PENN STATE
UNIVERSITY PRESS

Measuring the Brussels Effect through Access Requests: Has the European General Data Protection Regulation Influenced the Data Protection Rights of Canadian Citizens?

Author(s): René Mahieu, Hadi Asghari, Christopher Parsons, Joris van Hoboken, Masashi Crete-Nishihata, Andrew Hilts and Siena Anstis

Source: *Journal of Information Policy*, 2021, Vol. 11 (2021), pp. 301-349

Published by: Penn State University Press

Stable URL: https://www.jstor.org/stable/10.5325/jinfopoli.11.2021.0301

REFERENCES
Linked references are available on JSTOR for this article:
https://www.jstor.org/stable/10.5325/jinfopoli.11.2021.0301?seq=1&cid=pdf-reference#references_tab_contents
You may need to log in to JSTOR to access the linked references.

JSTOR is a not-for-profit service that helps scholars, researchers, and students discover, use, and build upon a wide range of content in a trusted digital archive. We use information technology and tools to increase productivity and facilitate new forms of scholarship. For more information about JSTOR, please contact support@jstor.org.

Your use of the JSTOR archive indicates your acceptance of the Terms & Conditions of Use, available at https://about.jstor.org/terms

This content is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License (CC BY-NC-ND 4.0). To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/.

Penn State University Press is collaborating with JSTOR to digitize, preserve and extend access to *Journal of Information Policy*

This content downloaded from
213.61.224.106 on Tue, 26 Oct 2021 12:38:04 UTC
All use subject to https://about.jstor.org/terms

MEASURING THE BRUSSELS EFFECT THROUGH ACCESS REQUESTS

Has the European General Data Protection Regulation Influenced the Data Protection Rights of Canadian Citizens?

René Mahieu, Hadi Asghari, Christopher Parsons, Joris van Hoboken, Masashi Crete-Nishihata, Andrew Hilts, and Siena Anstis

ABSTRACT

We investigate empirically whether the introduction of the General Data Protection Regulation (GDPR) improved compliance with data protection rights of people who are not formally protected under GDPR. By measuring compliance with the right of access for European Union (EU) and Canadian residents, we find that this is indeed the case. We argue this is likely caused by the Brussels Effect, a mechanism whereby policy diffuses primarily through market mechanisms. We suggest that a willingness to back up its rules with strong enforcement, as it did with the introduction of the GDPR, was the primary driver in allowing the EU to unilaterally affect companies' global behavior.

Keywords: Brussels Effect, data protection, right of access to personal data, enforcement, GDPR

The "Brussels Effect" describes a phenomenon where rules set by the European Union (EU) impacts global economic activity and leads to a tangible impact

René Mahieu: Vrije Universiteit Brussel, Belgium

Hadi Asghari: Delft University of Technology, the Netherlands

Christopher Parsons: University of Toronto, Canada

Joris van Hoboken: Vrije Universiteit Brussel, Belgium

Masashi Crete-Nishihata: University of Toronto, Canada

Andrew Hilts: University of Toronto, Canada

Siena Anstis: University of Toronto, Canada

DOI: https://doi.org/10.5325/jinfopoli.11.2021.0301

This work is licensed under Creative Commons Attribution CC-BY-NC-ND

This content downloaded from
213.61.224.106 on Tue, 26 Oct 2021 12:38:04 UTC
All use subject to https://about.jstor.org/terms

on the lives of citizens elsewhere.[1] It is, according to Bradford's seminal article introducing the concept, a form of unilateral regulatory globalization where a single state is able to externalize its laws and regulations outside its borders through market mechanisms, resulting in globalization of standards.[2] Data protection is one of the legal areas that may manifest the Brussels Effect. Scholars and politicians have specifically hypothesized that the EU's General Data Protection Regulation (GDPR)[3] would have such a global effect insofar as companies would adopt global practices paralleling those mandated under it.[4]

The primary mechanism that underlies the Brussels Effect is large international companies' incentives to streamline business operations. Once a multinational company that serves EU citizens brings its practices into compliance with the GDPR, for example by having hired staff, revised internal procedures, and modified technical systems to comply with the Regulation, it will often make economic sense to use the updated procedures and systems globally, instead of running different systems and procedures for different regulatory frameworks. In this case, the company will have adopted the more stringent data protection regulation globally on its own accord.

Against this background, we study global effects of the introduction of the GDPR as a way to empirically test the validity of the Brussels Effect thesis in data protection. Concretely, we study whether the introduction of the GDPR has influenced the compliance of international companies with the data protection rights of residents of Europe and Canada. In particular, we measure the changes in privacy policies (policy level) and the responses to access requests[5] based on the right of access to personal data (procedure and

1. Bradford, 6. There are divergent theories of policy diffusion, one of which being the Brussels Effect theory, and even that theory is understood in divergent ways by different authors. We clarify our understanding of the Brussels Effect theory and the key differences with other theories in the sections "*The Brussels Effect Theory*" and "Other Theories of Policy Diffusion."

2. Bradford, 3.

3. 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] OJ L119/1.

4. Albrecht, a member of European Parliament, serving as the rapporteur for the data protection regulation, and a driving force behind the GDPR, wrote: "it is paramount to understand how the GDPR will change not only European data protection laws but nothing less than the world as we know it."

5. An access request is a request by an individual (a data subject) to have access to data relating to him or her and to information about how an organization is processing that data, based on

This content downloaded from
213.61.224.106 on Tue, 26 Oct 2021 12:38:04 UTC
All use subject to https://about.jstor.org/terms

practice level) by data subjects in the two jurisdictions, before and after the implementation of the GDPR (by comparable companies that operate globally). In terms of cases, we focus on 35 multinational companies in the airline industry or social media sector, which operate in both jurisdictions of study and determine modifications to privacy policies, as well as data access request processes to assess the Brussels Effect. Canada provides a good testing ground for our hypothesis because there were no changes in the federal legal framework applicable to Canadian residents at that time, so any change in companies' behavior toward Canadian citizens cannot be explained by a change in the federal laws applicable to them. Moreover, there is prior empirical research into the compliance with data protection rights in Canada, which allows us to perform a longitudinal analysis.

With this study, we answer the following research questions: Firstly, we ask whether the introduction of the GDPR affected (multinational) companies' data protection behavior toward Canadian citizens who are not formally protected under the GDPR. Secondly, as we find that this is indeed the case, we ask whether the Brussels Effect is likely to have contributed to the changing behavior. Thirdly, we ask which aspect(s) of the GDPR are driving the Brussels Effect.

For this study, we recruited participants in Canada and the EU to submit access requests to these companies in the transition period leading to the GDPR. We compare the responses with the results of 2013 studies on the right of access in both jurisdictions,[6] and build a Bayesian regression model to analyse the changes in response over time between jurisdictions and sectors, and use the results to answer our research questions.

Our article contributes to the state of the art of privacy and data protection scholarship by engaging in the first empirical evaluation of the Brussels Effect by determining the GDPR's influence on businesses' policies and practices, which contributes to scholarly understandings of how policy diffusion takes place and to what consequence. Our research also determines, using a Bayesian regression model, to what extent various factors determine the likelihood that an access request will receive an answer from a company or not. Finally, it shows that the Brussels Effect, as a positive externality of law, depends significantly on the enforcement of EU law to carry forward.

---

the right of access to personal data, which is a cornerstone of data protection law. In this article, we will use the terminologies "access request" and "data access request," but the same right is also commonly referred to as "data subject access request" and "subject access request."

6. Norris et al.; Bennett, Parsons, and Molnar.

This content downloaded from
213.61.224.106 on Tue, 26 Oct 2021 12:38:04 UTC
All use subject to https://about.jstor.org/terms

Understanding whether the Brussels Effect is an important channel for policy dispersion matters: First, while theories that consider international negotiation as the main channel of policy diffusion focus on the diffusion of laws, the Brussels Effect focuses on change in companies' actual behavior. Second, this understanding clearly indicates whether, and under which conditions, legislative change in fact changes behavior. Third, if the Brussels Effect thesis is indeed correct, big economic blocks, such as the EU but also others (e.g., United States, China, and California), have the power to strongly influence corporate behavior on a global scale.

The article is organized as follows: In "Background," we provide an overview of the interlinked histories of data protection laws and theories of policy diffusion. In "Research Methods," we discuss our research setup. In "Findings," we present the empirical results by comparing how companies respond to residents' access requests in both jurisdictions and over time. Finally, in "Discussion: The Brussels Effect," we discuss the findings in light of the Brussels Effect theory of policy diffusion, and conclude.

Background

History of Data Protection Law in EU and Canada

Academic interest in the development of and interrelationship between data protection regulations in different jurisdictions is long-standing. In his 1992 work, Colin Bennett recounts how by the end of the 1960s there was a sharp rise in public policy questions around the processing of personal data by electronic means.[7] According to him, over time, most countries settled on a set of principles on which most data protection legislation was based, through a process of "policy convergence." Several international organizations, most prominently the Council of Europe (CoE) and the Organisation for Economic Co-operation and Development (OECD), contributed to this convergence. The central aim behind the work of these international organizations, and the agreements they reached, was to make sure that countries would not close their borders to the international transfer of personal data.[8] By agreeing on a common standard for data

7. Bennett.

8. Bygrave. The Council of Europe created a Treaty, the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, No. 108, January 28, 1981.

This content downloaded from
213.61.224.106 on Tue, 26 Oct 2021 12:38:04 UTC
All use subject to https://about.jstor.org/terms

protection, countries would be less prone to unduly restrict data transfers with the argument of protecting the privacy of their citizens.

Nevertheless, the convergence on data protection principles did not mean that the level of protection was the same everywhere. To deal with differences within Europe, in 1995, the European Communities enacted the Data Protection Directive (DPD)[9] to harmonize European data protection regimes, and thereby safeguard the free flow of data and a European single market. According to the DPD, all member states had to enact data protection laws that offered the same high level of protection.

The DPD also included rules about the transfer of data to countries outside the EU. According to Article 25 of the Directive, data transfers to third countries were only allowed under the condition that these countries ensured an "adequate level of protection." This requirement put pressure on other countries to create data protection legislation that was in line with European requirements.

Following the introduction of the DPD, many countries outside the EU introduced data protection laws that included specific high data protection standards—similar to those found in the DPD.[10] According to James B. Rule, the desire to receive a so-called "adequacy decision" by the EU was a key concern in drafting Canada's Personal Information Protection and Electronic Documents Act (PIPEDA).[11] As a consequence, Canada's federal data protection law—which was passed in 2000 and has been in effect since January 1, 2001[12]—has many commonalities with the European privacy legislation (a point that will be elaborated on further in the section "Research Methods" of this article). In 2001, the European Commission

This Treaty has recently been amended with the adoption of the Modernised Convention for the Protection of Individuals with regard to the Processing of Personal Data (consolidated text), by the 128th Session of the Committee of Ministers, 17–18 May 2018. The OECD published Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, O.E.C.D. Doc. (C 58 final) (October 1, 1980), which have been revised in 2013 when the OECD Council adopted a revised Recommendation Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data ("Privacy Guidelines").

9. Council Directive 95/46/EC of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L281/31.

10. Greenleaf.

11. Rule, 260; Personal Information Protection and Electronic Documents Act, SC 2000, c 5.

12. Implementation Schedule for the Personal Information Protection and Electronic Documents Act, https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/r_o_p/legislation/02_06_02a/.

This content downloaded from
213.61.224.106 on Tue, 26 Oct 2021 12:38:04 UTC
All use subject to https://about.jstor.org/terms

determined that PIPEDA afforded an adequate level of protection, enabling the flow of personal data between the EU and Canada.[13]

The latest major change in data protection legislation in Europe was the adoption of the GDPR in 2016, and its subsequent coming into force in 2018. The GDPR retains the regulatory framework of the DPD while, nonetheless, representing a major shift in data protection legislation in Europe and beyond.[14] The GDPR was principally meant to further improve the harmonization of data protection in Europe. The main difference between them is that the GDPR is a regulation that, as law, is directly applicable in all member states. While the DPD, as directive, requires member states to individually enact laws on the national level and allows for more differences among various member states. Furthermore, the GDPR aimed to increase the effectiveness of the right to data protection, for example, by strengthening the powers of Data Protection Authorities (DPAs).[15] With the introduction of the GDPR, the Commission also had the explicit intention to affect data protection beyond European borders, stating in its first communication on the need for new legislation that, "A high and uniform level of data protection within the EU will be the best way of endorsing and promoting EU data protection standards globally."[16]

The Brussels Effect Theory

Per Bradford, the "Brussels Effect" is a key policy diffusion mechanism through which European data protection spreads.[17] This form of unilateral regulatory globalization "occurs when a single state is able to externalize its laws and regulations outside its borders through market mechanisms, resulting in the globalization of standards." According to Bradford, there are five conditions that need to be met for the Brussels Effect to occur. First, the jurisdiction must have a *large market* power so that it is not an option for a company to forgo selling its product in that market, and the benefits of accessing the market outweigh the adjustment costs. Second, the jurisdiction

13. COMMISSION DECISION of 20 December 2001 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data provided by the Canadian Personal Information Protection and Electronic Documents Act. https://data.europa.eu/eli/dec/2002/2(1)/oj.

14. Kuner, Bygrave, and Docksey, 3.

15. European Commission, "Safeguarding Privacy in a Connected World," 6.

16. European Commission, "Comprehensive Approach on Personal Data Protection," 19.

17. Bradford, 3.

This content downloaded from
213.61.224.106 on Tue, 26 Oct 2021 12:38:04 UTC
All use subject to https://about.jstor.org/terms

must have the *regulatory capacity* to enforce its rules. This includes having the regulatory expertise to make the rules and the legal authority to enforce them. Third, the regulatory bodies in the jurisdiction must have a *preference for strict rules*, including the will to enforce them. This means that companies can rationally expect that there will be a high cost associated with noncompliance. Fourth, the target of the regulation has to be *inelastic*. That means that the regulation is connected to a target that is fixed in terms of location, such as the consumers that buy a product, so that the producer will not be able to escape its jurisdiction as a consequence of being regulated. Finally, the production process should be *indivisible*, which means that producing different versions of the same good or service comes at a high cost.

