above to obtain a bird's-eye view of the development of U.S. privacy policies around the entry into force of the GDPR. Remember that the U.S. privacy policies were obtained from websites operated by U.S. and other non-EU service providers.¹⁵⁷ These websites were

153. Note that there is a plethora of candidate measures available. The choice of these three measures does not necessarily imply that they are better suited than others to illustrate the effects in question. Rather, I use these three measures because they represent three fundamentally different approaches to track changes in privacy policies. In a series of robustness checks, I replicated the analyses in this subsection using a large range of alternative measures. The results of these analyses are not substantially different from the ones presented in this paper. The results of several robustness checks are reported in the Online Appendix. See *Online Appendix, supra* note 140, at 13-16.

154. The measure ranges from 0 to 1, with 1 indicating a privacy policy that was completely rewritten. I obtained the measure using the following steps: (1) calculate the tri-gram frequency vectors for the earlier and the later document; (2) subtract the vector representing the earlier document from the vector representing the later document; (3) set all negative values to 0; and (4) divide the sum of the resulting vector by the sum of the tri-gram vector representing the later document.

155. The output of a topic model consists of two main components. The first component is a set of distributions of topics over documents. Simply put, each document is assigned a numerical vector (whose components add up to 1), indicating the influence of each of the topics on the document. The second part is the topics themselves. Topics are also represented by numerical vectors adding up to 1. In the case of topics, these numerical vectors represent probability distributions over words.

156. The Online Appendix contains detailed information on the procedure used to determine K and on descriptions of the topics that were included in *GDPR_vocab*. See *Online Appendix, supra* note 140, at 8-9.

157. *Supra* Section IV.B.

under no *legal* obligation to apply the GDPR in interactions with U.S. customers,¹⁵⁸ and the policies were obtained in ways that make sure that the dataset only contains the policies that were used for these customers. Against this background, if the GDPR only affected interactions that fall under its legal scope, one might expect to see no or only a few unusual changes in the texts of these policies around the time of the entry into force of the GDPR.

I begin by analyzing the timing of changes in the texts of privacy policies. For this, I use the *compare_docs* measure described above.¹⁵⁹ Figure 1 depicts the development of this measure graphically. The figure features two panels, with the upper panel representing U.S. websites and the lower panel EU websites. A gray line represents each website in the sample. A measure close to 0 indicates no or only minimal changes between a privacy policy at the dates shown on the x-axis and the same website's privacy policy seven days before. A measure close to 1 indicates that almost the entire text of the privacy policy was revised. The black line displays the average amount of text added across the websites in a jurisdiction. The day of the GDPR's enactment, May 25, 2018, is marked by a black, dashed vertical line.

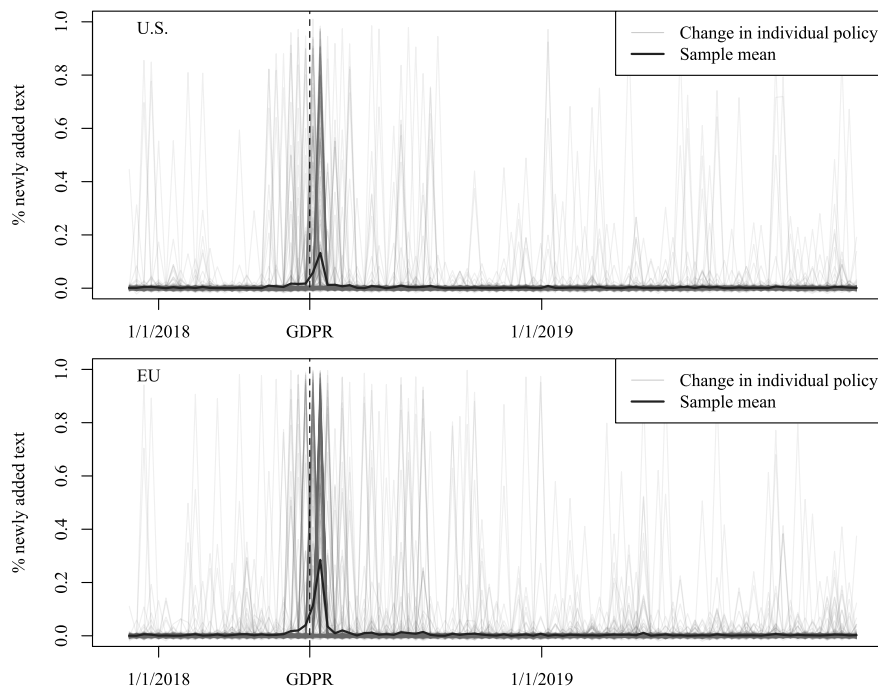
The focus here is on the upper panel, which depicts changes for U.S. websites. As this graph shows, privacy policies change at various times in the period under observation. However, there is a flurry of activity around the entry into force of the GDPR. In the two weeks surrounding this event, U.S. websites added an average of almost 20% of new text to their privacy policies. This change is far bigger than any other change observed during the time under observation.

However, it merits mention that the reactions observed for different websites in the sample differ considerably. 133 out of 357 websites in the sample (37.3%) added no new text to their privacy policies between April 2018 and July 2018 (Amazon's U.S. website is among this group). 178 out of 357 U.S. websites in the sample (49.9%) added 10% or more new text to their privacy policies between April 2018 and July 2018. Changes of a similar magnitude are unusual under normal circumstances; for example, between November 2017 and February 2018, such changes could only be observed for 20 websites (5.6% of the sample). Only 66 websites (18.4% of the sample) changed their privacy policies to the same extent as Google and Facebook, whose privacy policies featured more than 75% newly added text in July 2018.

158. See *supra* Section II.C.

159. *Supra* Section IV.C.1.a.

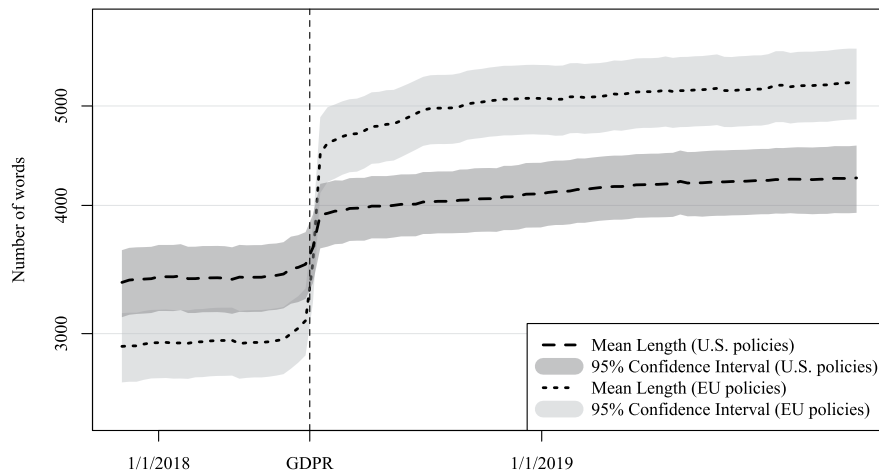
Figure 1: Newly Added Text Per Week



Notes: Amount of newly added text to privacy policies by week. Gray lines represent individual websites in the sample. x-axis: date. y-axis: amount of newly added text (variable compare_docs). Measures close to 0 indicate limited or no changes. Measures close to 1 indicate a full revision of the privacy policy. Black line depicts the sample mean. Black dashed line: Date of the entry into force of the GDPR.

An analysis of the length of privacy policies yields similar results. Figure 2 reports the mean length of all U.S. and EU policies in the sample at any given point in time (using a logarithmic scale on the y-axis). The grey areas surrounding the means depict 95% confidence intervals.

Figure 2. Length of Privacy Policies



Notes: Mean length of privacy policies (measured in number of words) in different jurisdiction at different points in time. x-axis: date. y-axis: number of words in privacy policy. y-axis uses a logarithmic scale. Grey areas represent 95% confidence intervals. Black dashed line: Date of the entry into force of the GDPR.

As Figure 2 shows, the length of U.S. privacy policies increased substantially in the weeks around the entry into force of the GDPR. On April 2, 2018, they averaged 3,405 words. By July 2, 2018, they had grown to an average of 3,973 words, an increase of around 16.7% compared to April 2, 2018. The rate of growth spiked around the entry into force of the GDPR. In the two-week period starting on May 21, 2018 (the week of the entry into force of the GDPR), the average length of privacy policies increased by 410 words. This increase is more than 1,000% larger than any increase observed for any two weeks outside May and June 2018.

