The Data Privacy Law of Brexit: Theories of Preference Change

*Paul M. Schwartz**

Upon Brexit, the United Kingdom chose to follow the path of EU data protection and remain tied to the requirements of the General Data Protection Regulation (GDPR). It even enacted the GDPR into its domestic law. This Article evaluates five models relating to preference change, demonstrating how they identify different dimensions of Brexit while providing a rich explanation of why a legal system may or may not reject an established transnational legal order. While market forces and a "Brussels Effect" played the most significant role in the decision of the UK government to accept the GDPR, important nonmarket factors were also present in this choice. This Article's models of preference change are also useful in thinking about the likely extent of the UK's future divergence from EU data protection.

Introduction

Data privacy is a topic that is front-and-center in the news and on the agenda of regulatory entities. We live in an age of digital information, and much of this data references and identifies specific persons. Moreover, the economies of the world are intertwined, and global exchanges of personal data are both commonplace and crucial for many international businesses.

In this global digital marketplace, the data protection law of the European Union plays a prominent legal role. In an illustration of the prominence of EU law, a swell of voices worldwide greeted May 25, 2018 as a watershed occasion. On this day, the General Data Protection Regulation (GDPR) took

* Jefferson E. Peyser Professor of Law, UC Berkeley School of Law; Director, Berkeley Center for Law & Technology. I am grateful for the comments and suggestions of John Bowman, Richard R.W. Brooks, David Fang, Stavros Gadinis, Rebecca Goldstein, Rosemary Jay, Kevin Yang, and the editors of Theoretical Inquiries in Law. The Article benefitted from a helpful workshop at Chicago Kent Law School.

Electronic copy available at: https://ssrn.com/abstract=3895999

effect throughout the European Union.[1] Many commenters observed that it represented a law not just for the EU, but for the world.[2] Indeed, most countries with data privacy regimes now follow EU-style data protection law and have enacted similar statutes.

This volume honoring Robert Cooter asks whether the law can change people's preferences. Like so many questions of interest to my brilliant colleague, the issue is one that is complex, multifaceted, and elusive. In his work, Professor Cooter posits an idealized case of Pareto optimal preferences.[3] In his view, people can and will change their own preferences to improve them. Legal sanctions can prompt a rational person to modify her proclivities.[4]

Professor Cooter's intriguing work unpacks how the law shapes the internalization of individual values. In this Article, I wish to go beyond individual preferences and explore how legal systems choose among competing legal norms. Posed at this level of abstraction, the issue is how a social system decides on its normative commitments and engages in a legal expression of them. In particular, how can an available foreign legal model affect preferences within a different legal system?

Extensive scholarship has studied small groups and their ability, at least at times, to develop efficient rules for cooperation.[5] Moreover, Professor Cooter has noted that the common law itself has developed "a surprising level of efficiency" in its rules.[6] In this Article, in contrast, I consider not why people obey the law, or how they internalize its rules, but why an entire legal order might select one set of rules over another. The test case for this analysis will be data privacy law, and this Article will focus on the choice by the UK during Brexit to continue following the EU's data protection law.

At this juncture, a few words are helpful about terminology. First, "data protection" is the accepted, standard term applied to Europe's extensive body of law concerning the processing, collection, and transfer of personal

---

1 Commission Regulation 2016/679, Art. 99(2), 2016 O.J. (L 119) 1, 87 (EU) [hereinafter GDPR].

2 *See* Paul M. Schwartz, *Global Data Privacy: The EU Way*, 94 N.Y.U. L. Rev. 771 (2019) (describing how recent EU privacy laws have a global impact).

3 *See* Robert Cooter, *Models of Morality in Law and Economics: Self-Control and Self-Improvement for the "Bad Man" of Holmes*, 78 B.U. L. Rev. 903 (1998).

4 *Id*.

5 *See, e.g.*, Robert C. Ellickson, Order Without Law: How Neighbors Settle Disputes (1991); Lisa Bernstein, *Opting Out of the Legal System: Extralegal Contractual Relations in the Diamond Industry*, 21 J. Legal Stud. 115 (1992). For Robert Cooter's insightful review of Ellickson's book, see Robert D. Cooter, *Against Legal Centrism*, 81 Calif. L. Rev. 417 (1993).