The idea that market forces play an important role in the diffusion of European data protection standards is not new.[18] However, Bradford's "Brussels Effect" is a unique contribution. While scholars regularly apply the term Brussels Effect whenever countries enact new privacy laws in order to receive an "adequacy decision,"[19] their interpretations often do not differentiate between the *de facto* and the *de jure* Brussels Effect—an essential distinction in Bradford's analysis. Bradford stresses that the *de facto* Brussels Effect occurs when companies decide to apply the high standards of one jurisdiction (in this case EU's) on a worldwide level, *without* being forced to do so by law.[20] According to her theory, they would do so because once they comply with the rules of the stringent dominant regulator in one jurisdiction, such as the EU's, it is cheaper for them to apply their new way of doing business everywhere. After companies have adjusted their business interests, they may be inclined to lobby for more stringent regulation in their home countries to force their local competitors to incur similar costs. Bradford calls the implementation of new laws in this way the *de jure* Brussels Effect.

Strengthened Enforcement Under the GDPR

Although the requirements of the GDPR are substantially very similar to those under the DPD, the GDPR represents a major shift with regards to *enforcement*. Thus, one of the necessary conditions for the Brussels Effect—a *preference for strict rules*—is only met under GDPR.

---

18. See, for example, Shaffer, published in 2000. Shaffer argues that the EU was able to export its higher data protection standards essentially because of the economic power of the EU countries when they act united.

19. Kuner, "Reality and Illusion"; Burri and Schär.

20. Bradford, 8–9.

This content downloaded from
213.61.224.106 on Tue, 26 Oct 2021 12:38:04 UTC
All use subject to https://about.jstor.org/terms

Under the DPD, enforcement capabilities, as well as potential fines, varied widely across the different member states.[21] Article 24 of the DPD stated that "Member States shall adopt suitable measures to ensure the full implementation of the provisions of this Directive and shall in particular lay down the sanctions to be imposed in case of infringement of the provisions adopted pursuant to this Directive." In practice, most member states had modest maximum fines. Spain and the United Kingdom, which had the highest possible fines, set maximum fines at €600,000 and £500,000, respectively,[22] and the United Kingdom only issued its maximum fine once, in 2018, to Facebook in relation to the Cambridge Analytica scandal.[23]

For several reasons, however, the tendency to use the power to impose administrative fines was overall quite low.[24] The relatively low level of enforcement also applied to failures to comply with access requests. The highest fine levied in practice for noncompliance with an access request in the UK was £15,000, issued in 2019 to Cambridge Analytica. In the Netherlands, up to 2016, the DPA could levy a maximum administrative fine of €4,500, and only for the specific infringement of not registering a processing activity with the authority for which registration was mandatory.[25] For all other offences, such as not responding to an access request, the DPA could only impose a burden under penalty. In such cases, the DPA sanctions the offending organization to change their behavior under the threat of having to pay a fine if the demanded changes are not met within a specified time limit. In 2018, this led to the imposition of a penalty of €48,000 for a bank that did not fully comply with an access request.[26]

PIPEDA's fine regime is even more limited.[27] An update to the law made in 2015—which came into force on November 1, 2018—made it an offence for companies to not inform the Office of the Privacy Commissioner of Canada of data breaches. Still, the Commissioner does not have the ability to issue fines or compel changes in organizational practices in response to such failures. Instead, should a company fail to comply with PIPEDA, the Commissioner may refer information relating to the possible breach of

21. European Union Agency for Fundamental Rights; Golla.

22. Golla. At current exchange rates £500,000 equals roughly €550,000.

23. Information Commissioner's Office (ICO) to Facebook Ireland Ltd., par 10.

24. Golla.

25. College Bescherming Persoonsgegevens, 44; Autoriteit Persoonsgegevens, "Jaarverslag 2016," 42–43.

26. Autoriteit Persoonsgegevens, "TGB betaalt dwangsom na niet voldoen aan inzageverzoek."

27. Lawford.

This content downloaded from
213.61.224.106 on Tue, 26 Oct 2021 12:38:04 UTC
All use subject to https://about.jstor.org/terms

the law to the Attorney General of Canada, who may decide to undertake proceedings against the offending organization.[28] The Attorney General may levy fines up to $100,000 (CAD) for failing to comply with the obligation of data breach notification. To date, no fines have ever been levied on Canadian companies for failing to meet the responsibilities or obligations under PIPEDA.

Under the GDPR, the enforcement capabilities of DPAs have gone up substantially. According to Article 83 of the GDPR, fines of up to €20 million can be levied—or 4% of global turnover—whichever is higher. According to Article 83(5)(b) GDPR, these high-level fines can also be issued if organizations do not comply with obligations regarding the right of access to personal data. This means, for example, that Facebook, with a 2018 revenue of over $55 billion, would now face a maximum potential fine of around €2 billion. Moreover, some DPAs have started to impose higher fines in practice with the United Kingdom's Information Commissioner's Office (ICO) fining British Airways around €20 million,[29] and France's Commission Nationale de l'Informatique et des Libertés (CNIL) fining Google €50 million.[30] A fine of €830 thousand—the highest fine so far for noncompliance with the obligations regarding the right of access—has been given by the Dutch DPA to Bureau Krediet Registratie (BKR), a credit registration bureau.[31]

Related Work

Related Empirical Work

There is extensive previous empirical research into the effect of changes in data protection law on companies' data protection policies, procedures, and practices over time. Davis and Marotta-Wurchter demonstrate that most privacy policies shown to US consumers changed around the introduction of the GDPR; on average, policies became substantially longer, and mention more of the elements required by the GDPR, in particular, about the rights of access and other data subject rights.[32] However, there

28. Office of the Privacy Commissioner of Canada.

29. "ICO Fines British Airways £20m for Data Breach Affecting More than 400,000 Customers."

30. Commission nationale de l'informatique et des libertés. The CNIL fined Google primarily for not providing transparent information in their privacy policies and therefore not having obtained valid consent for ad personalization.

31. Autoriteit Persoonsgegevens, Letter to Bureau Krediet Registratie.

32. Davis and Marotta-Wurgler, 698; See also Linden et al., Section 8. It is interesting to note that these articles do not distinguish between European and American data controllers,

This content downloaded from
213.61.224.106 on Tue, 26 Oct 2021 12:38:04 UTC
All use subject to https://about.jstor.org/terms

have been disagreements on the readability of privacy policies, with Becher and Benoliel finding that English language policies have become more readable—whereas Linden et al. have found the opposite.[33]

There is a long history of empirically assessing compliance with access requests in various countries,[34] and most found that the average quality of responses was low. As far as we know, there are two longitudinal empirical studies that include data from both before and after the introduction of the GDPR. One study of access requests to vendors of popular apps in Germany found that the percentage of sufficient responses went up between the first measurement in 2015 and the second and third in 2018 and 2019.[35] The other is a study that has been conducted in France yearly since 2010, which shows that after the introduction of the GDPR, more requests received a response within the legal time limit, but the percentage of responses that were noncompliant was low (37%) and did not improve in comparison to the previous studies.[36]

There has also been some work on transnational aspects of data access requests. Bennett, Parsons, and Molnar studied the extent to which US-based companies respond to access requests sent by residents of Canada.[37] Norris et al. conducted a large study of over a 100 access requests sent from 10 member states of the EU.[38] In line with prior research, both found significant problems with obtaining access in general, and specifically strong obstacles regarding US-based firms.

Other Theories of Policy Diffusion

Scholars have debated the extraterritorial reach of data protection laws ever since the introduction of the DPD.[39] In addition to the Brussels Effect, other channels of policy diffusion in the area of data protection have been discussed in scholarship as well. Schwartz, for example, argues that EU-style data privacy regulation is spreading throughout the world because the EU

nor between policies specifically shown to American or European residents. The existence of a Brussels Effect seems to be simply assumed.

33. Becher and Benoliel; Linden et al. The differences might be a result of variations in the empirical setup. For example, while Becher and Benoliel look at the top websites from the United Kingdom and Ireland, Linden and others look at the top worldwide websites.

34. For example, Raento; Hoepman; Mahieu, Asghari, and Van Eeten; Parsons, Hilts, and Crete-Nishihata; The Citizen Lab.

35. Kröger, Lindemann, and Herrmann.

36. Association Française des Correspondants à la Données à caractère Personnel.

37. Bennett, Parsons, and Molnar.

38. Norris et al.

39. For example, Bennett and Raab, "The Adequacy of Privacy."

This content downloaded from
213.61.224.106 on Tue, 26 Oct 2021 12:38:04 UTC
All use subject to https://about.jstor.org/terms

engages in bilateral negotiation with other countries. According to him, the EU has a strong negotiation power and lawmakers in other jurisdictions have become convinced that GDPR-like regulation was an appealing proposition "in the marketplace of regulatory ideas."[40] He also argues that the history of negotiations over adequacy decisions show that the EU-like policy is not diffusing through the channels identified by Bradford—companies are changing their policies because of changing laws, not as a result of economic forces.

Others, such as Kuner[41] and Lynskey,[42] argue that European-style data protection regulation is spreading primarily because, ever since the introduction of the DPD, the EU only allows international transfer of personal data to third countries when "adequate" levels of protection can be guaranteed. From this point of view, the introduction of EU-style data protection laws by these countries may be seen as a pragmatic move, necessary to safeguard the interests of safeguarding trade with the EU.

It is undeniable that through various mechanisms, European data protection law has impacted the creation of data protection laws elsewhere. However, we need to be aware that when new data protection regulations are implemented, this does not necessarily mean that companies do indeed implement the necessary steps to comply with the new obligations. Therefore, when evaluating the impact of data protection law, we should carefully distinguish between the legal obligations applying to data controllers and their actual practices. In other words, to assess the disparity between what controllers are required to do by law and what they are actually doing. So far, most authors in the debate on data protection policy dissemination have focused primarily on the dissemination of laws while the question of practical compliance with data privacy laws has been less studied.

Research Methods

High-Level Approach

To test for the Brussels Effect by measuring companies' actual practices, we select requirements of data protection laws *that are measurable/observable,* and check to see:

40. Schwartz, "Global Data Privacy."
41. Kuner, "Reality and Illusion."
42. Lynskey, 42–44.

This content downloaded from
213.61.224.106 on Tue, 26 Oct 2021 12:38:04 UTC
All use subject to https://about.jstor.org/terms

I. If these measurements change as a result of the GDPR coming into force within Europe, which, as we hypothesize, happens given the presence of more substantial fines (i.e., we expect changes in the data protection practices of EU companies to all data subjects, and non-EU companies toward EU data subjects).
II. If we also observe a change in the measurements for data subjects in other jurisdictions where the legal situation has not changed, and which are not legally covered by the GDPR (e.g., we observe changes in data protection practices toward Canadian data subjects by non-EU companies). This change suggests the existence of the Brussels Effect, caused either by some form of organization learning, business streamlining, or other harmonization of data protection practices.

In other words, we treat the policy intervention of the introduction of the GDPR in the EU and the simultaneous nonintervention in Canada as a natural experiment. We assess its impact on companies' compliance with data protection obligations, both at a policy level ("privacy policies") and procedure and practice level (using data access requests) in the two jurisdictions (EU and Canada).[43] We differentiate between these two levels of policy implementation because it allows us to assess to what extent data protection requirements are implemented in the companies' processes. Although updating a privacy policy is a relatively simple task that can be performed by a team of lawyers—and which only expresses companies' intended behavior—responding to access requests requires implementation by the companies and goes beyond mere rewriting of legal texts.

As a proxy for the level of implementation of data protection practices of companies, we, therefore, study their compliance with (and handling of) the right of access to personal data.[44] We use this, firstly, because access is a fundamental part of data protection legislation that enables

43. Data protection consists of a complex set of requirements. Bennett and Raab argue that evaluations of the performance of data controllers should distinguish between *policy*, *procedural,* and *practice* aspects of compliance. The *policy* level consists of a description of data privacy policy practices by lawyers and policymakers that is represented in the privacy policies; this layer is the most easily observable. The *procedural* level consists of the steps that an organization takes to implement the policy decisions expressed at the policy level. The *practice* level consists of the substantive ways in which an organization uses personal data, and is hardest to observe. Bennett and Raab, *The Governance of Privacy*, Chapter 9.

44. In fact, access requests let us observe compliance with data protection requirements externally at all *three levels* mentioned in the previous footnote. At the policy level, a privacy policy may be in line with the current law expressing that data subjects have the right to access their personal data. Next, procedures need to be implemented throughout the company to fulfil

This content downloaded from
213.61.224.106 on Tue, 26 Oct 2021 12:38:04 UTC
All use subject to https://about.jstor.org/terms

many other data subject rights.[45] Secondly, contrary to many other data protection requirements, it is possible to externally observe certain aspects of compliance with this obligation. Thirdly, the right of access is one of the (few) elements of data protection with which we have previous empirical data to compare new results. Consequently, we can use it to monitor changes in the use of personal data over time (in both a longitudinal and cross-sectional manner). In our research setup, we conduct measurements in Canada and the EU in 2018, and use data from Bennett, Parsons, and Molnar, and Norris et al. as comparison points.

The legal requirements pertaining to right of access under PIPEDA, GDPR, and DPD are very similar.[46] Under all laws, data subjects have the right to access (receive a copy) of their personal data from data controllers, as well as to receive supplementary information about its processing—such as the purposes for which this data is used, the recipients, and sources of the data.[47] Minor differences exist with regard to the permissibility of asking fees, the information to be provided (e.g., retention period, right to lodge a complaint), and reasons that companies can use to restrict access.[48] These laws are also generally similar insofar as they apply extraterritorially (see Appendix B for a more detailed discussion). Their obligations apply to companies established in their jurisdiction as well as to all companies that provide services to people in their region, and, therefore, process personal data. Under both the DPD and the GDPR, Europeans generally had the

this policy. At the practice level, access allows data subjects to monitor controllers' compliance with regards to the boundaries on the types of data processing conducted.