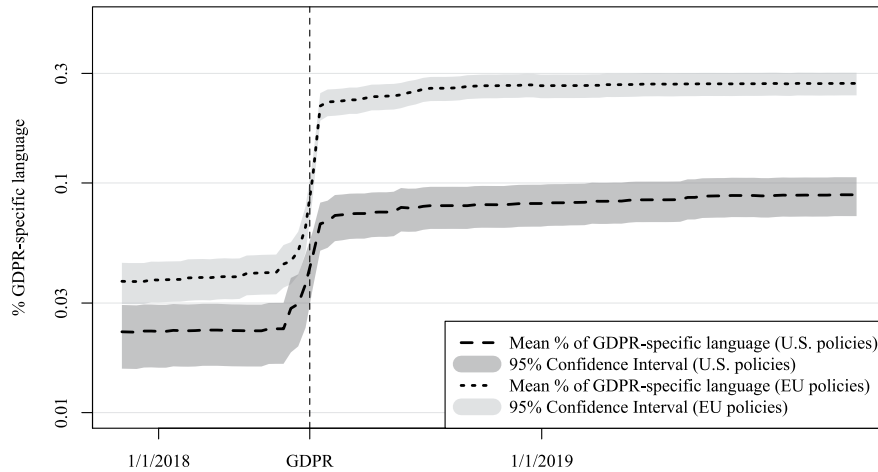
The distribution of changes mirrors the one for *compare_docs*. The privacy policies of 185 websites (37.8%) did not increase in length between April and July 2018. 132 websites (37.0%) showed increases in length by at least 300 words. And only 68 websites (19.0%) showed changes in the order of magnitude of Google and Facebook, which increased their privacy policies by more than 1,500 words.

A similar picture also emerges when focusing on the use of GDPR-specific language, *GDPR_vocab*.¹⁶⁰ As shown in Figure 3, such language played a minor role in U.S. privacy policies before the entry into force of the GDPR, with an average of less than 3% of the policy texts. In fact, for most sites (263, or 73.7% of the sample), such language represented below 0.5% of the total vocabulary used in privacy policies. This changes after the entry into force of the GDPR. By

160. See *supra* Section IV.C.1.a.

July 2, 2018, privacy policies in the United States used, on average, more than 7% of GDPR specific language. At the same time, this change affected only a minority of privacy policies: 152 privacy policies (among them that of Amazon’s U.S. site) still featured less than 0.5% of GDPR-specific language.

Figure 3: Use of GDPR-Specific Language over Time



Notes: Mean percentage of GDPR-specific language (*GDPR_vocab*) in different jurisdictions at different points in time. x-axis: date. y-axis: use of GDPR-specific language. y-axis uses a logarithmic scale. Grey areas represent 95% confidence intervals. Black dashed line: Date of the entry into force of the GDPR.

Overall, these changes seem to suggest that a considerable number of U.S. privacy policies changed in reaction to the enactment of the GDPR. This finding suggests that the GDPR affected online transactions beyond its legal scope.

At the same time, these results on their own do not allow for the conclusion that many online services introduced GDPR-compliant privacy standards globally. Rather, it is interesting to observe that the changes observed for most privacy policies (~80%) were a lot less pronounced than those of Google’s and Facebook’s.

The limited nature of the changes observed for U.S. privacy policies is also evident from comparing U.S. privacy policies and EU privacy policies. As Figures 1 to 3 illustrate, the changes for most U.S. websites were considerably smaller than those of average EU websites.

Consider first the *compare_docs* measure. The lower panel of Figure 1 represents changes observed for EU websites. In principle, the pattern looks similar to that observed for U.S. websites. However, the changes appear to be of a bigger magnitude than the changes observed for U.S. websites. In fact, the responses observed for Facebook and Google (which were in the top quintile of

U.S. websites) seem fairly typical for EU websites. 147 EU websites (43.8%) showed changes of the same magnitude or bigger.

In a similar vein, the changes observed for the numbers of words used in U.S. privacy policies and the use of GDPR-specific language appear modest compared to the changes observed in the EU. As described above, the average length of U.S. privacy policies increased by 16.7% between April 2, 2018, and July 2, 2018. As Figure 2 demonstrates, these changes pale in comparison with the changes observed for EU privacy policies: these privacy policies increased by an average of 1,752 words (59.6%), with a mean increase of 1,404 words in the two weeks after May 21, 2018, alone. As Figure 3 illustrates, the same picture emerges for changes in the amount of GDPR-specific language.

The differences between U.S. and EU websites persist when one limits the analysis to U.S. websites operated by service providers known to interact with consumers in the EU ($EU_target = 1$ and/or $EU_twin = 1$). For example, while the length of these websites' privacy policies grew somewhat more than that of other U.S. privacy policies (the average growth in length for this subsample was 735 words or 19.3%), this increase is still more than 1,000 words fewer than the increase observed for EU websites.

ii. A Quantitative Test of Global Compliance

As a second step, I test more formally whether U.S. privacy policies changed in a way that suggests a GDPR-compliant treatment of U.S. consumers by U.S. online services.

Similar to the informal comparisons between U.S. privacy policies and EU privacy policies in Section IV.C.1.b.i above, this test uses the changes observed for EU privacy policies as a baseline against which it compares the changes observed for U.S. privacy policies. Remember that the EU websites were under a *legal* obligation to treat consumers in line with the GDPR. Against this background, if CBCEs forced U.S. online service providers to treat their U.S. customers in line with the GDPR, one would expect U.S. privacy policies (at least those used by services that also interacted with consumers in the EU) to show patterns of change similar to those of EU privacy policies.

However, unlike the informal comparisons presented above, this test uses only the subsample of U.S. websites that feature a separate website version directed at EU consumers whose privacy policy is included in the EU part of my sample.¹⁶¹

The reason to restrict the sample in this way is that, on their own, differences between the U.S. and EU samples are not sufficient to conclude that the GDPR affected U.S. and EU online services differently. This is because of the potential role of differences in the two samples. As described above, EU policies were sampled with an eye toward ensuring that all websites in this sample were under a legal obligation to treat EU consumers according to EU data

161. See *supra* Section IV.B.

privacy law.¹⁶² No emphasis was placed on ensuring that the EU websites in the dataset were comparable to the U.S. websites. Against this background, it seems possible that some or even all of the observed differences between U.S. policies and EU policies are not due to general differences in the way U.S. websites and EU websites react to the entry into force of a new law like the GDPR. Instead, these differences could be explained by differences in the characteristics of the websites in both samples. In other words, the analysis above might not be comparing apples to apples.

Restricting the sample to services whose EU policies are included in the dataset provides an effective way to tackle these and other related concerns. This is because the same service providers operate both the U.S. privacy policies in this sample and the EU privacy policies. Therefore, any differences in the observed reactions of service providers cannot be attributed to unobserved website characteristics. Moreover, one can directly observe how many individual service providers implement similar changes to their U.S. and EU privacy policies. If CBCEs forced online service providers to treat consumers in all jurisdictions alike, one would expect these changes to be identical.

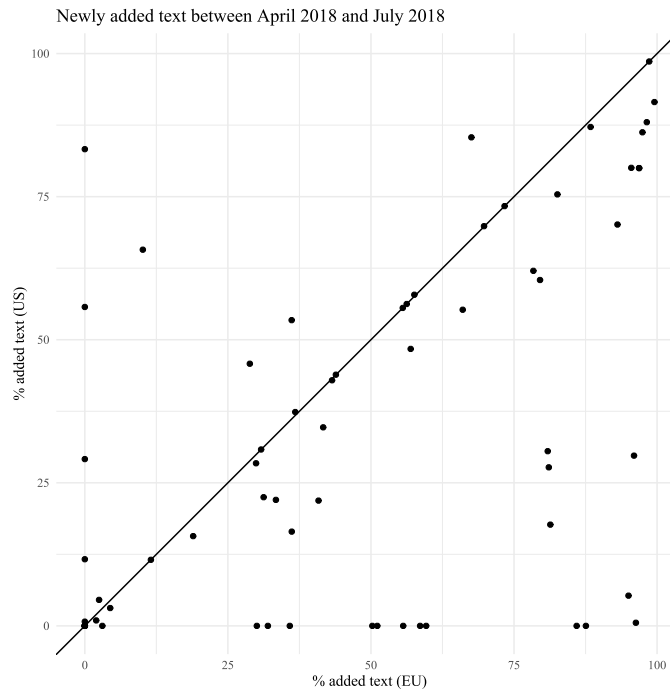
The resulting dataset consists of 67 U.S. privacy policies and their EU counterparts. Examples of online service providers in this sample include Amazon and WhatsApp, whose reactions to the entry into force of the GDPR I described above.¹⁶³

Figure 4 reports how the service providers' policies in the United States and the EU changed around the entry into force of the GDPR. More specifically, it reports the amount of newly added text between April 2 and July 2, 2018 (a version of the *compare_docs* measure described above). Each point represents one service provider. The x-axis depicts how much text the same service provider added to its EU privacy policy. The amount of added text to a provider's U.S. privacy policy is shown on the y-axis. If service providers changed the texts of their U.S. privacy policies in roughly similar ways to the texts of their EU privacy policies, the points would be clustered around the diagonal line running from the bottom left to the upper right corner of the graphic. Instead, the graph shows that a substantial number of providers added considerably more text to their EU privacy policies than to their U.S. privacy policies. Overall, 33 out of 67 websites in the matched sample added at least five percentage points more new text to their EU privacy policy than they did to their U.S. privacy policy. On average, EU privacy policies grew by 13.7 percentage points more than the respective U.S. privacy policies. A paired samples Wilcoxon test indicates that these differences are statistically significant, with a p-value of .0002.¹⁶⁴

162. *Id.*

163. *See supra* Section IV.A.3.