45. Ausloos, Mahieu, and Veale, 5.

46. Note that cf. Bennett, *Regulating Privacy* and Fuster, despite the similarities, regions do have different traditions and use different language and definitions. This is reflected, for example, in the fact that in Europe, these laws are generally called *data protection laws* (e.g., DPD and GDPR) and in Canada, they are called *privacy laws*. Moreover, the terminology used in the European and Canadian laws differ: While the GDPR uses the words "data subject," "data controller," and "personal data," whereas PIPEDA uses the words "the organization," "the individual," and "personal information." Under detailed scrutiny, these terms are not exact substitutes. For the purposes of the analysis in this article, these differences between European and Canadian data protection laws are not relevant.

47. PIPEDA Principle 4.9; Article 12 DPD; Article 15 GDPR.

48. We acknowledge that the question of what falls under the scope of "personal data" under GDPR is a question that has been considered by the ECJ several times and is a topic of intense scholarly debate, but a detailed discussion of this falls outside the scope of this article. See, for an in-depth analysis in particular, Purtova, who explains the doctrine developed by Article 29 Working Party: "Information can 'relate' to an individual in content, purpose, or result, meaning that information 'relating to' a natural person includes but is broader than the information 'about' that person." This has, over time, been confirmed by the ECJ. Purtova.

This content downloaded from
213.61.224.106 on Tue, 26 Oct 2021 12:38:04 UTC
All use subject to https://about.jstor.org/terms

right to access personal data held by companies that operate internationally, such as airlines and social media companies. Likewise, Canadians generally had this right with respect to European companies (under the DPD and the GDPR), as well as to non-Canadian companies providing services to people in Canada (under the PIPEDA).[49]

Data Collection

We tested for the Brussels Effect by investigating whether social networks or airlines increased their compliance with the right of access in the EU and Canada since the GDPR transition. We chose companies from these sectors because they have different economical and operational natures, which allows us to study, in addition to our main research question, whether the Brussels Effect is influenced by sectoral differences.

We recruited study participants in both jurisdictions that have ongoing commercial relationships with companies in these sectors. Participants included the authors, colleagues from their respective research centers, and some of their direct acquaintances. Nine participants in Canada and eight participants in the EU participated in this study.[50]

Participants were asked to submit data access requests to a preidentified set of airline and social networking companies. Our participants had relations with 38 of these companies, and we subsequently asked participants to issue access requests based on their interests, with participants being assigned a median of five companies each (to avoid too much workload per participant), and each company being assigned to a median of two participants (and a max of six, to have repeated measurements while not overwhelming any particular company). In total, the participants submitted 80 access requests.

Participants sent a common access request letter, which can be found in Appendix C. The letter invoked relevant data protection legislation, and requested the following from the company: (a) whether the company processes personal data, (b) a copy of the personal data, (c) the sources of the data, (d) the purpose of the processing, (e) the parties to whom the data is disclosed, and (f) the time period for which the data is stored. Requests

49. It must be said however—as we explain in detail in Appendix B—that while under the GDPR the applicability of the rules to foreign companies providing services to people in Europe is very clearly stated in the law, under DPD and PIPEDA it was less clear.

50. This is excluding three participants who dropped out because they did not share their results and/or did not follow the research protocol.

This content downloaded from
213.61.224.106 on Tue, 26 Oct 2021 12:38:04 UTC
All use subject to https://about.jstor.org/terms

also inquired about categories of data specific to each sector. For airlines, the letter asked about flight information, passenger name records, and security screening data. For social media companies, it asked about contacts, geolocation data, and browsing history.[51] We consulted the organizations' privacy policies to find contact information for data protection officers and addresses for submitting access requests in both jurisdictions.[52] Participants included information to help controllers identify them but did not include a government ID with the initial request. If a controller subsequently asked for it, participants complied.

The access requests were sent between April 19th and May 11th 2018. This was just prior to the date that the GDPR came into force. However, since the GDPR was already passed by the EU parliament in 2016, many companies were in the final stretches of organizationally implementing the new requirements, and there is evidence that compliance with access rights was already at GDPR levels at that time.[53] We asked the participants to send a reminder if they hadn't received a response within a month, and to follow-up with a request for clarification if the responses to access were incomplete or unclear. Except for in a handful of cases, communications with controllers continued well after the GDPR enforcement date, with one responding in November 2018.

The final list of companies is presented in Table 4 in Appendix A. The majority of these companies are based in the EU, Canada, and the United States.

Scoring Responses and Regression Analysis

We compared commonalities and differences between responses to Canadian and European requests. For many of the controllers, where we were able to send access requests from both Canadian and European subjects, we conduct a pairwise comparison of the responses.

---

51. Moreover, the letter to social media companies stated: "If your service includes a data download tool, you are free to direct me to it, but ensure that in responding to this letter, you do provide requested data associated with me that is not included in the output of this tool."

52. If no specific address for submitting an access request was mentioned, we sent the request to the general address indicated in the privacy policy, such as the address of the DPO. If no means of communication was mentioned, we submitted the request through general means of communication provided by the company, such as channels for customer service.

53. Kröger, Lindemann, and Herrmann have shown that the level of compliance with access requests in March 2018, just before the introduction of the GDPR, was much higher than in 2016, but also higher than in 2019. Kröger, Lindemann, and Herrmann.

This content downloaded from
213.61.224.106 on Tue, 26 Oct 2021 12:38:04 UTC
All use subject to https://about.jstor.org/terms

To generalize our findings, we distinguished between factors that may influence the outcome of an access request—such as the data controller's sector and location, and the data subject's persistence—as well as whether the GDPR formally applies to the request. For this purpose, we use *Bayesian multivariate logistic regression analysis.*[54] The "multivariate" part controls multiple factors at the same time, the use of Bayesian analysis is more robust with regards to stochasticity[55] and limited numbers of observations.[56]

The "logistic" part means that we evaluate responses in a binary manner—either as success or failure. We adopt a metric developed by Norris et al., where access responses are classified as either *facilitative* or *restrictive*.[57] This metric is more lenient than strictly determining whether a response is compliant or noncompliant, as, for instance, many controllers have delays longer than the legal time frame in responding, and in most cases do not provide a response to all subquestions asked about the processing of the data.

To be able to evaluate the GDPR impact, we need longitudinal data. For this purpose, we supplemented our dataset with data from two earlier studies of access rights in both jurisdictions, Norris et al. for the EU and Bennett et al. for Canada[58] (the regression model will be presented and discussed in the "Findings" section).

Ethical Considerations and Research Limitations

For this research, we followed the protocol approved by the ethics board of Delft University. Under this protocol, participants received a clear explanation of how their personal data would be used, and they were informed

54. *The actual tools we used include Jupyter Notebooks, Python Pandas (v1.1), PyStan (v 2.19), and Arviz (v0.10).*

55. To say that the outcome is stochastic means that there is an element of randomness there. In the case of access requests, controllers do not always send the same response, even when they get exactly the same request. This may, for example, be because processing access requests is not fully standardized in most organizations, or a request letter could get lost in the post.

56. McElreath; Kruschke.

57. Norris et al., 15. The judgment whether a response is facilitative or restrictive is made based on a range of criteria including how timely a company deals with a request, the level of detail of the response, whether their response included distinct answers to the subquestions asked in the requests, and also more subjective criteria such as the tone/helpfulness of the staff.

58. Norris et al.; Bennett, Parsons, and Molnar. The Bennett data we recoded ourselves based on the facilitative/restrictive metric.

This content downloaded from
213.61.224.106 on Tue, 26 Oct 2021 12:38:04 UTC
All use subject to https://about.jstor.org/terms

that they had the right to stop their participation and request that we delete their personal data at any moment and for any reason. During the study, the personal data of participants was stored securely. The number of researchers allowed to access the responses to access requests, which include identifiable data, was limited, and sensitive information was redacted before sharing. Considering the side of the controllers, we acknowledge that responding to access requests imposes a burden. However, given the relevance of the research, particularly given the fact that the right of access is a fundamental right, imposing this burden is deemed justified. In order to protect the privacy of the controller's employees, we do not mention their names.

Limitations: Some caveats on the regression analysis include (1) the general caveat in all quantitative analysis regarding generalizability; we believe our sample is quite representative of the sectors we investigate, as it covers a big share of the market in those sectors; (2) the methods in collecting the data between our study and the prior work are not fully uniform; we have tried to standardize our processes and correct for differences in encoding to the extent possible; and (3) the 2013 Canadian data is limited to only social media firms. Although the regression and sensitivity analysis partially accounts for this, it remains a limitation of data availability. By combining different forms of evidence, we counter some of these limitations and have confidence in the reliability of our main findings.

Findings

Overview

Out of the 80 subject access requests sent by both the European and Canadian participants, around two thirds received a response. Slightly more than half of the responses are "facilitative."

In most cases, the access process took considerably longer than the legally allowed time (approximately one month), with the median number of days to receive a substantive response being around 62 days. Some controllers cited a higher workload than usual (possibly due to extra work generated by the introduction of the GDPR) as reasons for their delay. In other cases, the procedure took longer because the controller didn't return all the information asked for, or because participants took time to provide additional identification as requested, which sometimes took a number

This content downloaded from
213.61.224.106 on Tue, 26 Oct 2021 12:38:04 UTC
All use subject to https://about.jstor.org/terms

of back-and-forths to resolve.[59] In four cases, our participants abandoned their requests once the controller asked for additional verification, and we excluded these requests from our analysis.

Table 1 offers an overview of the quality of responses to access requests by jurisdiction and sector. In light of our research questions, we shall offer an in-depth comparison of the similarities and differences between the Canadian and European responses in the next sections.

TABLE 1 Descriptive Statistics of Access Requests Sent for This Study (in 2018)

Jurisdiction	Sector	Firms	Requests (2018)	Facilitative response (%)	Restrictive response (%)	No. Response (%)
CA	Airlines	14	23	9 (39%)	7 (30%)	7 (30%)
	Social Media	12	21	5 (24%)	7 (33%)	9 (43%)
EU	Airlines	14	15	8 (53%)	2 (13%)	5 (33%)
	Social Media	16	17	5 (29%)	7 (42%)	5 (29%)
Total		**35**	**76**	**27 (36%)**	**23 (30%)**	**26 (34%)**

Qualitative Comparison of Responses

I. ***Pairwise comparison reveals no structural differences between European and Canadian responses***

A pairwise comparison of the responses sent by the same company to Canadian and EU citizens shows that responses are mostly the same[60]:

– Of the 20 companies that received requests from both Canada and Europe, 12 sent the same, or a very similar, response to both.
– In the other eight cases, there was a difference, but these did not point toward a structural difference in the way companies deal with European and Canadian requests.

59. The additional burden for data subjects of having to go through multiple back-and-forths has been discussed by prior research (e.g., Norris et al.; Ausloos and Dewitte; Mahieu, Asghari, and Van Eeten), and as explained in the sections, is one of the elements feeding into the "facilitative" and "restrictive" metric.

60. Appendix A shows for which companies we had responses to both EU and Canada residents. Nineteen out of 20 were not from the EU.

This content downloaded from
213.61.224.106 on Tue, 26 Oct 2021 12:38:04 UTC
All use subject to https://about.jstor.org/terms

– Among these eight cases, the European response was more facilitative in four, while the Canadian response was more facilitative in the other four.

The responses by Google and Microsoft provided an example of these differences in responses, seemingly indicating no structural differences. While Google's response to a follow-up sent to a Canadian requester included an overview of IP addresses, which were associated with logins to its services, this overview was not included in a response to a similar European follow-up request. Responses by Microsoft differed in the opposite direction with the EU response containing an IP-log, which was not provided in response to the Canadian request.

These and other small differences found through pairwise comparison of responses indicate that most controllers use a hybrid system of automated tools and manual intervention by the customer service (or privacy team) employees answering the requests. For example, some responses made clear that responders used semistandard emails but with differences in the order of sentences and small additions to text being included in responses. For example, Snap (the company behind Snapchat) included the sentence "Snap has not had a data breach" and ended with "Hope that helps ☺" only in its response to the EU in letters that were otherwise identical. In other words, with many small differences in the responses, it seems more reasonable to attribute these to the difference in the employee attending to the request, and not to any jurisdictional or sectoral difference.

Besides looking at differences in the substance of the responses, we also noted when responses to access requests contained references to the specific data protection regulations (e.g., GDPR or PIPEDA) as a possible indication for differences on responses based on the residence of the data subject. We found that 12 responses to access requests sent to airlines referred in some way to the specific regulations. These references seem to be merely nominal, however, as there is no relationship between these references and the substantive content of the actual replies.

The response by Cathay Pacific to the EU participant, for example, stated: "We enclose further personal data that you are entitled to pursuant to Article 15 of the GDPR" whereas the response by the same airline to the Canadian participants does not refer to the GDPR, nor to PIPEDA. Substantively, the responses are exactly the same. Meanwhile, the responses by an American airline to a Canadian participant refers to specific paragraphs of PIPEDA that require the company to verify

This content downloaded from
213.61.224.106 on Tue, 26 Oct 2021 12:38:04 UTC
All use subject to https://about.jstor.org/terms

the identity of the requestor and allows for certain restrictions to access while similar provisions are included in the GDPR.

II. ***Sectoral differences: airlines are more facilitative, social media firms prefer download tools***

Overall, the proportion of facilitative responses from airlines was greater than from social media companies. This point can be observed from the overall statistics in Table 1: both in Canada and Europe, the percentage of responses that was facilitative was higher for airlines than for social media companies.

Another clear difference between the sectors is that many social media companies refer to download tools by which data subjects can download their personal data directly from the service's website (or an app).[61] Although none of the airlines offered a download tool, the majority of social media companies did.

III. ***Being a persistent data subject pays off***

Persistence (or stubbornness) of the participants in pursuing their request led to a higher response rate. An example of this is our experience with United Airlines, which did send personal data to the EU participant and not to the Canadian participant. The Canadian participant sent the request to a general information email, and when no response was received, they left it at that. The EU subject was more persistent: He first tried to reach customer care through a web form, finding the functionality to upload .pdf attachments to be broken. Consequently, he sent a message through the web form requesting that another channel for communication of an access request would be provided. In response, he was told to call a specific telephone number. However, the customer care representative that he spoke to informed him that her department could only help with inquiries into booking or changing tickets. Then, he made another attempt by sending an email to an email address found in the dedicated WI-FI privacy policy, upon which he received an error message indicating that the email address did not receive emails. With no other contact information to be found, the EU participant sent the access request by post to the US HQ to the attention of the Data Protection Officer (DPO). Thus, the more

61. Regarding the facilitative/restrictive metric, the existence of a download tool is facilitative, but if the tool is incomplete, and a company does not respond to requests for additional information, the overall response is still restrictive.

This content downloaded from
213.61.224.106 on Tue, 26 Oct 2021 12:38:04 UTC
All use subject to https://about.jstor.org/terms

complete response was received after a lot of effort and not by following the instructions provided in the privacy policy.

IV. ***Controllers outside the EU, Canada, and the United States are more often noncompliant***

We observed comparable quality of the responses from data controllers located in North America and the EU. The least complete replies, in particular among airlines, came from controllers located in Asian countries about whom no data protection adequacy decision was made by the European Commission. In five out of eight cases, no reply was received whatsoever. Turkish Airlines responded that "*we are unable to share personel [sic] information regarding our guest and passengers without being ordered by official institution*." JET Airways responded to one of two requests sent, but saying only that there was no data related to their loyalty programme and did not reply to all other elements of the request. China Southern replied to one out of two requests after a reminder was sent. In reply to the reminder, they wrote "Dear passenger, Hello! This is No.7705 agent of China Southern Airlines. So sorry that do you have anything to consult?" In the ensuing conversation, no clear communication was established.[62]

Regression Analysis: Testing for the Brussels Effect

In order to test for the Brussels Effect, we compared responses to access requests sent pre- and post-GDPR, by individuals from both Canada and the EU, as described in the "Research Methods" section.

The pre-GDPR EU study sent 37 access requests from multiple European countries to the major tech companies that are relevant for our study (Facebook, Google, Microsoft, and Twitter) as well as to airlines. The Canadian study contains 11 access requests sent to social media companies. Fortunately, both studies provided many details about their results,

62. Several interpretations could be made for the lower compliance. The language barrier is likely part of the explanation. We saw many indications that the level of English proficiency of those responding to the access requests was not of a native speaker. Another barrier may be that there is far less history of data protection in these countries. In our interaction with China Southern, for example, it seemed as if the employees that had to deal with the request did not understand the request at all. Even when speaking on the phone with a customer service agent who spoke perfect English, a request for access seemed a concept so alien that it was not understood, rather than denied.

This content downloaded from
213.61.224.106 on Tue, 26 Oct 2021 12:38:04 UTC
All use subject to https://about.jstor.org/terms

TABLE 2 Access Request Results Based on Two Studies Conducted in 2013

Jurisdiction	Sector	Firms	Requests (2013)	Facilitative response (%)	Restrictive response (%)	No response (%)
CA	Airlines	–	–	–	–	–
	Social Media	11	11	1 (9%)	4 (36%)	6 (55%)
EU	Airlines	8	9	4 (44%)	3 (33%)	2 (22%)
	Social Media	4	28	5 (18%)	12 (43%)	11 (39%)
Total		**19**	**48**	**10 (20%)**	**19 (40%)**	**19 (40%)**

allowing us to combine them with our own dataset.[63] The data from these studies is presented in Table 2.

Comparing Tables 1 and 2 shows a general improvement in the response rates (as measured by total proportion of facilitative responses) between 2013 and 2018, especially for social media responses in both Canada and the EU.[64] Doing a longitudinal pairwise comparison to the responses by individual companies also shows an improvement in the level of detail provided,[65] as well as in answer to follow-up questions.[66]

63. Norris et al. already reported their results in the facilitative-restrictive metric in *Unaccountable State of Surveillance*—in fact, we have adapted our metric from them. The study is done by multiple teams across different countries. Whenever the results were not reported as clearly, we contacted the specific researchers and managed to get more details. Note that the requests to airlines in that study were, in some cases, restricted to the data related to the air-miles programs and, in others, to the advanced passenger information (in both cases, it tests the right of access, so it is comparable). We did not use the requests to Amazon, as it is a different sector. For the Bennett, Parsons, and Molnar's study, we recoded their results to our metric.

64. The introduction of download tools may be a key contributing reason why the compliance rate in the social media sector has improved between past studies and ours.

65. For example, whereas Twitter previously provided very limited information about tweets, the company now provides more detail—such as how many times a tweet has been retweeted, by whom, and whether the tweet has been truncated. Moreover, whereas Twitter previously shared 17 categories of data, it now provides 43. Data now includes information about advertising on Twitter, including a list of inferred interests and a file called "ad-engagements" that shows, among other things, which advertisements have been shown on the basis of which targeting criteria the ad was shown, and if it resulted in a "chargeable impression."

66. Google, for example, has not responded to follow-up questions in the past, after data subjects found that the information made available for download did not correspond to all the questions asked (see Norris et al., 244 and 389). In our current study, we also asked Google follow-up questions after we found that their initial response did not address all our questions, and received a detailed response.

This content downloaded from
213.61.224.106 on Tue, 26 Oct 2021 12:38:04 UTC
All use subject to https://about.jstor.org/terms

To distinguish whether the improvements we see in the descriptive statistics are due to the Brussels Effect, or other differences among the requests such as data subject persistence and the location of the data controller, we used multivariate regression analysis. The outcome variable follows a Bernoulli distribution,[67] where a one indicates a *facilitative* response, which can occur with probability p, and a zero indicates a *restrictive* response. Specifically, we used the following model to predict the (expected) probability of a facilitative response for a request:

$$y \sim \text{Bernoulli}(p)$$

$$\begin{aligned}\text{logit}(p) = {} & \alpha_{\text{firm}} + \beta_{\text{sector.}}\text{Sector} + \beta_{\text{hqna.}}\text{HQNA} + \beta_{\text{subjp.}}\text{SubjP} \\ + {} & \beta_{\text{eulaw13.}}\text{EULaw13} + \beta_{\text{neulaw13.}}\text{NonEULaw13} \\ + {} & +\beta_{\text{eulaw18.}}\text{EULaw18} + \beta_{\text{neulaw18.}}\text{NonEULaw18}\end{aligned}$$

The probability p is defined via (a logit link function to) the following factors:

- *Sector*: the controller's sector (1 for social media, 0 for airlines)
- *HQNA*: whether the controller's headquarters is located in a country without any adequacy relationship with the EU
- SubjP: the data subject's persistency (–1 = not, 0 = unknown, 1 = persistent)[68]
- *EULaw13, NonEULaw13, EULaw18, and NonEULaw18*: these four dummy variables group the requests based on jurisdiction and year. EUlaw = EU law applies (because the controller is European or the data subject is in the EU) and NonEULaw = EU does not apply (because the controller is not European and the data subject is not in the EU).
- $\alpha_{\texttt{firm}}$: a pooled varying intercept for each firm, which allows controllers to have a different "compliance level" from their peers, irrespective of the jurisdiction/law[69]

We ran approximately 20,000 simulations and their chains converged well. The full Bayesian model description (along with the priors and convergence details) can be found in Appendix D, while the parameter

67. The Bernoulli distribution is the probability distribution for a binary outcome.

68. Data subjects are considered persistent when they send multiple reminders, follow-up requests when responses are incomplete, or use alternative communication channels when the initial channels are unsuccessful.

69. Using a multilevel varying intercept model is especially important since we have repeated requests to some controllers.

This content downloaded from
213.61.224.106 on Tue, 26 Oct 2021 12:38:04 UTC
All use subject to https://about.jstor.org/terms

estimates from the model are presented in Figure 1 and explained in the next paragraph. In Figure 1, we have converted the logit coefficient values into the "odds interpretation." We also provide the "highest density interval" range, which is how parameter uncertainty is expressed in Bayesian analysis.

The results can be interpreted as follows: the sample baseline for a facilitative response is around 27%. If the controller sector is in the social media sector, the odds of a facilitative response drops by 55% (on average); if the controller is located outside of EU and North America (nonadequacy), the odds of a facilitative response drops by 68%; and if the data subject is persistent, the odds of a facilitative response increases by 41%.

Interpreting the jurisdiction/year effects to evaluate the GDPR and Brussels Effects requires looking at the distribution of the *differences* between the groups, as shown in Figure 2. We interpret the difference between $\beta_{eulaw18}$ and $\beta_{eulaw13}$ as the GDPR Effect, and the difference between $\beta_{neulaw18}$ and $\beta_{neulaw13}$ as the Brussels Effect:

- Based on our data, we find it 91% likely that the GDPR Effect exists (i.e., responses to which EU data protection applies improved).
- Based on our data, we find it 82% likely that the Brussels Effect exists (i.e., responses to requests to which EU law does not formally apply improved).

The model fit is decent; the balanced accuracy, which is the combined true positive and negative rates, is approximately 77%. To check for overfitting, we use the "Widely Applicable Information Criterion" (WAIC) to compare with simpler models, and the model presented here has the best power. (The WAIC details and the posterior predictive plots are provided in Appendix D).[70]

70. We also tested other variables, for example, testing separating out the "GDPR Effect" into three categories: (1) Base GDPR Effect (EU controller responding to EU requests), (2) "Extraterritorial GDPR Effect I" (non-EU controllers responding to EU requests), (3) "Extraterritorial GDPR Effect II" (EU controllers responding to non-EU requests), but found that as our number of requests is limited, creating more categories resulted in variables that would be based on such a limited number of requests that the statistical relevance of the results would be very limited. We have limited evidence that the improvement in responses is larger in non-EU companies than in EU companies. Further research is needed to look into these differences and to corroborate our results.

This content downloaded from
213.61.224.106 on Tue, 26 Oct 2021 12:38:04 UTC
All use subject to https://about.jstor.org/terms

Parameter	Mean (Stdev)	Odds Change (HDI 80%)
Average intercept	-1.3 (1.0)	*Baseline: 27%*
β_{sector}	-0.8 (0.7)	-55% (-81% to +4%)
β_{hqna}	-1.1 (0.8)	-68% (-89% to -12%)
β_{subjp}	0.3 (0.4)	+41% (-15% to +121%)
$\beta_{eulaw13}$	-0.5 (0.7)	-39% (-74% to +54%)
$\beta_{neulaw13}$	-0.4 (0.8)	-33% (-74% to +100%)
$\beta_{eulaw18}$	0.4 (0.7)	+52% (-33% to +261%)
$\beta_{neulaw18}$	0.5 (0.7)	+58% (-35% to +268%)
$\beta_{eulaw18}$ - $\beta_{eulaw13}$	0.9 (0.7)	+150% (+2% to +503%)
$\beta_{neulaw18}$ - $\beta_{neulaw13}$	0.9 (0.9)	+137% (-31% to +636%)

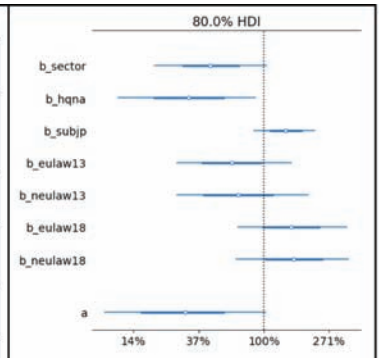

FIGURE 1 Parameter Values and Forest Plot for Full Regression Model (Values Converted to Odds Ratios; 80% highest density interval (HDI) Range Shown; n = 124; Model Balanced Accuracy is 77%).

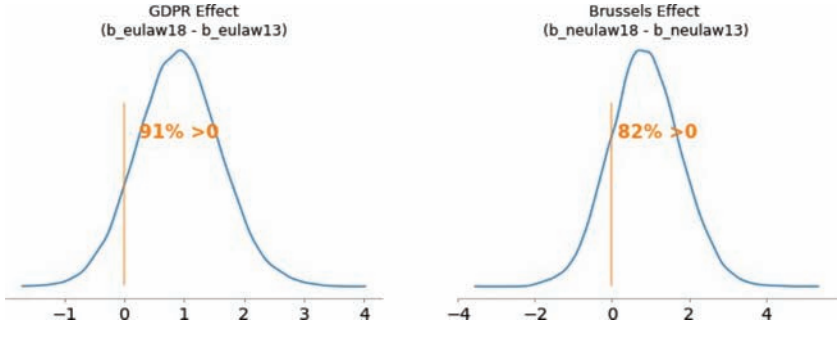

FIGURE 2 GDPR and Brussels Effect, with Their Likelihood Being the Portion of the Distributions Being Over Zero (91% and 82%, Respectively). The Point Estimate for the GDPR Effect is +150% and for the Brussels Effect is +137%.

This content downloaded from
213.61.224.106 on Tue, 26 Oct 2021 12:38:04 UTC
All use subject to https://about.jstor.org/terms

Changes to Privacy Policies After the GDPR

One might argue that the difference between the facilitative response rate for groups NonEULaw18 and NonEULaw13, which we argue is caused by the Brussels Effect, is, instead, a general incremental improvement over time—unrelated to the GDPR. However, as the improvement for requests that did formally fall under EU data protection law, was virtually the same as the improvement under requests that did not fall under EU data protection law, this would also have the unlikely implication that the improvement for responses that did fall under European data protection law was not caused by the introduction of the GDPR. Moreover, there is another piece of evidence in support of the Brussels Effect hypothesis: Companies that change their privacy policies to comply with GDPR, also apply these changes to their Canadian privacy policies.