164. Because the distribution of the difference between the added text is not normal, a Wilcoxon test is more appropriate than the standard t-test. A paired t-test yields a p-value of .001. In the Online Appendix, I replicate this analysis using *num_words* and *GDPR_vocab* as outcome variables. *See* Online Appendix, *supra* note 140, at 15-16. These tests confirm that the existence of systematic differences in

Figure 4: Changes for Services with U.S. and EU Privacy Policies

Notes: Scatterplot showing the amount of newly added text between April 2, 2018 and July 2, 2018 for a service's EU (x-axis) and U.S. privacy policy (y-axis). Each point represents one service provider.

This result suggests the existence of systematic differences in how U.S. businesses with operations in Europe adjusted the privacy policies of U.S. websites and EU websites in reaction to the GDPR's entry into force. In other words, it points to the possibility that a sizeable share of U.S. online services with operations in the EU did not follow the example of Google and Facebook in adopting a global privacy policy that extended the rights established in the GDPR to consumers in the United States. Instead, this result suggests that numerous websites might not have granted U.S. consumers the same privacy protections they offered to EU consumers post-GDPR.

2. Manual Coding

While the computational analysis suggests that U.S. websites reacted differently to the entry into force of the GDPR than EU websites, this method is ultimately unable to determine the degree to which U.S. consumers profited from the rights established in the GDPR. One important reason for this is the existence

how online service providers changed U.S. privacy policies and EU privacy policies in reaction to the entry into force of the GDPR.

of privacy protections the scope of which is limited to consumers in the EU, a fact that would arguably be missed by most available automated text analysis tools.¹⁶⁵ Therefore, in this part of the analysis, I analyze the contents of privacy policies using a manually coded subsample.¹⁶⁶

a. Sample Selection and Coding Scheme

The hand-coded sample consists of two privacy policies for each of 246 randomly selected websites in the dataset. The first privacy policy for each website is the one that was in place on April 2, 2018. The second is the policy from October 1, 2018. Given the focus of this project, the sampling scheme prioritized U.S. over EU privacy policies. 150 privacy policies are from U.S. websites, 96 from EU websites (82 from Germany and 14 from U.K.).

Websites were coded according to a coding scheme that attempts to capture whether privacy policies satisfy a range of requirements of the GDPR. As described above, the GDPR contains a set of rather specific requirements that have to be met before businesses can legally obtain consumer data. Among others, businesses have to have a privacy policy that contains a description of the legal bases for gathering data under EU law and communicates to the consumer the various rights she has against the business.¹⁶⁷ The coding scheme distills these requirements into nine items that—at least in principle—have to be present to achieve compliance with the GDPR. Seven of the items in the coding scheme represent rights that consumers have against the business; two concern the legal basis for gathering data.

For each of the nine items, three different responses were allowed under the coding instructions: (1) compliance (the requirement established by the GDPR was met); (2) no compliance (the privacy policy failed to implement the requirement); and (3) compliance limited to EU citizens (the policy contained the provision required by the GDPR, but stipulated that the provision would not apply to U.S. citizens).

The following examples illustrate the use of the coding scheme. The GDPR requires businesses to provide consumers with information about “the existence of the right to request from the controller . . . erasure of personal data.”¹⁶⁸ The coding scheme asks whether websites conform with this requirement. One example of a compliant privacy policy (coded as a “1”) is Airbnb’s U.S. privacy policy adopted in April 2018. The privacy policy contains the following provision:

We generally retain your personal information for as long as is necessary for the performance of the contract between you and us and to comply with our legal obligations. If you no longer want us to use your information to provide the Airbnb

165. See *supra* Section IV.A.3.

166. The hand-coding was done in the context of a parallel project with a coauthor at Max Planck Bonn. See Frankenreiter & Hermstrüwer, *supra* note 26.

167. GDPR, *supra* note 2, art. 13; see *supra* Section II.B.

168. GDPR, *supra* note 2, art. 13(2)(b).

Platform to you, you can request that we erase your personal information and close your Airbnb Account.

In January 2019, Airbnb updated its privacy policy. From that point on, the respective paragraph in the privacy policy read as follows:

We generally retain your personal information for as long as is necessary for the performance of the contract between you and us and to comply with our legal obligations. In certain jurisdictions, you can request to have all your personal information deleted entirely.

Compared with the previous provision, this change suggests that AirBnb would reserve the right to reject requests for data deletion if such request were not made by consumers protected by the GDPR. Therefore, this provision would have been coded as a “3” under the coding scheme.

From the coding, I construct a compliance score reporting the number of items for which the privacy policy corresponds with the requirements of the GDPR. The score ranges from 0 to 9, with 9 indicating compliance with all items. For websites in the United States, I calculate two versions of this score. The first version tracks compliance with the GDPR from the perspective of U.S. customers (*compl_UScust*). In other words, this measure captures whether the policy promises a treatment of U.S. customers that is in line with the requirements of the GDPR. Second, I measure compliance from the perspective of EU customers, who, as described above, might profit from additional rights granted exclusively to them (*compl_EUcust*). For EU websites, which generally do not differentiate between customers from different jurisdictions, I only calculate *compl_EUcust*.

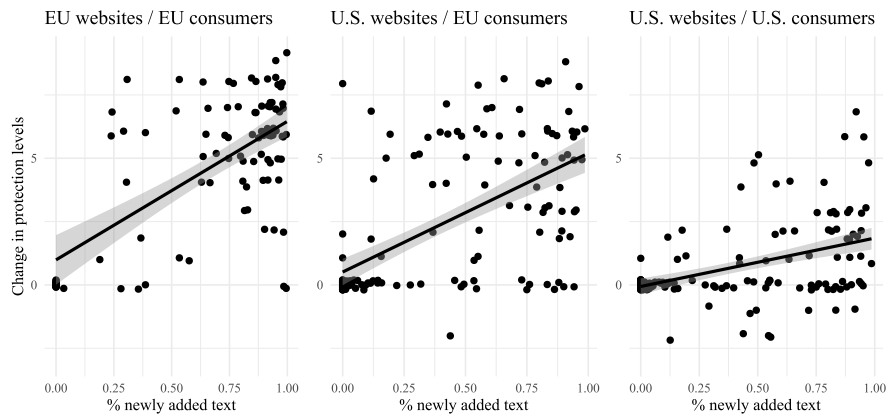
b. Results

i. The Legal Significance of Privacy Policy Changes

First, using these compliance scores, I examine whether the changes to privacy policies documented in Section IV.C.1.b.i above correspond to improvements in GDPR compliance. Figure 5 reports the relationship between the measure for the change in the text of websites between April 2, 2018 and October 1, 2018 (*compare_docs*) and the measure of legal change in the same period (calculated as the difference between compliance levels for two versions of the same website).

The left panel depicts EU websites. These websites exhibit a strong relationship between textual changes and improvements in compliance levels: only a few websites that changed the text of their privacy policies between April and October 2018 did so without increasing compliance with the GDPR’s requirements. At the same time, websites that changed less than 25% of the text of their privacy policies generally did not improve their GDPR compliance.

Figure 5: Changes in Privacy Policy Texts and Compliance Scores



Notes: Scatterplots showing correlations between changes to the text of privacy policies and compliance for different groups of websites and consumers. x-axis: amount of newly added text between April 2, 2018 and October 1, 2018 (*compare_docs*). Black solid lines depict estimates and confidence intervals from univariate OLS regressions. Y-axis: change in compliance scores from April 2, 2018 to October 1, 2018 (*compl_UScust/compl_EUcust*). Left panel: EU websites/*compl_EUcust*. Middle panel: U.S. website/*compl_EUcust*. Right panel: U.S. websites/*compl_UScust*.

A similar (although weaker) relationship exists for U.S. websites insofar as they interact with EU consumers, shown in the middle panel in Figure 5. By contrast, the relationship is considerably weaker for U.S. websites’ treatment of U.S. consumers (depicted in the panel on the right). As this panel shows, many U.S. websites that implemented substantial changes to the text of their privacy policies did so without extending GDPR-required protections to their U.S. consumers. These results suggest that analyses that rely solely on measuring changes to the texts of U.S. privacy policies likely overstate the GDPR’s impact on the relationship between U.S. websites and their U.S. customers. Many U.S. websites modified the text of the privacy policies they used in their relationship with U.S. customers. However, many of the changes did not substantially alter the legal status of consumers based in the United States but instead exclusively benefited EU consumers.

ii. Protection Levels

Second, I investigate in more depth how compliance scores changed for different types of websites between April 2018 and October 2018, and whether U.S. websites systematically treat U.S. consumers different from EU consumers.