Compared to PIPEDA and DPD, the GDPR introduced new requirements for privacy policies. The only information that the Directive unequivocally required was for organizations to denote the identity of the controller and the purposes of the processing. The DPD was quite vague about the information that had to be provided, and left the conditions under which controllers had to provide information about the existence of the right of access ambiguous.[71]

PIPEDA was comparatively clearer in terms of scope of the information that needs to be provided, as well as the way in which it has to be provided. For example, it states in clear terms that the organization should make information about how an individual can gain access to the personal data held by the organization available.[72] The GDPR, in contrast to the DPD, unequivocally requires data controllers to provide the elements already required by the DPD, as well as new elements; including the right of

71. The only information that the Directive unequivocally required to be given were the identity of the controller and the purposes of the processing (DPD, Articles 10 and 11). The Directive indicated that in some cases other information needed to be provided but did not specify unequivocally which other information had to be provided. According to the DPD, information such as "the categories of the data concerned" as well as "the existence of the right of access." DPD, Articles 10 and 11. Moreover, the Directive did not specify clearly in which cases other information had to be provided. The DPD stated that other information should only be provided "in so far as such information is necessary, having regard to the specific circumstances in which the data are processed, to guarantee fair processing in respect of the data subject."

72. But, contrary to the GDPR, it does not demand that organizations provide information about the period for which the personal data will be stored (PIPEDA, Principle 8 (under 4.8.2(b))).

This content downloaded from
213.61.224.106 on Tue, 26 Oct 2021 12:38:04 UTC
All use subject to https://about.jstor.org/terms

access to personal data and to lodge a complaint with the relevant DPA.[73] Moreover, the GDPR requires data controllers to provide the information in ways that make them easily understandable to the data subject, for example, by compelling controllers to use "clear and plain language" and making information easily accessible.[74]

As the GDPR adds new transparency requirements, we expect privacy policies shown to EU data subjects to expand and reflect these requirements. If we observe similar changes in the privacy policies shown to Canadians, we can attribute this change to the Brussels Effect.

We tested this by using a semiautomated method to collect and compare privacy policies over time. For each company, we collected the URL for the privacy policy shown to Canadians and Europeans by visiting the company websites from within Canada and Europe in 2018 (during the research setup phase), and once again in 2019. We then wrote a script that used the Wayback Machine[75] to obtain historical copies of the policy pages, from early 2016 (before the enactment of the GDPR), to the end of 2019, on a monthly basis.[76] We converted all the HTML pages to text documents, and compared them using "difflib."

We selected four privacy policies per company for further manual analysis: the policies from before and after the GDPR came into force, one for Canada and one for Europe. In comparing the privacy policies, we particularly recorded what was written about the right of access, the controller contact point, and the complaints procedure.

Foremost, we found that the majority of companies in our sample show the same privacy policy to their Canadian and European customers. Information that explains how personal data is being processed, such as which data is collected, for which purposes it is collected, how it is used, and with whom it is shared, is the same in both jurisdictions. However, the policy document may state that some sections (or rights/terms) apply only to customers from specific jurisdictions.[77] WeChat, for example, states: "YOUR RIGHTS: The following section applies only to persons that are

73. GDPR, Articles 13 and 14. And also the period of time for which data will be stored.

74. GDPR, Article 12.

75. The Wayback Machine, created and provided by The Internet Archive, offers access to archived versions of web pages. https://archive.org.

76. For Icelandair, we unfortunately did not find a prior policy crawl on the Wayback Machine.

77. Note that if the European policies were available in multiple languages, we compared the English version of the policy. Also note that European companies are required by GDPR to treat all their customers according to the rules set out by the GDPR, which is typically the case.

This content downloaded from
213.61.224.106 on Tue, 26 Oct 2021 12:38:04 UTC
All use subject to https://about.jstor.org/terms

resident in the European Union." Some companies, such as Facebook and Google, show slightly different privacy policies based on the IP address from which the connection with their service is made. Other companies, such as United Airlines, ask people to select their country when first visiting their website, directing them to country-specific URLs (e.g., united.com/ual/ca).

Secondly, we found that almost all the companies within our sample changed their privacy policies in April or May of 2018, just before the GDPR went into force.[78]

We found, thirdly, that the length of these policies increased, on average, by about 50%. Table 3 presents some of the differences between the pre- and post-GDPR policies.[79] The most salient changes were the following:

- The level of detail in describing how companies process personal data, for example, with regards to the data collection and data sharing, went up.
- More companies explicitly address data subject rights in their privacy policies, including the right of access to personal data (or do so in more detail).
- More companies provide a dedicated contact point for communication regarding data protection, and mentioned the right to lodge a complaint to a supervisory authority.

Importantly, the additional information offered to Canadians happened as a result of changes in EU law, which is an example of the Brussels Effect at the "policy level."

TABLE 3 Presence of Certain Aspects of Privacy Policies

Topic	Pre-GDPR	Post-GDPR
Right of access	24/33*	34/35**
Right to complain	9/33*	34/35**

Notes:

(*) *We could not access pre-GDPR notices for Icelandair and Wow Air (hence out of 33).*

(**) *Signal is the only company that doesn't mention the right to access or complain; they imply that they do not process personal data, although their policy does not unequivocally state that.*

78. The exceptions were Air Canada, which introduced their GDPR-related changes already in 2017; China Eastern and China Southern, which introduced them in late 2018; and Turkish Airlines, which introduced their GDPR version in mid-2019 (and only for EU users).

79. It should be noted that while the newer privacy policies contain more information, that does not mean they necessarily are more respectful of data subjects and their rights. Both pre- and post-GDPR, we found clauses along the following lines: "Please note that this Privacy Policy is not a contract and does not create any legal rights or obligations." Additionally, as other research on privacy policies have discussed in depth, the longer policies may be harder for the average person to read and understand.

This content downloaded from
213.61.224.106 on Tue, 26 Oct 2021 12:38:04 UTC
All use subject to https://about.jstor.org/terms

Discussion: The Brussels Effect

We found that the introduction of the GDPR did not significantly change the right to get access to personal data. Just as under the previous law in Europe (DPD) and Canada (PIPEDA), companies have to provide access to personal data to data subjects who are in Canada or Europe. Nonetheless, when looking at companies' behavior in responding to access requests, we observe a clear change over time and across jurisdictions. In this section, we discuss what drove these changes and argue that the introduction of the GDPR led to a Brussels Effect, in particular because of the expectation of strong enforcement of its requirements.

Overall, companies are now more facilitative in providing access for Europeans and, to a marginally lesser extent, for Canadians. We also found that sectoral differences are large; airlines are more than twice as likely to provide a facilitative response to access requests than social media companies. Moreover, privacy policies have become more detailed, including mentioning the right of access, and in almost all cases changes apply within and outside of Europe.

Responses to access requests by Canadians improved markedly over time. Specifically, the likelihood of a Canadian receiving a facilitative response from a non-EU company more than doubled according to our model.[80] This change cannot be explained by a change in Canadian data protection law, because there was no relevant change in PIPEDA. Instead, we attribute this change to the effect of the introduction of the GDPR.

It is not likely, however, that the improved responses in Canada are caused by the particular obligations regarding access requests under GDPR. As we saw in the "*Data Collection*" section, the obligations regarding access requests under GDPR are substantially the same as those under PIPEDA and the DPD. Moreover, the changes cannot be explained by the extraterritorial reach of the GDPR, because the GDPR does not apply to a Canadian requesting access to personal data from a non-European company.

Instead, an analysis of the situation through the lens of the Brussels Effect points to enforcement as the likely driver of compliance improvement. As we saw in the "Background" section, there are five conditions for the Brussels Effect to occur. The jurisdiction has to have (1) a large

80. See the section "*Regression Analysis: Testing for the Brussels Effect*": The odds ratio for the Brussels Fffect is 2.37, whereas the odds ratio for variable GDPR Effect is 2.50.

This content downloaded from
213.61.224.106 on Tue, 26 Oct 2021 12:38:04 UTC
All use subject to https://about.jstor.org/terms

market power, (2) regulatory capacity, (3) preference for strict enforcement of rules. Furthermore, the product has to be (4) inelastic and (5) the production process indivisible. Europe already met three or four out of five conditions in regulating data protection under the DPD.

Looking at the first condition—market size—it is clear that it would be more likely for a Brussels Effect to occur with regulation from the EU or the United States, than from Canada. The US's gross domestic product (GDP) is 20.5 trillion USD, the EU's GDP is 18.7 trillion USD, whereas Canada's GDP is 1.7 trillion USD.[81] As a result of its large market, most companies would rather comply with EU law than forgo the European market altogether.[82] Regarding the second condition, all three jurisdictions have strong regulatory capacity, and Europe in particular has a long tradition of DPAs since the 1970s. Furthermore, the fourth condition is met—European data protection is inelastic, since the application of the rules is tied to the location of the data subject. In other words, producers cannot evade the data protection responsibilities by moving their production (and processing of personal data) to a country with lower standards.

One condition, however, a preference for strict enforcement of rules, was only met by the introduction of the GDPR. As we discussed in the section "*Strengthened Enforcement Under the GDPR*," enforcement capabilities of European DPAs went up substantially, and they are being used in practice. Moreover, a string of recent European Court of Justice (ECJ) cases, such as *Schrems*,[83] *Google Spain*,[84] and *Wirtschaftsakademie*,[85] also indicate that Europe is willing to enforce its rules. This is also because the data protection was recognized as a fundamental right in the Charter of Fundamental Rights of the European Union, which became part of EU primary law in 2009.[86] Moreover, the introduction of the GDPR was highly mediatized

81. The World Bank 2018 statistics.

82. Some companies, for most of whom the EU was likely not an important market, first decided—and sometimes, still prefer—to restrict access to users in the EU, rather than complying with the GDPR (e.g., https://www.bbc.com/news/world-europe-44248448; https://econsultancy.com/gdpr-which-websites-are-blocking-visitors-from-the-eu-2/; https://dig.watch/updates/many-us-news-sites-unavailable-due-gdpr-restrictions-compliance; etc.)

83. Case C-362/14 Schrems v. Data Protection Commissioner [2015] ECLI:EU:C:2015:6506.

84. Case C-131/12 Google Spain SL, Google Inc v Agencia Española de Protección de Datos (AEPD) and Maria Costeja González [2014] ECLI:EU:C:2014:317.

85. Case C-210/16 Wirtschaftsakademie Schleswig-Holstein [2018] ECLI:EU:C:2018:388.

86. See, for example, Kuner, "Reality and Illusion," providing an analysis of the *Schrems* case in the context of the policy diffusion.

This content downloaded from
213.61.224.106 on Tue, 26 Oct 2021 12:38:04 UTC
All use subject to https://about.jstor.org/terms

and led to substantial public debate, thereby drawing considerable attention to the topic and the potential for strict enforcement.

Whether the production process is indivisible when it comes to compliance for data protection—the fifth condition of the Brussel Effect—is less clear. The level of divisibility varies for different data protection obligations. We will in turn discuss three levels: policy, procedure, and practice.

Producing a privacy policy has a high initial cost; a detailed analysis of all the companies' data processing is needed, and has to be performed through the lens of the data protection laws, which involve high labor costs. However, marginal costs of showing a privacy policy to customers are close to zero once it has been produced. To the contrary, preparing a different version of a privacy policy for each jurisdiction costs more than showing the same one in all jurisdictions. This changes when the privacy policy describes rights to the data subject, in which case an additional cost would be involved in extending the rights to people in jurisdictions that do not mandate these rights.

Our empirical results follow this pattern. Most privacy policies changed around the introduction of the GDPR. The changes were implemented across jurisdictions in as far as these changes involved a general description of the processing of personal data by the companies. However, in some cases, where companies are allowed to do so, individual rights are restricted to individuals that live in countries where companies are obliged to give access. But even in these cases, the GDPR may help clarify which rights people in other jurisdictions are lacking on the basis of an organization having different privacy policy outside of Europe. These differences with the European privacy policy may help create insight in the practices outside of Europe.

Setting up effective procedures for responding to access requests also has a high initial and fixed costs.[87] On top of mapping all the processes, which is necessary to produce a privacy policy, a process needs to be built to gather all the data undergoing processing and to combine it in such a way that makes it accessible to data subjects. Insofar as this process is automated, the marginal cost of giving access to an individual can be low or close to zero.[88] But when the process is manual, or access has to be provided to elements that have not been automated, costs can be high.

87. McQuinn and Castro, 8, estimates that the fixed cost for maintaining the data infrastructure necessary to deal with data subject rights for large companies is US $91,000, per year.

88. McQuinn and Castro, 9.

This content downloaded from
213.61.224.106 on Tue, 26 Oct 2021 12:38:04 UTC
All use subject to https://about.jstor.org/terms

In any case, through a learning effect, the marginal cost of providing access is likely to decrease in most situations over the number of times that access is given. Because of this, it is likely that the overall tendency of companies to provide access will go up once they are forced to provide access in one jurisdiction (in other words, an altered cost–benefit analysis incentivizes them). This can also explain why access to personal data through data download tools is often provided across jurisdictions, including jurisdictions that do not have a legal right of access to personal data. Furthermore, it can explain why access to additional data, and information related to its processing that is not included in the download tools, is often refused.[89]

Altering the core of the data processing operations—the actual practice of how personal data is used by organizations—is likely to involve both high initial as well as ongoing costs, whether it is only for one jurisdiction or for all. Generally, when a company processes personal data, they do so because it is in their financial benefit. Moreover, from a system design and operational point of view, maintaining different operations for different jurisdictions could be less efficient and costly.

Although our research did not directly target the underlying data processing operations, we did not see changes in privacy policies, or responses to access requests, pointing at companies changing the way they are processing personal data. However, as is clear from our work and other existing research, most privacy policies and responses to access requests are so unspecific—with regards to crucial elements that explain the underlying data practices—that it is simply impossible to judge if companies changed their practices on this basis.[90]

The *expectation* of enforcement is likely to be the key element driving corporate change in the direction of higher data protection standards, as the expectation of enforcement is the main difference between the GDPR, on the one hand, and the DPD and PIPEDA on the other. Moreover, the

89. Download tools are a technical solution to the right of access, which also have limiting characteristics (see also Knockel et al.). Following Lessig's famous phrase in *Code* that "Code is law," we clearly see that code determines the conditions by which rights can be exercised. It is another instance in which data protection by design clashes with data subject rights (cf. Veale, Binns, and Ausloos).

90. In reaction to the introduction of the GDPR, some companies decided to change the way they process personal data of European customers while leaving their processes for other customers untouched. The *New York Times*, for example, decided to stop the use of behavioral advertising and switch completely to contextual and geographical, which is much less invasive to privacy. Davies.

This content downloaded from
213.61.224.106 on Tue, 26 Oct 2021 12:38:04 UTC
All use subject to https://about.jstor.org/terms

expectation of enforcement was amplified by the high level of attention that was given to the GDPR in the period around its introduction; the GDPR was grabbing headlines at both sides of the Atlantic. This general attention to the content of the GDPR, and the potential stringent enforcement in particular, would lead businesses to pay increased attention to data protection.

This attention effect may evaporate, however, especially when actual enforcement does not follow. Therefore, in order for the Brussels Effect to be sustainable, this expectation has to be met by actual enforcement of the regulators. Otherwise, the GDPR may have the same limited effect as the DPD in the long run. As Bygrave argued, the power of the EU to bring data protection regimes in line with its own was severely limited under the DPD—because of limited harmonization, enforcement and compliance with the law within Europe, and limited strength shown in the application of adequacy requirements abroad.[91]

The GDPR clearly improves the situation in those respects, but it also has considerable potential weaknesses. Although the GDPR harmonizes data protection regulation within the EU to a much farther extent than the DPD, it still allows for many aspects to be dealt with at the national level. For instance, under the one-stop-shop mechanism, companies are regulated through the authority of the country where they have their main establishment, creating room for companies to locate in countries with relatively weak enforcement, such as Ireland.[92]

Separate from whether the Brussels Effect exists, it may be asked how reasonable it is to expect companies that primarily operate in other jurisdictions to conform to European data protection regulations. Much of this criticism against the broad scope of the GDPR comes from the United States. Scott and Cerulus in *Politico* wrote, for example, that: "the upcoming data protection changes risks being viewed as yet another diktat handed down by former colonial powers in a form of 'data imperialism.'" Schwartz argued, in alarmist terms, that the GDPR proposal was going too far and would lead to a "privacy collision" between the EU and the United States.[93]

---

91. Bygrave, 47.

92. Voss and Bouthinon-Dumas. This problem has also been noted in resolution P9_TA(2021)0111 of the European Parliament, calling on the DPAs of Ireland and Luxembourg to speed up their enforcement efforts, and on Member State governments to adequately fund the national authorities https://www.europarl.europa.eu/doceo/document/TA-9-2021-0111_EN.html.

93. Schwartz, "The EU-U.S. Privacy Collision."

This content downloaded from
213.61.224.106 on Tue, 26 Oct 2021 12:38:04 UTC
All use subject to https://about.jstor.org/terms

An alternative—and possibly more productive—way of looking at Europe setting standards for the offering for goods and services delivered to people in Europe is to see it as autonomous policy-setting.[94] In this case, the EU is asserting its right to unilaterally set laws for people within its jurisdiction, leading to compliance extending beyond its borders. This global Brussels Effect is a side effect of this central effort (which economists may call externality).

The deeper tension is the contrast between free economic development based on the uninhibited flow of personal data, and the protection of fundamental rights—which may be at odds with such unimpeded flow of personal data. As we have seen in in the section "*History of Data Protection Law in EU and Canada,*" discussions about the need to adequately protect individuals across borders without impeding the flow of data have been central in efforts to create international policy instruments. Continued efforts to find a common ground in policymaking and finding a form of consensus can be beneficial. Uniform and clear rules help create a level playing field, and prevent companies from stopping legitimate processing just because they are unsure about the rules. Whether the EU is justified in setting a high standard for data protection should be seen in the context of a general confrontation between global economic liberalism and the protection of fundamental rights, which we see playing out in diverse policy areas such as climate change, labor rights, and agricultural policy.[95]

Conclusion

Our work shows that while companies' compliance with the right of access to personal data has improved with the introduction of the GDPR, it

94. In this context, the trope of "imperialism" is often applied as a discursive label. See Yakovleva, explaining how in the policy discussions on the relation between data protection and free trade economic discursive practices are often foregrounded at the expense of multidisciplinary discourses that include more than only economic arguments. She concludes that "The discussion should be not about what protectionism means but rather about how far domestic regimes are willing to let trade rules interfere in their autonomy to protect their societal, cultural, and political values."

95. See, for example, De Ville and Siles-Brügge, for a discussion of the validity of the criticisms raised against the proposed new free trade agreement between the EU and the US TTIP.

This content downloaded from
213.61.224.106 on Tue, 26 Oct 2021 12:38:04 UTC
All use subject to https://about.jstor.org/terms

still remains insufficient. In line with other research, we found that—it is often necessary to be persistent, there are marked sectoral differences, and controllers outside of the EU, Canada, and the United States are noncompliant even more often.

As empirically shown, the Brussels Effect is likely an important channel of data protection policy diffusion. In particular, we have shown that companies complied better with the right of access to personal data of Canadian residents, without Canada's law having changed. This indicates that the introduction of the GDPR instantiated a Brussels Effect, which led global companies to change their behavior, and to improve compliance with data protection requirements for people in Europe and beyond. Finally, based on an analysis of the conditions that need to be present for the Brussels Effect to occur, we argue that improved enforcement is likely to be the key driver of this change.

Future Work

While our work shows it is likely that the GDPR had an effect in diffusing corporate compliance with its rules beyond EU borders, stronger and more precise quantitative evidence is needed. Evidence could be strengthened by having more longitudinal studies, based on more data and with stricter protocols, for example by asking participants to delegate requests to researchers. Quantitative evidence from studies such as ours should be supplemented with insights from other methods, such as interviews, for example, with data protection officers.

Generally, more work is urgently needed on the conditions that make policy interventions effective. While data protection laws based on the same principles that are now in the GDPR exist since the 1970, there is abundant evidence that overall compliance—in particular, compliance with those aspects of data protection that when strictly adhered to would limit certain profitable business models—is still low. Scholars have, so far, done most of the work on the diffusion of laws, but should focus on the channels that drive actual change of behavior.

Work is also needed on the question: to what extent does the desire to refrain from unduly limiting the free flow of data stifles the ability to set limits to the freedom of corporate and state behavior—in order to protect people's rights, both in the realm of data protection and beyond?

This content downloaded from
213.61.224.106 on Tue, 26 Oct 2021 12:38:04 UTC
All use subject to https://about.jstor.org/terms

Acknowledgments

We thank all study participants, and the researchers from earlier studies who communicated with us about their work for their contributions. We also thank Paul de Hert, Ilaria Buri, and two anonymous reviewers for their careful reading and constructive feedback, as well as Mirna Sodré de Oliveira for her meticulous help in editing this article.

APPENDICES

Appendix A: Companies in Study

TABLE 4 Companies Included in the Study (Request Count Includes Those Received with no Response, but Excludes Requests Abandoned by the Participants)

Company Name	Sector	Requests EU	Requests Canada
Academia.edu	Social Media	1	0
Aegean	Airlines	1	0
Air Canada	Airlines	2	4
Air France	Airlines	1	1
American Airlines	Airlines	0	2
British Airways	Airlines	1	1
Brussels Airlines	Airlines	1	0
Cathay Pacific	Airlines	1	2
China Eastern	Airlines	0	2
China Southern	Airlines	1	1
Delta	Airlines	1	2
Easy Jet	Airlines	1	0
Facebook (service: Facebook)	Social Media	2	0
Facebook (service: Instagram)	Social Media	1	3
Google (service: Hangouts)	Social Media	1	2
Icelandair	Airlines	0	2
Jet Airways	Airlines	1	1
KLM	Airlines	1	2
LinkedIn	Social Media	1	3

(*Continued*)

This content downloaded from
213.61.224.106 on Tue, 26 Oct 2021 12:38:04 UTC
All use subject to https://about.jstor.org/terms

TABLE 4 Companies Included in the Study (Request Count Includes Those Received with no Response, but Excludes Requests Abandoned by the Participants) (*Continued*)

Company Name	Sector	Requests EU	Requests Canada
Microsoft (service: Skype)	Social Media	1	1
Pinterest	Social Media	1	1
Reddit	Social Media	1	1
Signal	Social Media	1	1
Snapchat	Social Media	1	3
Soundcloud	Social Media	1	0
Telegram	Social Media	1	0
Transat	Airlines	0	1
Tumblr	Social Media	0	1
Turkish Airlines	Airlines	1	1
Twitter	Social Media	0	2
United Airlines	Airlines	1	1
WeChat	Social Media	1	2
WhatsApp	Social Media	1	1
Wire	Social Media	1	0
WOW Air	Airlines	1	0

Notes:

- The line between service brand, department, subsidiary, and parent company can be murky in the internet world; Here, the company refers to the legal entity named as the data controller in the privacy policy. This company may, in some instances, be itself a subsidiary of a larger company (e.g., LinkedIn, WhatsApp, and Tumblr).
- The companies Jet Airways and WOW Air went bankrupt between the research and its publication.
- In cases where we have looked only at a specific service for a company, such as Skype or Hangouts, we mention those services in parenthesis.

Appendix B: Do Access Rights Apply to Companies in Third Countries?

Part of what we investigate in this article is whether European and Canadian data subjects can effectively exercise the right of access to foreign companies. A step in this investigation is to assess if and under which conditions their respective national laws give them such rights. In this appendix, we offer a legal analysis of the territorial reach of the European data protection regulation (General Data Protection Regulation [GDPR] and Data Protection Directive [DPD]) as well as the Personal Information Protection and Electronic Documents Act

This content downloaded from
213.61.224.106 on Tue, 26 Oct 2021 12:38:04 UTC
All use subject to https://about.jstor.org/terms

(PIPEDA). We will see that the extent of the extraterritorial scope was contested under the DPD,[96] and was interpreted extensively in the *Google Spain* judgment of the Court of Justice of the European Union (EU). The GDPR extends the extraterritorial scope further and more clearly.

DPD

According to the letter of the law, the DPD applied when (Art 4(1)(a)) "the processing is carried out in the context of the activities of an establishment of the controller [. . .]"[97] or (Art 4(1)(c)) "makes use of equipment [. . .] situated on the territory of the member state."[98]

It has generally been accepted that the article about the territorial scope of the DPD was unclear. According to Moerel, for example, the application of this aspect of the DPD was "extraordinarily complex."[99] However, the prevailing opinion expressed in the legal literature, by the European Commission as well as by data protection authorities, was that the DPDs territorial scope should be interpreted rather extensively. First, the applicability of the DPD was related to the processing of an establishment under Article 4(1)(a) DPD, which meant that it was enough when this was just a secondary establishment like a subsidiary, branch, or agency. Second, under Article 4(1)(a), the law applied when the processing took place "in the context of the activities" of that establishment, so that the law would also apply when the processing itself took place outside the EU. Third, Article 4(1)(c) was added to make sure that the law could not be circumvented by just reestablishing a company outside of Europe.[100]

According to Kuner, the term "equipment" was initially meant to cover physical objects such as computer servers and terminals.[101] However, the

96. Moerel, "Back to Basics," 92.

97. See Article 4(1) DPD: "Each Member State shall apply the national provisions it adopts pursuant to this Directive to the processing of personal data where: a) the processing is carried out in the context of the activities of an establishment of the controller on the territory of the Member State; when the same controller is established on the territory of several Member States, he must take the necessary measures to ensure that each of these establishments complies with the obligations laid down by the national law applicable."

98. See Moerel, "The Long Arm of EU Data Protection Law" for a more detailed discussion of Article 4(1)(c).

99. Moerel, "Back to Basics," 92.

100. Moerel, "The Long Arm of EU Data Protection Law."

101. Kuner, "International Jurisdiction on the Internet (Part 2)," 228.

This content downloaded from
213.61.224.106 on Tue, 26 Oct 2021 12:38:04 UTC
All use subject to https://about.jstor.org/terms

Working Party[102] was of the opinion that the interpretation of the term equipment should be broad and include the setting of cookies on the computer of a user within the EU (Working Party, 2010).[103] Over time, through ECJ case law, the extensive interpretation of the territorial scope was affirmed, in particular by *Google Spain* in 2014 and *Weltimmo* in 2015.[104]

Taken together, the DPD applied to European companies irrespective of whether they were processing data relating to European or Canadian data subjects, and irrespective of whether the processing was happening in Europe. It also applied to non-European airlines because they sell tickets to European customers through European sales offices, and the processing of personal data takes place in the context of these activities. The DPD also likely applied to social media companies because they make use of equipment (servers and cookies) in the EU, and because most of them have branches in Europe.

GDPR

Under GDPR, the location of the activities of the company is no longer the only determinant factor.[105] If a company does business with EU citizens, the GDPR applies—irrespective of the location of the company.[106] Thus,

---

102. The Article 29 Working Party is an independent advisory body consisting of members from the national DPAs, which writes opinions interpreting specific elements of data protection law. While these documents are not legally binding, they do tend to have impact. Kuner, *European Data Protection Law*, 9–10.

103. See, for a more detailed discussion, van der Sloot and Zuiderveen Borgesius.

104. Case C-131/12 *Google Spain SL, Google Inc., v Agencia Española de Protección de Datos* (AEPD) and Maria Costeja González [2014] EU:C:2014:317 and Case C230/14 *Weltimmo sro v Nemzeti Adatvédelmi és Információszabadság Hatóság* [2015] ECLI:EU:C:2015:639. In these cases, the Court decided to take an extensive interpretation of the first criterion that there should be an establishment on the territory, as well as an extensive interpretation of the second criterion that processing has to take place in the context of the establishment's activities. In particular, for an establishment to exist, it is not necessary that the controller is headquartered in the country. Instead, it is enough if there is "effective and real exercise of activity through stable arrangements." Therefore, an establishment can be a subsidiary, a branch, or even a single employee such as a sales representative. De Hert and Czerniawski, 233.

105. See EDPB "Guidelines 3/2018 on the Territorial Scope of the GDPR (Article 3) Version 2.1," for a general and more in-depth analysis of the territorial scope of the GDPR.

106. See Article 3(2) GDPR: "This Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to: (a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or (b) the monitoring of their behavior as far as their behavior takes place within the Union." See also recital 23 and 24 GDPR. It matters if the controller "envisages offering goods or services to data subjects in the Union."