I begin by reporting results for the EU sample. Websites in this sample were under a legal obligation to comply with the GDPR. If these websites reacted to the GDPR’s entry into force by updating their privacy policies to make them

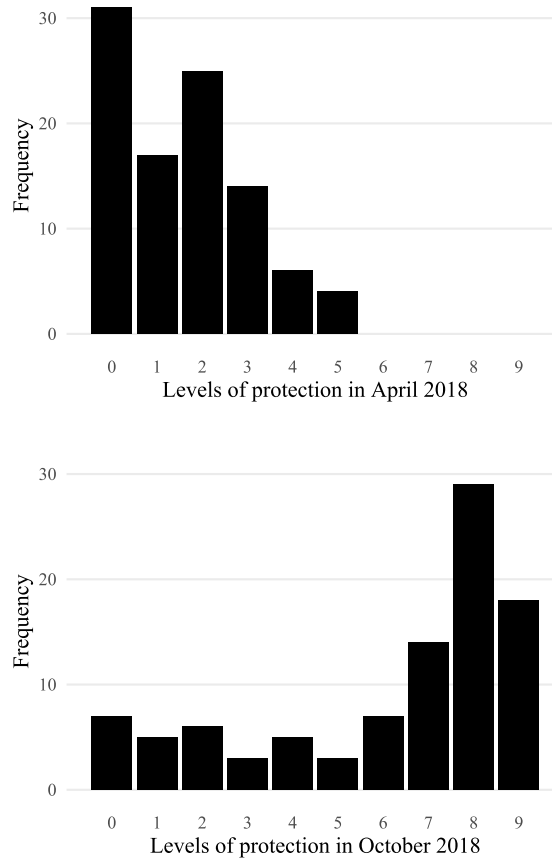
GDPR-compliant, compliance scores should increase substantially between April 2018 and October 2018.

Figure 6 reports compliance scores (*compl_EUcust*) for EU websites before and after the entry into force of the GDPR. The figure indicates that the measure for GDPR-compliance increased dramatically over the six months between April 2018 and October 2018. Only four websites in the sample featured a privacy policy that fulfilled most of the GDPR's requirements by early April. In October 2018, by contrast, most EU privacy policies seemed to, by and large, comply with the GDPR: the number of websites that complied with the majority of the requirements of the GDPR had increased to 73 (76% of the sample).

The substantial shift in GDPR compliance can also be illustrated by comparing mean *compl_EUcust* scores before and after the entry into force of the GDPR. In April 2018, EU websites had an average *compl_EUcust* score of 1.57. In October 2018, this score had increased to 6.13.¹⁶⁹ These results suggest that the coding scheme captures changes induced by the GDPR in a meaningful way.

169. These changes are highly significant; a one-sample t-test yields a p-value of < .0001.

Figure 6: Compliance Scores for EU Websites

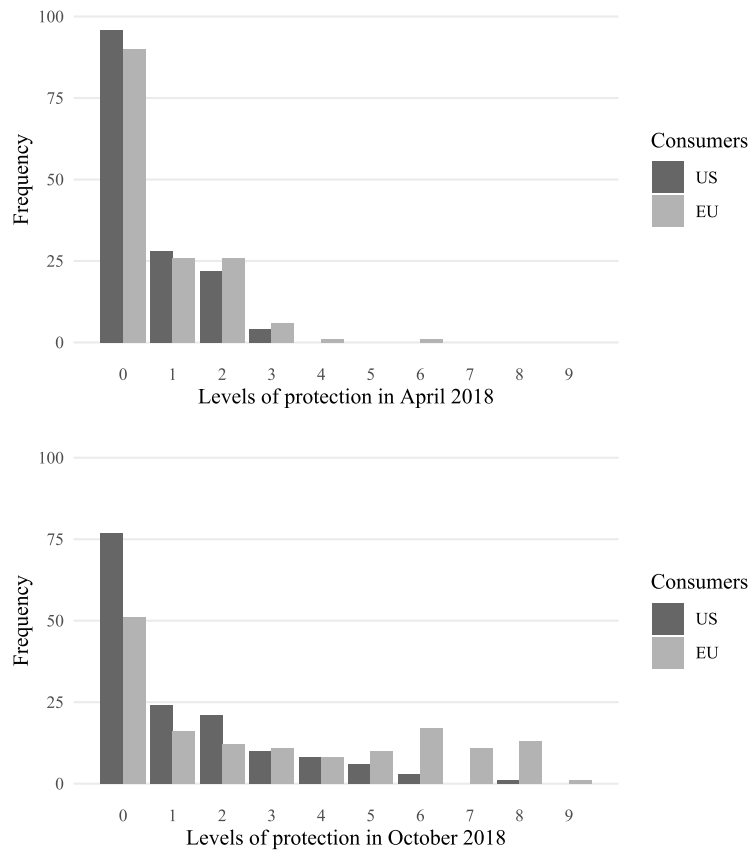


Notes: Histograms depicting the distribution of compliance scores (*compl_EUcust*) for EU privacy policies. The upper panel reports scores for privacy policies in use on April 2, 2018. The lower panel reports scores for privacy policies from October 1, 2018. Values further to the right indicate a higher degree of GDPR-compliance.

Figure 7 reports GDPR compliance for U.S. websites. Consider first the dark grey bars. These plots report the level of protection that U.S. consumers enjoyed under the respective privacy policy. The level of protection enjoyed by U.S. consumers increased somewhat between April 2018 and October 2018. Forty-four out of 150 websites increased the level of protection offered to U.S. consumers, while 10 websites reduced the level of protection. These changes are substantial enough that they cannot be explained by chance.¹⁷⁰ Yet only a small minority of websites (10, or 6.7%) complied with more than half of the requirements of the GDPR captured by the coding scheme.

170. A t-test yields a p-value of <.0001.

Figure 7: Compliance Scores for U.S. Websites



Notes: Histograms depicting the distribution of compliance scores for U.S. privacy policies. Dark grey bars report compliance vis-à-vis U.S. consumers (*compl_UScust*), light grey bars compliance vis-à-vis EU consumers (*compl_EUcust*). The upper panel reports scores for privacy policies in use on April 2, 2018. The lower panel reports scores for privacy policies from October 1, 2018. Values further to the right indicate a higher degree of GDPR-compliance.

At the same time, the level of protection afforded to EU consumers visiting the same websites (depicted as light grey bars) changed to a much larger degree. In October 2018, a substantial share of privacy policies (52 websites or 34.7% of the sample) had a policy in place that complied with the majority of requirements captured by the coding scheme. This result also suggests that numerous U.S. websites assumed that they would fall under the scope of the GDPR (at least insofar as they dealt with EU consumers).

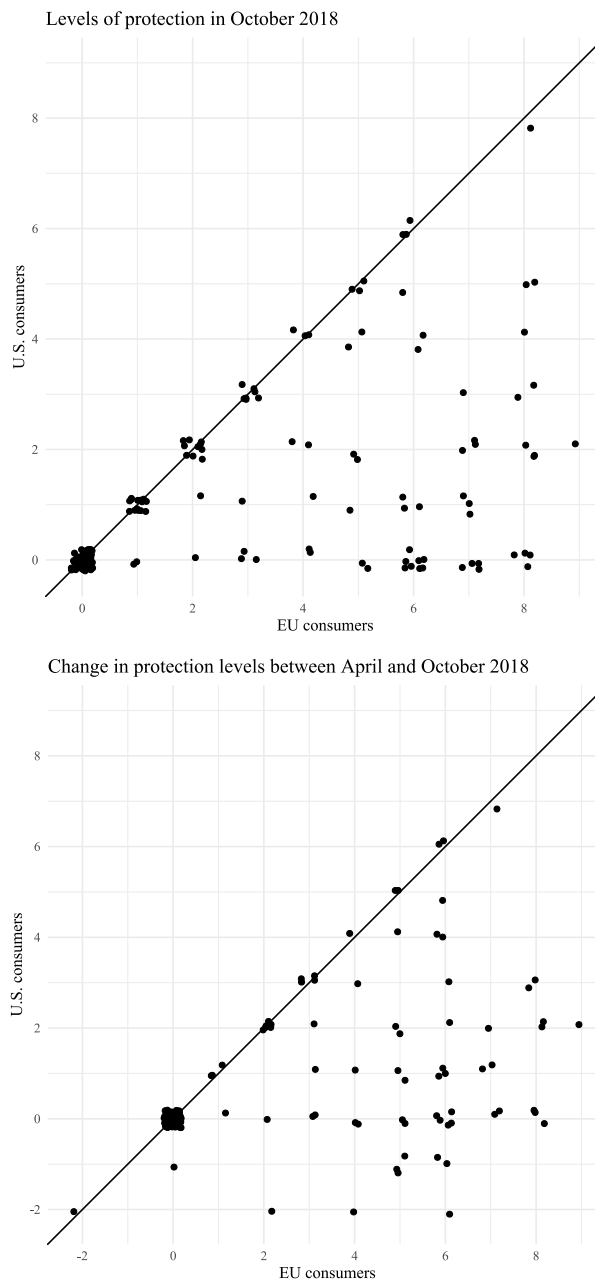
The differences in protections granted to EU consumers and U.S. consumers were substantial. Figure 8 reports a comparison of the levels of protection offered by U.S. websites to U.S. and EU consumers. Each point represents one service provider. The upper panel reports absolute levels of

protection offered in October 2018; the lower panel reports changes in levels of protection between April 2018 and October 2018. In both panels, the x-axis depicts the websites' promised treatment of EU consumers, the y-axis the protections promised to U.S. consumers. Overall, in October 2018, 58 out of 150 U.S. privacy policies established a preferential treatment of EU consumers. The mean *compl_EUcust* score for U.S. websites was 2.98, the mean *compl_UScust* score 1.23. A paired samples Wilcoxon test indicates that these differences are statistically significant, with a p-value of <.0001.¹⁷¹

These results confirm that most U.S. websites that changed their treatment of EU consumers in the wake of the GDPR's entry into force did not treat consumers in all jurisdictions identically. By contrast, most websites that introduced stronger privacy protections between April 2018 and October 2018 took active measures to differentiate between consumers in different jurisdictions and ensure that consumers outside the EU would not profit from the stringent privacy protections introduced in the GDPR.