This content downloaded from
213.61.224.106 on Tue, 26 Oct 2021 12:38:04 UTC
All use subject to https://about.jstor.org/terms

with the entry into force of the GDPR, EU citizens should be able to exercise a right of access toward a company that offers goods and services to them in the EU, irrespective of whether this company has its main establishment, a subsidiary, or no presence at all in the EU.

According to Recital 23 GDPR, the Regulation applies when the company "envisages offering goods and services to data subjects in the Union." Since airlines have localized European versions of their websites, often with the ability to show prices in Euros and in European languages, the intention to sell to European citizens is clear.[107] Similarly, because social media companies offer their apps in European app stores, the GDPR applies. Moreover, European companies have to apply the GDPR to their worldwide activities.

PIPEDA

Companies routinely provide services to Canadian consumers while retaining a minimal operational footprint in the country. This is especially true of Internet-based services, such as social networking, and less true in the case of companies with significant physical assets, such as airlines. A minimality of presence, however, does not diminish the potential reach of Canada's PIPEDA. This legal situation was decided in a case that involved AccuSearch, where the Federal Court of Canada asserted that the Office of the Privacy Commissioner of Canada had jurisdiction over a privacy complaint pertaining to the company's practices.[108] The Court recognized that the *enforcement* of the law may be challenged, but its applicability was certain. Specifically, so long as a company has a real and substantial connection between an entity or the actions that were complained about, the law applies. Drawing on this decision, the Office of the Privacy Commissioner of Canada concluded:

> "Where the Privacy Commissioner has jurisdiction over the subject matter of the complaint but the company deals with cloud computing infrastructure and thus is not obviously located in Canada, current jurisprudence is clear that the Privacy Commissioner may

107. De Hert and Czerniawski argue in "Expanding the European Data Protection Scope beyond Territory" that the formulation of Article 3(2)(a) is not clear enough and may lead to legal uncertainty, especially on the part of the controllers, who may not know whether the GDPR applies to them (or may have multiple laws apply to them). Although this may be the case in certain situations, we think that it is clear in the cases under consideration in this article.

108. https://reports.fja.gc.ca/fja-cmf/j/en/item/331930/index.do?q=lawson+accusearch.

This content downloaded from
213.61.224.106 on Tue, 26 Oct 2021 12:38:04 UTC
All use subject to https://about.jstor.org/terms

exert jurisdiction when assessment indicates that a real and substantial connection to Canada exists."[109]

Over the years and based on the extraterritorial reach of PIPEDA, the Office of the Privacy Commissioner has launched investigations into a range of foreign-based companies, such as Facebook, Google, Netflix, WhatsApp, and others. While the assertion of jurisdiction has not always been accepted by international companies, including companies being confronted with data access requests under PIPEDA,[110] the law pertaining to PIPEDA's jurisdiction has not changed since 2007. Based on these analyses, and the fact that all the companies included in our study had ongoing commercial relations with Canadians, PIPEDA—and in particular its Subject Access Request (SAR) provisions—applied to all of the companies included in our study.

Appendix C: Text of Access Request Letters

Social Media DAR Template

<Name participant>
<Street participant>
<Postal code participant>
<City participant>

Confidential
<Name organization>
Data Protection Officer
<Street organization>
<Postal code and city organization>
<Country organization>
<City>, <Date>
Subject access request
Dear Sir or Madam,
I am a customer of <name service>, and am interested in both learning more about your data management practices and the personal data you

109. https://www.priv.gc.ca/media/1723/cc_201003_e.pdf.
110. Bennett, Parsons, and Molnar; Parsons, Hilts, and Crete-Nishihata.

This content downloaded from
213.61.224.106 on Tue, 26 Oct 2021 12:38:04 UTC
All use subject to https://about.jstor.org/terms

process about me. Please supply within one month the following information, as I am entitled to under article <X> of <LAW NAME>:

A. Whether you process my personal data (*including storing it*)
B. If so, a copy of *all* my personal data (whether collected from me, from another party, or *derived by other means*)
C. The source(s) of the data
D. The purpose of the processing
E. The parties to whom you have disclosed or been legally compelled to disclose this data, and an itemization of data categories disclosed
F. The time period(s) for which you intend to store or are storing the various data categories you may retain

Please provide this data, where possible, in a structured and nonproprietary digital format, at free or minimal cost.

If your service includes a **data download tool**, you are free to direct me to it, but ensure that in responding to this letter, you do provide requested data associated with me that is *not* included in the output of this tool.

In particular, I request that item "A" through "F," above, be provided in respect of each of the following. If you do not process such data, please indicate so explicitly:

1. **My contacts** (whether collected from my mobile device address book, or other sources)
2. **Geolocation data** (about me, my devices, and/or my account)
3. **Browsing history** (including URLs visited by me, my devices, and/or my account)
4. **IP address logs** (associated with me, my devices, and/or my account)
5. **Lifestyle information and profile** (that you may have collected or derived about me, such as interests, income, health and well-being, alcohol or drug use, or sexual preferences, and advertiser segments)
6. **"Deleted" data** (data that, while no longer visualized from the front-end interface presented to end-users, remains in your backend databases)

Finally, I would like to know if your company has suffered any **data breach** in which my data may have been exposed to unauthorized parties. If so, please provide information about the breach.

In order for you to establish my identity, please find below my identifying information:

- First name <FIRST NAME>
- Last name: <LAST NAME>

This content downloaded from
213.61.224.106 on Tue, 26 Oct 2021 12:38:04 UTC
All use subject to https://about.jstor.org/terms

- Email address associated with account: <EMAIL ADDRESS>
- Username (if applicable): <USERNAME>
- Telephone number (if applicable): <PHONE NUMBER>

Please let me know if your organization requires additional information from me before proceeding with my request.

Yours faithfully,
<Name participant>

Appendix D: Regression Model Details

Model Code. The Bayesian regression model is defined in Stan (https://mc-stan.org/) as follows. Note that we have used weakly informative priors as recommended by for instance McElreath (2020).

```
data {
  int<lower = 1> N; // number of observations
  int<lower = 1> nF; // number of firms (for varying intercepts)
  int fid[N]; // identify firms for pooled varying intercepts
  int<lower = 1> nP; // number of (individual) predictors
  matrix[N, nP] X; // predictors, which include:
  // 'sector_sm','hq_noa','subj_p','eul13','neul13','eul18','neul18'
  int<lower = 0, upper = 1> Y[N]; // outcome/observations
}
parameters {
  vector[nF] a_f; // unique intercepts (pooled)
  real a; // pooled intercepts: mean
  real<lower = 0> sigma; // pooled intercepts: sigma
  vector[nP] beta; // beta for all predictors
}
model {
  vector[N] p;
  target += normal_lpdf(beta | 0, 1);
  target += normal_lpdf(a_f | 0, 1);
  target += normal_lpdf(a | 0, 10);
  target += cauchy_lpdf(sigma | 0, 0.5);
  for ( i in 1:N )
```

This content downloaded from
213.61.224.106 on Tue, 26 Oct 2021 12:38an 1976 12:34:56 UTC
All use subject to https://about.jstor.org/terms

```
    p[i] = a + sigma * a_f[fid[i]] + X[i] * beta;
  target += binomial_logit_lpmf(Y | 1, p);
}
generated quantities {
  vector[N] yh1;
  vector[N] yh2;
  vector[N] ll;
  for ( i in 1:N ) {
  real p;
      p = a + sigma * a_f[fid[i]] + X[i] * beta;
  yh1[i] = inv_logit(p); // actual predicted values
  yh2[i] = bernoulli_logit_rng(p); // 0,1s
  ll[i] = bernoulli_logit_lpmf(Y[i] | p);
  }
}
```

Model Convergence/Fit. We use MCMC sampling with 4 and 10,000 iterations (half for warm-up). The chains converge well, with the Gelman-Rubin statistic (rhats) approximately 1.0 (standard deviation 0.0003). Stan generates no major warnings. The model has a balanced accuracy (the average of the true positive and true negative rates) of 77%. The Arviz package reports a pseudo R_2 of 0.53.

Alternative Models. Our full model includes pooled varying intercepts per company, as well as eight predictors. We compare this model with two simpler models—one that includes all the predictors, but no varying intercepts (altmodel_2); and another which includes the varying intercepts, but not the interaction terms for the jurisdictional variables (altmodel_3). We compare the models using the widely applicable information criterion (WAIC), which also accounts for over-fitting. As shown in Table 5, the full model performs equal to, or better, than the alternative specifications.

TABLE 5 Comparison among the Article Model and Alternative Specifications Based on WAIC

	Rank	loo (log)	p_loo	d_loo	Weight	se	dse
model _article	**0**	−63.3	19.9	0	**0.57**	6.0	0
altmodel_3	1	−63.5	16.7	0.2	0.42	5.9	1.5
altmodel_2	2	−70.5	5.0	7.5	0.01	5.4	3.5

This content downloaded from
213.61.224.106 on Tue, 26 Oct 2021 12:38:04 UTC
All use subject to https://about.jstor.org/terms

BIBLIOGRAPHY

Albrecht, Jan Philipp. "How the GDPR Will Change the World." *European Data Protection Law Review* 2, no. 3 (2016): 287–89. doi:10.21552/EDPL/2016/3/4.

Article 29 Data Protection Working Party. "Opinion 1/2008 on Data Protection Issues Related to Search Engines (Wp148)." Brussels, 2008. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2008/wp148_en.pdf. Accessed May 22, 2021.

Association Française des Correspondants à la Données à caractère Personnel (AFCDP). "Publication de l'Index AFCDP Du Droit d'accès." L'Association Française des Correspondants à la Données à caractère Personnel (AFCDP), January 24, 2020. https://afcdp.net/media/documents/CP-AFCDP-Index-du-droit-d-acc-s-24-janvier-2020-3-.pdf. Accessed May 22, 2021.

Ausloos, Jef, and Pierre Dewitte. "Shattering One-Way Mirrors — Data Subject Access Rights in Practice." *International Data Privacy Law* 8, no. 1 (February 1, 2018): 4–28. doi:10.1093/idpl/ipy001.

Ausloos, Jef, René Mahieu, and Michael Veale. "Getting Data Subject Rights Right — A Submission to the European Data Protection Board from International Data Rights Academics, to Inform Regulatory Guidance." *JIPITEC* 10, no. 3 (2019): 283–309. https://www.jipitec.eu/issues/jipitec-10-3-2019/5031. Accessed May 22, 2021.

Autoriteit Persoonsgegevens. "Jaarverslag 2016." Den Haag: Autoriteit Persoonsgegevens, 2017. https://autoriteitpersoonsgegevens.nl/nl/publicaties/jaarverslagen. Accessed May 22, 2021.

———. "TGB betaalt dwangsom na niet voldoen aan inzageverzoek." August 9, 2018. https://autoriteitpersoonsgegevens.nl/nl/nieuws/tgb-betaalt-dwangsom-na-niet-voldoen-aan-inzageverzoek. Accessed May 22, 2021.

Autoriteit Persoonsgegevens. Letter to Bureau Krediet Registratie (BKR). "Besluit Tot Het Opleggen van Een Bestuurlijke Boete BKR." July 30, 2019. https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/besluit_bkr_30_juli_2019.pdf. Accessed May 22, 2021.

Becher, Shmuel I., and Uri Benoliel. "Law in Books and Law in Action: The Readability of Privacy Policies and the GDPR." In *Consumer Law and Economics*, 9: 179–204. Economic Analysis of Law in European Legal Scholarship. Cham, Switzerland: Springer, 2020. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3334095. Accessed May 22, 2021.

Bennett, Colin J. *Regulating Privacy: Data Protection and Public Policy in Europe and the United States*. 1st ed. Ithaca and London: Cornell University Press, 1992.

Bennett, Colin, Christopher A. Parsons, and Adam Molnar. "Real and Substantial Connections: Enforcing Canadian Privacy Laws Against American Social Networking Companies." *Journal of Law, Information & Science* 23, no. 1 (2014): 50–74. doi:10.2139/ssrn.2226647.

Bennett, Colin J., and Charles D. Raab. "The Adequacy of Privacy: The European Union Data Protection Directive and the North American Response." *The Information Society* 13, no. 3 (1997): 245–64. doi:10.1080/019722497129124.

———. *The Governance of Privacy: Policy Instruments in Global Perspective*. Cambridge, MA: MIT Press, 2006.

Bradford, Anu. "The Brussels Effect." *Northwestern University Law Review* 107, no. 1 (2012): 1–68.

Burri, Mira, and Rahel Schär. "The Reform of the EU Data Protection Framework: Outlining Key Changes and Assessing Their Fitness for a Data-Driven Economy." *Journal of Information Policy* 6 (2016): 479–511. doi:10.5325/jinfopoli.6.2016.0479.

Bygrave, Lee A. "International Agreements to Protect Personal Data." In *Global Privacy Protection*, edited by James B. Rule and Graham Greenleaf, 15–49. Glos: Edward Elgar, 2008.

This content downloaded from
213.61.224.106 on Tue, 26 Oct 2021 12:38:04 UTC
All use subject to https://about.jstor.org/terms

Cline, J. "U".S. Takes the Gold in Doling out Privacy Fines." Computerworld, February 17, 2014. https://www.computerworld.com/article/2487796/data-privacy/jay-cline--u-s--takes-the-gold-in-doling-out-privacy-fines.html. Accessed May 22, 2021.

College Bescherming Persoonsgegevens. *Jaarverslag 2011*. Den Haag: College Bescherming Persoonsgegevens, 2012. https://www.autoriteitpersoonsgegevens.nl/sites/default/files/downloads/jaarverslagen/jv_2011.pdf. Accessed May 22, 2021.

Commission nationale de l'informatique et des libertés (CNIL). "Deliberation of the Restricted Committee SAN-2019-001 of 21 January 2019 Pronouncing a Financial Sanction against GOOGLE LLC." 2019. https://www.cnil.fr/sites/default/files/atoms/files/san-2019-001.pdf. Accessed May 22, 2021.