171. Because the distribution of the difference between the protection levels is not normal, a Wilcoxon test is more appropriate than the standard t-test. A paired t-test also yields a p-value of <.0001. Tests for the differences between the changes in protection levels yield similar results.

Figure 8: Protection Levels for U.S. and EU consumers



Notes: Scatterplot showing the levels of protection offered by U.S. websites to U.S. consumers (y-axis) and EU consumers (x-axis) in October 2018 (upper panel) and the changes between the levels of protection from April to October 2018 (lower panel). Each point represents one service provider.

3. Determinants of Global Compliance

While the results above suggest that only a minority of U.S. websites started offering GDPR-style privacy protections to U.S. consumers after the entry into force of the GDPR, it offers only limited insights into the mechanisms at work. In particular, the analysis does not, on its own, allow for the conclusion that CBCEs are absent from data privacy law. Some online services in the sample did extend the protections introduced in the GDPR to consumers in the United States. Is it possible that these online services faced differentiation costs that were higher than those of other websites?

In this part of the analysis, I shed some light on this question. To do so, I use regression analysis to analyze which website characteristics predict the adoption of a more GDPR-compliant privacy policy that applies equally to consumers in the United States and the EU. My dependent variable is a dummy variable capturing whether a website offered the same privacy protections to consumers in the United States and the EU in October 2018. I restrict the sample to all U.S. websites that introduced stronger privacy protections (for any type of consumer) to their privacy policies between April 2018 and October 2018 (N = 70).

In the analysis, I focus on two variables. The first variable is *Pct_EU_Users*, a measure of the share of visitors accessing a website from the EU. As discussed above, if CBCEs are at play, organizations that do a lot of business in a high-standard jurisdiction are more likely to apply the rules of this jurisdiction globally than others.¹⁷² Therefore, if costs of differentiation are responsible for the global adoption of GDPR-compliant privacy policies, we would expect the probability of the adoption of such a policy to increase with the share of consumers accessing the website from the EU.

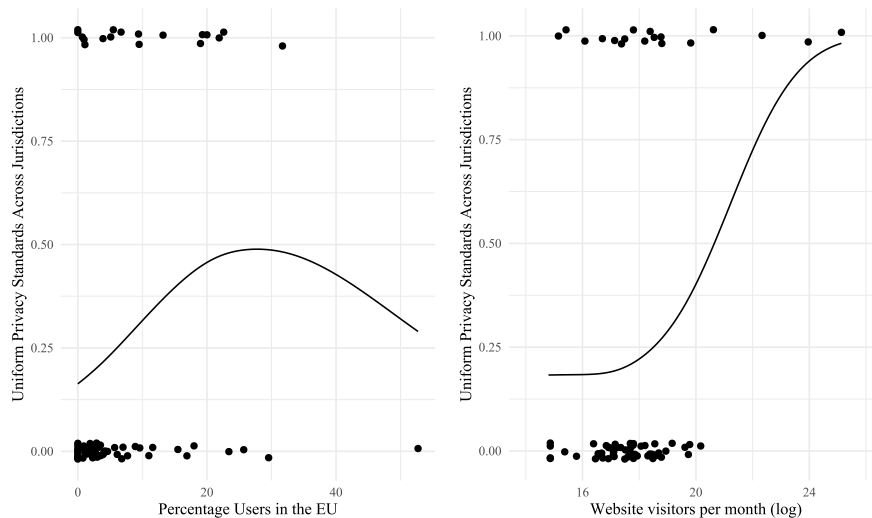
The second variable is *Log_Total_Users*, the average number of monthly visits to the website. Suppose global compliance is mainly due to CBCEs, and some of the costs of applying different standards of protection across jurisdictions are fixed costs. In that case, larger websites should more easily be able to treat consumers in different jurisdictions differently. For example, consider that holding consumer data apart might require companies to develop systems that document where the data was obtained. For small companies, these investments might not be worth the costs, because the potential benefits from processing the data of consumers from low-standard jurisdictions without constraints are comparably small. By contrast, bigger companies might more easily be able to make this investment. Accordingly, the probability of adopting a uniform GDPR-compliant privacy policy should decrease with the number of visitors to a website.

Figure 9 shows the relationship between these two variables and my dependent variable, the adoption of a uniform privacy policy with a higher level of protection than the one in place before the entry into force of the GDPR. In

172. See *supra* Section I.A.2.

both panels, each website is represented by a black dot. The y-axis represents the (jittered) dependent variable. The x-axis of the left panel shows the percentage of website visitors from the EU. The right panel displays the total number of website visitors per month.

Figure 9: Website Characteristics and Uniform Privacy Standards



Notes: Predictors of the adoption of a uniform privacy policy in October 2018 for all websites that adopted more protective privacy policies between April 2018 and October 2018 ($N = 70$). Websites are represented by black dots. y-axis: dummy variable for whether the privacy policy granted the same rights to U.S. consumers and EU consumers. x-axis: percentage of users in the EU (left panel); logarithmic version of the number of website visitors per month (right panel). Black lines: predicted probabilities obtained from smoothing splines.

Several results are immediately apparent. First, none of the variables predicts the global application of EU privacy rights perfectly. For example, one can find both websites with very few and substantial numbers of visitors from the EU among the websites that extend EU-style privacy rights to U.S. customers. Second, both measures are positively correlated with the dependent variable. This result is particularly surprising for the number of website visitors. As described above, if differentiation costs were a major factor in the adoption of globally compliant privacy standards, one would expect to see a higher share of adopters among the smaller websites in the sample. Figure 9 indicates that the opposite is the case. The more visitors a website has, the more likely it is to extend EU-style privacy rights to consumers from other jurisdictions.

I next use regression analysis to investigate the relationship between these variables more closely. In addition to my variables of interest, I include a categorical variable that captures the industry in which the website is active. I

estimate all regressions using both linear probability (ordinary least squares) and probit models. I also estimate a probit model that uses a “Heckman correction” to deal with potential concerns about selection effects.¹⁷³ Table 1 reports results.

Table 1: Regression Analysis

	Dependent variable: binary variable indicating global adoption of GDPR-compliant privacy policy								
	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)
	OLS	OLS	OLS	OLS	Probit	Probit	Probit	Probit	Probit+ Heckman
<i>Pct_EU_Users</i>	.009 (.194)	-	.007 (.316)	.003 (.556)	.026 (.154)	-	.021 (.264)	.009 (.601)	.002 (.906)
<i>Log_Total_Users</i>	-	.057** (.003)	.051* (.012)	.071** (.001)	-	.209* (.016)	.195* (.030)	.314** (.007)	.290* (.022)
<i>Category:</i>									
<i>Computers & Technology</i>	-	-	-	-.110 (.364)	-	-	-	-.524 (.225)	-.508 (.229)
<i>Dating & Adult</i>	-	-	-	.450* (.030)	-	-	-	1.52* (.013)	1.36* (.040)
<i>E-Commerce</i>	-	-	-	-.036 (.894)	-	-	-	-.225 (.769)	-.153 (.833)
<i>Education</i>	-	-	-	-.124 (.548)	-	-	-	-.318 (.680)	-.238 (.741)
<i>Entertainment</i>	-	-	-	-.118 (.442)	-	-	-	-.261 (.622)	-.290 (.563)
<i>_Intercept</i>	.190** (.004)	-.746* (.027)	-.702* (.046)	-.989** (.006)	-.863*** (.000)	-4.39** (.006)	-4.32* (.010)	-6.31** (.004)	-5.42* (.045)
<i>N</i>	70	70	70	70	70	70	70	70	70

Notes: p-values based on robust standard errors included in parentheses. p < 0.05, **p < 0.01, *** p < 0.001.

Table 1 shows that the relationship between the share of users in the EU and the dependent variable is not statistically significant. Moreover, the coefficient’s size decreases substantially when additional variables are included in the analysis.¹⁷⁴ By contrast, the relationship between the number of users and

173. To understand these concerns, recall that I use only those websites that introduced additional privacy protections between April 2018 and October 2018 in the analysis. As a result, the sample used in the analysis does not constitute a random subsample of all policies, giving rise to potentially biased results.

174. This result persists when various transformations of the variable are used.

the adoption of global privacy standards is significant across specifications and changes comparably little with the inclusion of additional variables.¹⁷⁵

These results raise doubts about the importance of differentiation costs in bringing about the global application of the GDPR. There is no evidence of a systematic relationship between the share of users in the EU and the global adoption of a (more) GDPR-compliant privacy policy. Furthermore, contrary to what one would expect if CBCEs were at play, bigger websites are considerably more likely to treat consumers in different jurisdictions alike than smaller websites.

4. Other Potential Explanations

If the global adoption of GDPR-compliant privacy policies is not primarily driven by differentiation costs, what explains this phenomenon? The analysis above allows for some preliminary insights into potential alternative explanations.

First and foremost, the results seem to suggest that consumer demand plays a major role in the decision by some services to extend GDPR-style privacy rights to consumers in other jurisdictions. Most importantly, the analysis reveals that websites in the Adult & Dating category are substantially more likely to adopt GDPR-compliant privacy policies on a global level than other websites.¹⁷⁶ There is little reason to believe that websites in this category face higher differentiation costs than other websites. Instead, as others have argued, it seems reasonable to assume that consumers are more likely to use these services if they trust their privacy protections.¹⁷⁷ Therefore, it seems plausible to assume that these services adopted GDPR-compliant privacy policies to signal high standards of privacy protections to their customers.

The positive relationship between the number of visitors to a website and the probability of the global adoption of a GDPR-compliant privacy policy presents a bigger puzzle. One potential explanation also points to consumer demand: maybe consumers worry more about the treatment of their personal data by organizations they perceive as powerful. If this conjecture is right, the voluntary adoption of more stringent privacy protections might allow these organizations to increase demand for their products, while similar decisions

175. The size of this effect is also substantial. According to the model estimates in Column (9), an average e-commerce website in the baseline category with 10% users in the EU and a number of monthly visitors at the upper end of the first quartile (~22.1M visitors) is predicted to adopt a global, GDPR-compliant privacy policy with a probability of ~23.5%. A similar website with a number of visitors at the upper end of the third quartile (~113M visitors) does so with a probability of ~40.2%.

176. The analysis suggests that the differences between websites in this group and other websites are substantial. To understand the magnitude of the predicted effect, consider again a website with a 10% share of EU users and an average number of visitors per month of 22.1 million. As described above, an e-commerce website with these characteristics would be predicted to adopt a GDPR-compliant privacy policy with a probability of ~23.5%. *See supra* note 175. By contrast, a dating website with similar characteristics would adopt such a privacy policy with a probability of 80.6%.

177. *See* Davis & Marotta-Wurgler, *supra* note 87.

would not entail any increased demand for the products offered by smaller online services.

Alternatively, it also seems possible that major online services adopted purportedly GDPR-compliant privacy policies everywhere to deflect regulatory scrutiny by government agencies in other jurisdictions, particularly in the United States. The business practices of companies like Google and Facebook have come under increased public scrutiny in recent years. One hotly debated topic is whether additional privacy protections are needed in the United States to protect consumers in their interactions with these services. Against this background, the decisions by these services and some of their prominent peers to extend GDPR-style privacy protections to consumers in the EU could have been an attempt to convince regulators and the public that such additional regulation is unnecessary.

D. Interpretation and Limitations

Overall, the analysis suggests that the GDPR's influence on U.S. businesses' operations outside the EU is limited. The privacy policies of a sizeable share of U.S. websites showed no attempt by service providers to become GDPR-compliant at all. Even among U.S. websites that changed their data practices in response to the entry into force of the GDPR, most limited the bulk of privacy protections to customers located in the EU. Furthermore, the apparent ease with which many businesses differentiate between consumers in different jurisdictions suggests that CBCEs were not a major factor in the decisions by some online services to adopt GDPR-compliant privacy policies on a global level.

One might wonder whether this finding matters much, given that four out of the five biggest online service providers were among those that opted for global compliance with the GDPR. However, even for these businesses, the fact that differentiation between consumers in different jurisdictions appears technically and economically feasible makes a difference. Most importantly, this finding raises questions about the sustainability of the commitment of these websites to extend GDPR-style protections to all consumers worldwide. For example, it seems possible that the introduction of additional privacy protections in the EU could further increase the added costs of global compliance, thereby tipping the balance in favor of differentiation for those websites as well.¹⁷⁸ Also, if CBCEs do not dictate global compliance, even websites whose privacy policies promise to treat all consumers the same might in practice have slightly different privacy practices for consumers inside and outside the EU.¹⁷⁹

178. The example of Airbnb's introduction of limits on the rights to request deletion of personal data suggests that this is more than a theoretical possibility. *See supra* Section IV.C.2.a.

179. One example of such a differential treatment despite a uniform privacy policy is Facebook's decision to automatically turn on its facial recognition feature for consumers outside the EU. *See supra* note 122. Of course, insofar as this differential treatment is inconsistent with a service's privacy policy, the online service provider risks becoming the subject of an FTC enforcement action.

The results of this study are limited in important ways. The analysis focuses exclusively on protections reflected in the texts of privacy policies, with a particular focus on provisions that endow consumers with enforceable rights vis-à-vis the business (for example, the right to request deletion of one's data).

As a result of this approach, the analysis might miss some of the GDPR's effects on the levels of privacy protection enjoyed by U.S. consumers. This is because it is arguably relatively easy for service providers to restrict rights, such as the right to request data deletion, to consumers in certain jurisdictions. Insofar as the GDPR required businesses to make other changes to their privacy practices, it might have been more costly for them to treat consumers in different jurisdictions differently. In particular, the benefits of changes that require modifications to a website's structure or design are likely harder to restrict to a subgroup of consumers. One potential example of such a change to a website's structure concerns the reliance on third-party providers, which reportedly decreased globally following the entry into force of the GDPR.¹⁸⁰ Arguably, it is impossible to measure the full extent of such effects by studying privacy policies.

Another limitation of this study is that it focuses exclusively on developments around the time of the entry into force of the GDPR, potentially ignoring at least some of the changes to privacy policies following the law's adoption in 2016. However, the results in Section IV.C.2.b indicate that few, if any, U.S. websites had policies in place before April 2018 that implemented many of the GDPR's requirements. Also, all changes to the privacy policies of major service providers that are usually cited as evidence of CBCEs happened in the weeks preceding the entry into force of the GDPR. Together, these observations might suggest that the GDPR did not significantly affect U.S. online services' privacy policies in the roughly two years following the law's adoption.

V. Implications

A. *Implications for Data Privacy Law*

1. Normative Implications

The evidence obtained above indicates that CBCEs are less common in data privacy law than is often assumed. Here, I address the question of whether this result is good or bad, which is directly related to the more general question about the normative desirability of CBCEs.¹⁸¹

180. Peukert et al., *supra* note 25.

181. By contrast, the existence of California Effects does not have direct legal implications, as there is no rule in international law barring jurisdictions from regulating transactions in situations in which their rules give rise to such effects.

While there is no global multilateral treaty governing questions of jurisdiction, it is commonly assumed that customary international law imposes some limits on jurisdictions' powers to regulate activities taking place elsewhere. *See, e.g.*, RESTATEMENT (FOURTH) OF THE FOREIGN RELATIONS LAW OF THE UNITED STATES, § 407 (AM. L. INST. 2018). However, these limits are comparably lax. *See*

There are striking differences in observers' views on the normative desirability of CBCEs. Many view this phenomenon as inherently problematic because other jurisdictions' rules de facto govern activities taking place in one jurisdiction.¹⁸² By contrast, much of the literature on "California" and "Brussels Effects" paints this phenomenon in a more positive light. For example, Bradford acknowledges that CBCEs might undermine "the ability of foreign governments to serve their citizens in accordance with their democratically established preferences."¹⁸³ Nevertheless, she argues that CBCEs do not necessarily thwart the democratic process elsewhere, because they might override rules that "are too permissive, too weakly enforced, or otherwise suboptimal."¹⁸⁴

As these views suggest, there is no easy answer to the question of whether CBCEs are normatively desirable. As I argue below, the answer to this question ultimately depends on assumptions about the capacity of the political process in different jurisdictions to produce rules that conform with the preferences of their citizens (or meet certain objective standards such as efficiency). In short: those who consider data privacy rules adopted in most jurisdictions as inefficiently lax might lament the absence of CBCEs; others should view this outcome more positively.