Davies, Jessica. "After GDPR, The New York Times Cut off Ad Exchanges in Europe — and Kept Growing Ad Revenue." *DigidayUK* (blog), 2019. https://digiday.com/media/new-york-times-gdpr-cut-off-ad-exchanges-europe-ad-revenue/. Accessed May 22, 2021.

Davies, Simon. "Privacy Opportunities and Challenges with Europe's New Data Protection Regime." In *Privacy in the Modern Age*, edited by Marc Rotenberg, 55–60. New York and London: The New Press, 2015.

Davis, Kevin E, and Florencia Marotta-Wurgler. "Contracting for Personal Data." *New York University Law Review* 94 (2019): 662–705. https://www.nyulawreview.org/issues/volume-94-number-4/contracting-for-personal-data/. Accessed May 22, 2021.

De Hert, Paul, and Michal Czerniawski. "Expanding the European Data Protection Scope beyond Territory: Article 3 of the General Data Protection Regulation in Its Wider Context." *International Data Privacy Law* 6, no. 3 (August 1, 2016): 230–43. doi:10.1093/idpl/ipw008.

De Ville, Ferdi, and Gabriel Siles-Brügge. "Why TTIP Is a Game-Changer and Its Critics Have a Point." *Journal of European Public Policy* 24, no. 10 (October 27, 2017): 1491–505. doi:10.1080/13501763.2016.1254273.

The Citizen Lab. "Access My Info: Measuring Data Access Rights Around the World." The Citizen Lab, October 16, 2019. https://citizenlab.ca/2019/10/measuring-data-access-rights-around-the-world/. Accessed May 22, 2021.

European Commission. *Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions — A Comprehensive Approach on Personal Data Protection in the European Union*. Brussels: European Commission, November 4, 2010. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52010DC0609&from=EN. Accessed May 22, 2021.

———. "Safeguarding Privacy in a Connected World — A European Data Protection Framework for the 21st Century." Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of Regions. Brussels: European Commission, January 25, 2012. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52012DC0009&from=en. Accessed May 22, 2021.

European Data Protection Board (EDPB). "Guidelines 3/2018 on the Territorial Scope of the GDPR (Article 3) Version 2.1." November 12, 2019. https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_3_2018_territorial_scope_after_public_consultation_en_1.pdf. Accessed May 22, 2021.

European Union Agency for Fundamental Rights (FRA). *Access to Data Protection Remedies in EU Member States*. Luxembourg: Publications Office of the European Union, 2013. doi:10.2811/69883.

Frenkel, Sheera. "Tech Giants Brace for Europe's New Data Privacy Rules." *The New York Times*, January 28, 2018, sec. Technology. https://www.nytimes.com/2018/01/28/technology/europe-data-privacy-rules.html Accessed May 22, 2021.

This content downloaded from
213.61.224.106 on Tue, 26 Oct 2021 12:38:04 UTC
All use subject to https://about.jstor.org/terms

FTC. "Press Release: FTC Imposes $5 Billion Penalty and Sweeping New Privacy Restrictions on Facebook." July 24, 2019. https://www.ftc.gov/news-events/press-releases/2019/07/ftc-imposes-5-billion-penalty-sweeping-new-privacy-restrictions. Accessed May 22, 2021.

GDPR.EU. "2019 GDPR Small Business Survey." 2019. https://gdpr.eu/wp-content/uploads/2019/05/2019-GDPR.EU-Small-Business-Survey.pdf. Accessed May 22, 2021.

Golla, Sebastian J. "Is Data Protection Law Growing Teeth?" *Journal of Intellectual Property, Information Technology and E-Commerce Law* 8 (2017), 70–78. https://www.jipitec.eu/issues/jipitec-8-1-2017/4533. Accessed May 22, 2021.

González Fuster, Gloria. *The Emergence of Personal Data Protection as a Fundamental Right of the EU*. Law, Governance and Technology Series 16. New York, Dordrecht, London: Springer Science & Business, 2014. doi:10.1007/978-3-319-05023-2_3.

Greenleaf, Graham. "The Influence of European Data Privacy Standards Outside Europe: Implications for Globalisation of Convention 108." *International Data Privacy Law* 2, no. 2 (2012): 68–92. doi:10.1093/idpl/ips006.

Hoepman, Jaap-Henk. "Het recht op inzage is een wassen neus. Wat nu?" *Informatiebeveiliging* 2011, no. 6 (2011): 16–17. https://repository.tudelft.nl/view/tno/uuid:6be95e4c-a836-4d64-8ad2-eeb1b987bfa7/. Accessed May 22, 2021.

Information Commissioner's Office (ICO). "ICO Fines British Airways £20m for Data Breach Affecting More than 400,000 Customers." October 26, 2020. https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2020/10/ico-fines-british-airways-20m-for-data-breach-affecting-more-than-400-000-customers/. Accessed May 22, 2021.

———. "SCL Elections Prosecuted for Failing to Comply with Enforcement Notice." January 11, 2019. https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2019/01/scl-elections-prosecuted-for-failing-to-comply-with-enforcement-notice/. Accessed May 22, 2021.

———. Letter to Facebook Ireland Ltd. "Monetary Penalty Notice." October 24, 2018. https://duncheva.bg/wp-content/uploads/2018/10/r-facebook-mpn-20181024.pdf. Accessed May 22, 2021.

Knockel, Jeffrey, Christopher Parsons, Lotus Ruan, Ruohan Xiong, Jedidah Crandall, and Ron Deibert. *We Chat, They Watch — How International Users Unwittingly Build up WeChat's Chinese Censorship Apparatus.* Research Report. Toronto, Canada: The Citizen Lab, May 7, 2020. https://tspace.library.utoronto.ca/bitstream/1807/101395/1/Report%23127--wechattheywatch-web.pdf. Accessed May 22, 2021.

Kröger, Jacob Leon, Jens Lindemann, and Dominik Herrmann. "How Do App Vendors Respond to Subject Access Requests? A Longitudinal Privacy Study on IOS and Android Apps." In *Proceedings of the 15th International Conference on Availability, Reliability and Security*, 1–10. ARES '20. New York: Association for Computing Machinery, 2020. doi:10.1145/3407023.3407057.

Kruschke, John K. *Doing Bayesian Data Analysis: A Tutorial with R, JAGS, and Stan*. 2nd ed. Amsterdam: Academic Press, 2014.

Kuner, Christoper. *European Data Protection Law: Corporate Compliance and Regulation*. 2nd ed. Oxford: Oxford University Press, 2007.

———. "Data Protection Law and International Jurisdiction on the Internet(Part 1)." *International Journal of Law and Information Technology* 18, no. 2 (June 1, 2010): 176–93. doi:10.1093/ijlit/eaq002.

———. "Reality and Illusion in EU Data Transfer Regulation Post Schrems." *German Law Journal* 18, no. 4 (July 2017): 881–918. doi:10.1017/S2071832200022197.

Kuner, Christopher, Lee A. Bygrave, and Christopher Docksey. "Background and Evolution of the EU General Data Protection Regulation (GDPR)." In *The EU General Data*

This content downloaded from
213.61.224.106 on Tue, 26 Oct 2021 12:38:04 UTC
All use subject to https://about.jstor.org/terms

Protection Regulation (GDPR) — A Commentary, edited by Christopher Kuner, Lee A. Bygrave, and Christopher Docksey, 1–47. Oxford: Oxford University Press, 2020.

Lawford, John. *Consumer Privacy under PIPEDA: How Are We Doing?* Ottawa, Canada: Public Interest Advocacy Centre, 2004. https://www.deslibris.ca/ID/204998. Accessed May 22, 2021.

Lessig, Lawrence. *Code: And Other Laws of Cyberspace*. New York: Basic Books, 1999.

Linden, Thomas, Rishabh Khandelwal, Hamza Harkous, and Kassem Fawaz. "The Privacy Policy Landscape After the GDPR." *Proceedings on Privacy Enhancing Technologies* 2020, no. 1 (January 1, 2020): 47–64. doi:10.2478/popets-2020-0004.

Lynskey, Orla. *The Foundations of EU Data Protection Law*. Oxford, UK: Oxford University Press, 2015.

Mahieu, René L. P., Hadi Asghari, and Michel J. G. Van Eeten. "Collectively Exercising the Right of Access: Individual Effort, Societal Effect." *Internet Policy Review* 7, no. 3 (2018): 1–22. doi:10.14763/2018.3.927.

McElreath, Richard. *Statistical Rethinking: A Bayesian Course with Examples in R and STAN*. 2nd ed. Texts in Statistical Science. Boca Raton, FL: CRC Press, 2020. https://www.routledge.com/Statistical-Rethinking-A-Bayesian-Course-with-Examples-in-R-and-STAN/McElreath/p/book/9780367139919. Accessed May 22, 2021.

McQuinn, Alan, and Daniel Castro. "The Costs of an Unnecessarily Stringent Federal Data Privacy Law." Information Technology and Innovation Foundation, August 5, 2019. https://itif.org/publications/2019/08/05/costs-unnecessarily-stringent-federal-data-privacy-law. Accessed May 22, 2021.

Meese, James, Punit Jagasia, and James Arvanitakis. "Citizen or Consumer? Contrasting Australia and Europe's Data Protection Policies." *Internet Policy Review* 8, no. 2 (2019): 16. doi:10.14763/2019.2.1409.

Moerel, Lokke. "The Long Arm of EU Data Protection Law: Does the Data Protection Directive Apply to Processing of Personal Data of EU Citizens by Websites Worldwide?" *International Data Privacy Law* 1, no. 1 (February 1, 2011): 28–46. doi:10.1093/idpl/ipq004.

———. "Back to Basics: When Does EU Data Protection Law Apply?" *International Data Privacy Law* 1, no. 2 (May 1, 2011): 92–110. doi:10.1093/idpl/ipq009.

Norris, Clive, Paul De Hert, Xavier L'Hoiry, and Antonella Galetta, eds. *The Unaccountable State of Surveillance — Exercising Access Rights in Europe*. Law, Governance and Technology Series 34. Cham, Switzerland: Springer International Publishing, 2017. http://www.springer.com/us/book/97833194757l4. Accessed May 22, 2021.

Office of the Privacy Commissioner of Canada. "What You Need to Know about Mandatory Reporting of Breaches of Security Safeguards." October 2018. https://www.priv.gc.ca/en/privacy-topics/business-privacy/safeguards-and-breaches/privacy-breaches/respond-to-a-privacy-breach-at-your-business/gd_pb_201810/. Accessed May 22, 2021.

Parsons, Christopher, Andrew Hilts, and Masashi Crete-Nishihata. *Approaching Access: A Comparative Analysis of Company Responses to Data Access Requests in Canada*. Research Brief. Toronto, Canada: The Citizen Lab, February 12, 2018. https://citizenlab.ca/wp-content/uploads/2018/02/approaching_access.pdf. Accessed May 22, 2021.

Purtova, Nadezhda. "The Law of Everything. Broad Concept of Personal Data and Future of EU Data Protection Law." *Law, Innovation and Technology* 10, no. 1 (January 2, 2018): 40–81. doi:10.1080/17579961.2018.1452176.

Raento, Mika. "The Data Subject's Right of Access and to Be Informed in Finland: An Experimental Study." *International Journal of Law and Information Technology* 14, no. 3 (2006): 390–409. doi:10.1093/ijlit/eal008.

Rule, James B. "Conclusion." In *Global Privacy Protection*, by James B. Rule and Graham Greenleaf, 257–75. Cheltenham, UK: Edward Elgar, 2008.

This content downloaded from
213.61.224.106 on Tue, 26 Oct 2021 12:38:04 UTC
All use subject to https://about.jstor.org/terms

Schwartz, Paul M. "The EU-U.S. Privacy Collision: A Turn to Institutions and Procedures." *Harvard Law Review* 126, no. 7 (2013): 1966–2009. https://harvardlawreview.org/wp-content/uploads/pdfs/vol126_schwartz.pdf. Accessed May 22, 2021.

———. "Global Data Privacy: The EU Way." *NYU Law Review* 94 (2019): 771–818. https://www.nyulawreview.org/wp-content/uploads/2019/10/NYULAWREVIEW-94-4-Schwartz.pdf. Accessed May 22, 2021.

Scott, Mark, and Laurens Cerulus. "Europe's New Data Protection Rules Export Privacy Standards Worldwide." *Politico*, January 31, 2018. https://www.politico.eu/article/europe-data-protection-privacy-standards-gdpr-general-protection-data-regulation/. Accessed May 22, 2021.

Shaffer, Gregory. "Globalization and Social Protection: The Impact of EU and International Rules in the Ratcheting Up of U.S. Privacy Standards." *Yale Journal of International Law* 25, no. 1 (2000): 1–88. https://digitalcommons.law.yale.edu/yjil/vol25/iss1/2/. Accessed May 22, 2021.

Sloot, Bart van der, and Frederik Zuiderveen Borgesius. "Google and Personal Data Protection." In *Google and the Law*, edited by Aurelio Lopez-Tarruella, 22: 75–111. The Hague, The Netherlands: T. M. C. Asser Press, 2012. doi:10.1007/978-90-6704-846-0_4.

Veale, Michael, Reuben Binns, and Jef Ausloos. "When Data Protection by Design and Data Subject Rights Clash." *International Data Privacy Law* 8, no. 2 (2018): 105–23. doi:10.1093/idpl/ipy002.

Voss, W. Gregory, and Hugues Bouthinon-Dumas. "EU General Data Protection Regulation Sanctions in Theory and in Practice." *Santa Clara High Technology Law Journal* 37 (2021): 1–96. https://digitalcommons.law.scu.edu/cgi/viewcontent.cgi?article=1663&context=chtlj. Accessed May 22, 2021.

Yakovleva, Svetlana. "Privacy Protection(Ism): The Latest Wave of Trade Constraints on Regulatory Autonomy Symposium: Sin Limites: Law & Business at the Gateway to the Americas." *University of Miami Law Review* 74, no. 2 (2020, 2019): 416–519. https://repository.law.miami.edu/umlr/vol74/iss2/5. Accessed May 22, 2021.

This content downloaded from
213.61.224.106 on Tue, 26 Oct 2021 12:38:04 UTC
All use subject to https://about.jstor.org/terms