Perhaps the most important reason to be skeptical about CBCEs is their potential to work against some of the most important benefits of decentralized rulemaking. Mandatory laws invariably impose costs on some actors, and members of a population will almost always disagree about whether the benefits of a mandatory rule outweigh its costs. Whenever the preferences of discernible subpopulations differ, it can make sense to implement different rules for these

Goldsmith, *supra* note 10, at 1219 ("In contrast to the domestic interstate context, customary international law imposes few enforceable controls on a country's assertion of personal jurisdiction, and there are few treaties on the subject."). Jurisdictions can impose rules on activities as long as there is "a genuine connection between the subject of the regulation and the state seeking to regulate." RESTATEMENT (FOURTH) OF THE FOREIGN RELATIONS LAW OF THE UNITED STATES, § 407 (AM. L. INST. 2018); *see also* Jack Goldsmith, *Unilateral Regulation of the Internet: A Modest Defence*, 11 EUR. J. INT'L L. 135, 138 (2000) ("It is well accepted today that international law permits a nation to regulate the harmful effects of foreign conduct."). The fact that the same activity also falls under other jurisdictions' laws does not render the exercise of jurisdiction by the first state illegal, even if laws impose contradictory requirements on actors. *See* RESTATEMENT (FOURTH) OF THE FOREIGN RELATIONS LAW OF THE UNITED STATES, § 407 cmt. d (AM. L. INST. 2018). *But see id.* § 403 cmt. e. (stating that jurisdictions whose regulations conflict with those of other jurisdictions must take into account the latter's interests and potentially modify or abandon their regulatory efforts).

Further limits on the regulation of commercial activity can follow from areas such as trade law. While the details differ depending on the kind of products and regulations at issue, trade law focuses on national measures that discriminate against foreign products or services. *See, e.g.*, General Agreement on Tariffs and Trade 1994 arts. 1, 2, Apr. 15, 1994, 1867 U.N.T.S. 187; General Agreement on Trade in Services (GATS) arts. 2, 17, Apr. 15, 1994, 1869 U.N.T.S. 183. The mere fact that one jurisdiction imposes stricter standards on products or services than other jurisdictions in which the same products or services are sold, by contrast, does not usually constitute a violation of international trade law. For a detailed analysis of whether earlier versions of EU privacy law complied with international trade law, *see* Shaffer, *supra* note 49, at 46-55.

182. *See* Goldsmith, *supra* note 10.

183. BRADFORD, *supra* note 9, at 250.

184. *Id.* at 251.

subpopulations that reflect their respective preference distributions.¹⁸⁵ Besides, the costs and benefits of regulation can vary depending on the circumstances under which these laws apply, providing another justification for applying different rules to different subpopulations.¹⁸⁶

Decentralized decision making might offer other benefits as well.¹⁸⁷ In particular, variation in rules can be valuable because it provides an opportunity to learn about the effects of different types of rules.¹⁸⁸

In the presence of CBCEs, many of these benefits are weakened or disappear altogether, because the effects of rules are not limited to the jurisdiction that adopts them. As a result, decentralization cannot ensure that the rules that effectively apply in a jurisdiction correspond to the local population's preferences.¹⁸⁹

However, CBCEs may be beneficial in other circumstances.¹⁹⁰ The first scenario concerns situations in which the political process everywhere tends to produce rules that are not sufficiently protective of vulnerable actors. In this case, the inherent tendency of CBCEs to promote rules that set high standards of

185. Revesz, *supra* note 64, at 536.

186. *Id.* at 536-37. In principle, these benefits do not depend on the decentralization of political authority. In practice, however, the ability of central authorities to apply different rules to different subpopulations is limited. Maybe the most important reason for this is that central authorities usually do not have the information needed to customize rules to local populations' preferences. Therefore, it is reasonable to assume that the decentralization of political authority often constitutes a precondition for reaping many benefits of variation in rules.

187. See, e.g., Michael L. Livermore, *The Perils of Experimentation*, 126 YALE L. J. 636, 645-46 (2017) (providing an overview of various justifications for decentralization).

188. Justice Brandeis famously compared states to laboratories which can "try novel social and economic experiments without risk to the rest of the country." *New State Ice Co. v. Liebmann*, 285 U.S. 262, 311 (1932) (Brandeis, J., dissenting). Additionally, citizens might have more opportunities to participate in debates about rules that affect them. See Robert O. Keohane, Stephen Macedo & Andrew Moravcsik, *Democracy-Enhancing Multilateralism*, 63 INT'L ORG. 1, 8 (2009); Pascal Langenbach & Franziska Tausch, *Inherited Institutions: Cooperation in the Light of Democratic Legitimacy*, 35 J.L. ECON. & ORG. 364 (2019).

189. See BRADFORD, *supra* note 9, at 247 ("In particular, many consumers in developing country markets likely view the trade-off between product safety and cost differently than Europeans but are denied these preferences when the Brussels Effect steers companies toward more stringent regulation also in those markets.").

These issues are aggravated by the tendency of CBCEs to support rules that are systematically biased towards more stringent standards. From the viewpoint of public-choice theory, regulatory standards should (and tend to) be chosen so that they lie near the middle of the distribution of preferences of a population (more precisely, under stylized assumptions about the rulemaking process in democracies, regulatory standards will usually be set at the median voter's preferences). As described above, CBCEs compel actors to conform, at a minimum, with the rules which impose the most stringent requirements on the activity at hand. *Supra* Section I.A.1.b. This promotion of comparably extreme rules across jurisdictions appears problematic because these rules will often be further away from the middle of the distribution than more moderate rules. For advocates of theories that view efficiency as the goal of rulemaking, selecting outlier rules usually leads to bad outcomes whenever it can be assumed that rulemakers in different jurisdictions all strive to meet that standard, but fail because of uncertainty.

190. The arguments presented above implicitly rely on the assumption that individual jurisdictions' political process is—at least in principle—unbiased. In other words, they assume that, in the absence of California Effects, the rules of a jurisdiction in expectation meet certain standards, either corresponding to a measure of the distribution of preferences in the population (in the case of public choice theory) or converging towards an objective measure such as efficiency. In reality, this assumption is often unwarranted.

protection can act as a healthy counterweight to deficiencies in the political process. The tendency of the political process to undershoot the desirable standard of protection may, for example, be due to the fact that vulnerable actors' interests are less concentrated than their counterparties' interests.

A second, related scenario concerns situations in which the political process in some (but not all) jurisdictions is biased in a way that leads to inefficiently low protection levels. In these situations, CBCEs can promote the transjurisdictional application of rules originating in jurisdictions that do not suffer from similar problems.

What do these considerations imply for data privacy law and the finding that CBCEs are limited? The GDPR is no exception to the rule that mandatory regulations are almost always controversial. Numerous observers see a need for regulatory intervention in the field of data privacy,¹⁹¹ and the GDPR is usually viewed as the world's most important—and influential—privacy regulation.¹⁹² At the same time, commentators denounce the high costs of compliance and the alleged impact on innovation and competition.¹⁹³ Given these tradeoffs, it seems at least possible that the population in some jurisdictions would favor a different data privacy regime over a GDPR-like model. Notably, even some commentators who view the GDPR positively question whether its regulatory approach would be appropriate for jurisdictions like the United States.¹⁹⁴ Accordingly, one might consider the finding that the ability of the EU to unilaterally export its regulatory model to the rest of the world is limited good news.

Having said that, it also does not seem far-fetched to assume that the political process in many jurisdictions will often fail to generate data privacy rules that offer adequate protection to consumers. Data privacy law is concerned chiefly with conflicts of interests between consumers and businesses, and businesses' interests are often much better represented in the political process than consumers'. In her defense of the "Brussels Effect," Bradford makes a similar argument specifically concerning the protection of U.S. consumers. As she writes, "[t]he Brussels Effect may . . . have the effect of balancing the alleged overrepresentation of business interests in American public life by empowering

191. See Alessandro Acquisti, Curtis Taylor & Liad Wagman, *The Economics of Privacy*, 54 J. ECON. LIT. 442 (2016) (providing an overview of the economic literature on data privacy).

192. Schwartz, *supra* note 81, at 777 ("[T]here is agreement in the academic literature about the pathbreaking impact of EU privacy law."); see also Michal S. Gal & Oshrit Aviv, *The Competitive Effects of the GDPR*, 16 J. COMPETITION L. ECON. 349, 351 (2020) ("The importance of the GDPR cannot be overstated.").

193. *Id.* at 380-90; Damien Gerardin, Theano Karanikioti & Dimitrios Katsifis, *GDPR Myopia: How a Well-Intended Regulation Ended up Favouring Large Online Platforms— The Case of Ad Tech*, 17 EUR. COMPETITION J. 47 (2021); Smith, *supra* note 7. An emerging stream of empirical studies lends support to these claims. See James E. Bessen, Stephen Michael Impink, Lydia Reichensperger & Robert Seamans, *GDPR and the Importance of Data to AI Startups* (Sept. 10, 2020) (unpublished manuscript), <https://papers.ssrn.com/abstract=3576714> [<https://perma.cc/U76N-MR7Y>]; Rebecca Janssen, Reinhold Kesler, Michael Kummer & Joel Waldfoegel, *GDPR and the Lost Generation of Innovative Apps* (Feb. 8, 2021) (unpublished manuscript), https://conference.nber.org/conf_papers/f146409.pdf [<https://perma.cc/7BAV-JWNP>]; Peukert et al., *supra* note 25.

194. See Woodrow Hartzog & Neil Richards, *Privacy's Constitutional Moment and the Limits of Data Protection*, 61 B.C. L. REV. 1687 (2020).

consumers.”¹⁹⁵ According to this line of reasoning, the global application of the GDPR might be considered the lesser of two evils: even if other jurisdictions’ populations, in theory, preferred a data privacy regime that does not follow the GDPR’s model in every respect, in practice they would still prefer the GDPR over the data privacy regime adopted in their jurisdiction as a result of a flawed political process. Then, the absence of CBCEs in data privacy law might be considered lamentable.

2. Policy Implications

The absence of widespread CBCEs in data privacy law also has important implications for policymakers and privacy advocates in the United States.

First, the presence or absence of CBCEs affects U.S. policymakers’ ability to regulate data privacy law in accordance with local preferences. If CBCEs compelled most major online service providers to comply with EU law globally, legislative initiatives in data privacy would face important constraints. Were a proposed law to fall short of the protections of the GDPR, online service providers with operations in the EU would be compelled to comply with the GDPR everywhere. As a result, policymakers seeking to adopt a regulatory model different from that of the GDPR could be prevented from doing so, at least insofar as they rely exclusively on national regulatory instruments. In this situation, the most effective way for U.S. policymakers to change the effective standards of protection would often be through international negotiations. By contrast, this Article’s findings suggest that policymakers in the United States face comparably few external constraints in their pursuit of regulatory strategies in data privacy law.

Second, the findings imply that sustainable changes in data privacy practices in the United States will likely only come about due to domestic economic and political forces, not actions in other jurisdictions. It seems hard to imagine a setting in which the data privacy law of another jurisdiction would have had a better chance to influence U.S. businesses’ global data practices than the GDPR. Apart from the United States, the EU is commonly regarded as the most potent regulator capable of affecting major businesses’ global operations.¹⁹⁶ The GDPR also has a broad geographical scope, applying to all businesses that target consumers in the EU irrespective of where a business is based. Nevertheless, the Article’s analysis shows that the GDPR had only limited effects on the relationship between U.S. online service providers and their customers in the United States.

Third, the findings also have potential implications for the impact that legislative and regulative initiatives at the U.S. state level will have on the privacy protections enjoyed by consumers across the United States. In principle, CBCEs could occur at the interstate level in the United States, making the most

195. BRADFORD, *supra* note 9, at 250.

196. *See id.* at 31-37.

stringent data privacy law in any state the *de facto* law of the land. In fact, when the CCPA entered into force in January 2020, observers predicted that companies would extend CCPA-style protections to all U.S. consumers.¹⁹⁷ However, the costs of differentiating between consumers in different U.S. states would need to be substantial for that to happen. Given the apparent ease with which many businesses differentiate between customers in different countries, it seems at least possible that businesses will also find it worthwhile to treat customers in different states differently.

3. The Role of the EU

Finally, the findings also have implications for our understanding of the EU's role in data privacy law worldwide. As described above, while observers mostly agree that EU data privacy law has influenced data privacy law on a global level, there is less agreement about the mechanisms behind this effect. Some describe the global impact of EU law as a unilateral exercise of power by the EU.¹⁹⁸ According to these accounts, CBCEs are one of the primary mechanisms by which the EU asserts its global influence in data privacy law.¹⁹⁹ Others paint a different picture, describing the spread of EU privacy law as a story of “success in the marketplace of regulatory ideas”²⁰⁰ rather than the result of unilateral action.²⁰¹

The findings in this Article seem to offer some support for the latter camp's position. However, it is important to note that these results do not offer any evidence about other channels through which the EU could have unilaterally imposed its regulatory model on other nations.

B. Implications for Regulatory Interdependence

Besides these implications for data privacy law, the results also have several different implications for the role of traditional national and subnational governance in a globalizing world. The activities of businesses and similar organizations increasingly transcend jurisdictional boundaries, a reality that poses various challenges to the regulatory power of countries and subnational jurisdictions. CBCEs are one of a range of mechanisms that can contribute to this effect.

Against this background, the finding that CBCEs are largely absent from data privacy law suggests that nations—even in an age of incessant globalization—retain important areas of autonomy in which global influences

197. See Hill, *supra* note 37.

198. E.g., BRADFORD, *supra* note 9, at 22-26, 132-55; Christopher Kuner, *The Internet and the Global Reach of EU Law* 15-18, 21 (Univ. of Cambridge Legal Stud. Rsch. Paper Series 24/2017, 2017), <https://papers.ssrn.com/abstract=2890930> [<https://perma.cc/JA6C-HYPM>].

199. E.g., BRADFORD, *supra* note 9, at 142-47.

200. Schwartz, *supra* note 81, at 775.

201. See Schwartz, *supra* note 77; Schwartz, *supra* note 81; Schwartz & Pfeifer, *supra* note 79.

are constrained. This finding is particularly noteworthy for at least two reasons. First, data privacy law is an area where the existence of widespread CBCEs has often been treated as a given.²⁰² And second, traditional jurisdictional boundaries appear particularly porous for online services.

At the same time, the implications of this case study are also limited. Most importantly, the finding that CBCEs are less common in data privacy law than expected appears to say little about the prevalence of these effects in other legal areas. In particular, the costs of differentiation in exchanges involving digital goods or services are likely different from the costs of differentiation in transactions involving physical goods.

Still, this Article's results offer several lessons for our thinking about CBCEs in general. Most importantly, the results provide a powerful confirmation that CBCEs cannot be expected in every situation in which transjurisdictional actors interface with customers in different jurisdictions and in which there appear to be potential cost savings from treating them uniformly. Moreover, the case study also points to potential pitfalls of using anecdotal evidence to support claims about the existence of CBCEs. Anecdotes almost always involve companies or other actors that are in some way unusual, and therefore there is often limited reason to believe that behavior reported in these anecdotes is representative of the behavior of most other actors in the field. Anecdotal evidence might thus convey a misleading picture of the prevalence of CBCEs in other areas as well.²⁰³

Conclusion

Data privacy law is often cited as a prime example of a legal area in which businesses that operate across jurisdictions have to comply with the strictest set of rules everywhere because of an inability to offer differentiated sets of protections to consumers in different jurisdictions. This is one reason why the EU is said to play an outsize role in regulating the data practices of online services worldwide, including in the United States. The results of the analysis in this Article, however, suggest that this form of cross-jurisdictional influence—a “Cost-Based” California or Brussels Effect—is less widespread than is

202. BRADFORD, *supra* note 9, at 142-43.

203. Even in the case of California's role in promoting higher car emission standards across the United States, there are indications that CBCEs might be more limited than some suggest. For example, according to guidance issued by the California Department of Motor Vehicles in January 2020, “many manufacturers make vehicles . . . with smog equipment that meets federal emission standards, but not California standards.” *Fast Facts 29: Buying a Vehicle From Out of State—Can You Register It in California?*, CAL. DEP'T MOTOR VEHICLES (Jan. 2020), <https://www.dmv.ca.gov/portal/file/buying-a-vehicle-from-out-of-state-can-you-register-it-in-california-ffvr-29-pdf> [<https://perma.cc/5DN8-HZHM>]. Heated political battles in other states about the adoption of California-style emission rules similarly suggest that California's rules are not sufficient to induce all car manufacturers to change their production lines for all of the United States. See Danny Hakim, *Battle Lines Set as New York Acts to Cut Emissions*, N.Y. TIMES (Nov. 26, 2005), <https://www.nytimes.com/2005/11/26/nyregion/battle-lines-set-as-new-york-acts-to-cut-emissions.html> [<https://perma.cc/H3SQ-BFPB>]. Tellingly, advocates speculated in 2005 about whether the introduction of similar rules in several additional states might stop producers from producing different cars for high-standard and low-standard states. *Id.*

commonly assumed in the literature. Focusing on changes in the privacy policies of a sample of U.S. websites at the time of the entry into force of the GDPR, this Article documents that most websites do not adjust their policies in a way that would suggest a desire to achieve GDPR compliance everywhere.

This finding has various important implications. For data privacy law, it suggests that accounts describing the EU as the world's privacy cop might be overblown.²⁰⁴ Simultaneously, it exposes the limits of the idea that stringent data protection standards adopted in one jurisdiction can protect consumers in other jurisdictions as well. Advocates of stringent data privacy laws in the United States might view this last result as evidence supporting the adoption of comprehensive, nationwide privacy regulation. Finally, on a more general level, the findings in this Article highlight that nations remain the primary locus for politics and policymaking. While they can be deeply embedded in a global context, they still retain important areas of autonomy in which global influences are limited.

204. See Schwartz, *supra* note 81 (challenging the view that the EU unilaterally imposed its vision of data privacy law on other nations through the so-called adequacy procedure).