6 Cooter, *supra* note 3, at 909.

Electronic copy available at: https://ssrn.com/abstract=3895999

data. In the United States, we lack such a single, universally accepted term, but generally refer to this field of law as "information privacy." When this Article discusses the concept in neutral terms, it will refer to "data privacy" or "privacy." Thus, "data privacy" may refer to this area generally, or to the emerging body of transnational law to which many countries have contributed.

This Article will explore five models for possible preference change. First, Robert Cooter hypothesizes that legal sanctions can prompt a rational person, or presumably a rational legal system, to modify existing preferences.[7] The Cooter model is the model of "law-driven preference change." Second, and with particular reference to the UK, one can imagine that the UK's legal preferences and the EU's own values were in synch. This Article develops this paradigm, which it terms the "alignment model." Third, and as a related matter, a process of "persuasion or acculturation" of values may have caused the UK's legal preferences regarding its data protection law over time to accord with that in the EU.[8] Fourth, Anu Bradford has identified the "Brussels Effect," in which other countries change their regulation because a variety of market factors make the choice to follow the EU's regulation an optimal one.[9] The Brussels Effect proposes a market-driven model enhanced by the EU's regulatory capacity and other factors. Fifth, Alan Watson has identified the "accessibility" of a foreign law model as a key element in whether or not it will be adopted by another legal order.[10] As will be set out below, these models can overlap under real-world conditions.

This Article will evaluate these five possible explanations for the UK's decision to continue following the path of EU data protection. In focusing on Brexit and data protection, this Article looks at a question that is different from the classic question in comparative law, which is the transfer or transplant of a legal concept from one nation to another. At the time of Brexit, the UK had already accepted EU data protection law. In the ordering of world data privacy systems, the UK, from its first data protection statute to its current law, has been firmly grounded in the EU and not the U.S. camp. Thus, in light of the successful transfer of EU law to the UK, the critical issue for the latter was deciding whether to engage in an "untransfer," or rejection, of EU-style data protection law.

In *Moby Dick* (1851), Herman Melville devotes two chapters to explaining whale law and concludes with the assurance, "[T]here seems a reason in all

---

7 *Id*.

8 Ryan Goodman & Derek Jinks, *How to Influence States: Socialization and International Human Rights Law*, 54 Duke L.J. 621 (2004).

9 Anu Bradford, The Brussels Effect (2020).

10 Alan Watson, Legal Transplants 94 (2d ed. 1993).

Electronic copy available at: https://ssrn.com/abstract=3895999

things, even in law."[11] This Article explores the data privacy law of Brexit and identifies reasons for the path taken by the UK as well as a series of open issues for the future. The chosen UK solution was not to "take back control" of data protection law, but to carry out a maximalist adoption of EU law in this area. In explaining the retention of EU data protection law under Brexit, this Article does not point to a single winning model of preference change, but finds that each of the five models makes a distinct contribution to understanding the UK's actions. The situation recalls another novel, not *Moby Dick*, but Agatha Christie's *Murder on the Orient Express* (1934).[12] In this whodunit (spoiler alert), the great Belgian detective Hercules Poirot realizes that all twelve passengers contributed to the murder. Here, we have five contributors to an outcome, and each of the models adds to our understanding of the retention of EU data protection law during Brexit.

The Article proceeds as follows: Part I sets out the five theoretical models of legal preference change, and then considers the basic approaches to data privacy law on the world stage, which are those of the EU and the U.S. Understanding these two alternatives sets the stage for a section looking at the rise of UK data protection law in the 1980s and its enactment of a European-like statute. This initial period demonstrates a market-driven choice by the UK as well as the high quality of EU data protection and its appeal as a model for transplantation.

In Part II, the Article looks at Brexit and the GDPR. Breaking up is hard to do, as an old song would have it, and the UK decided to adopt the GDPR as its post-Brexit approach to data protection. This choice is perhaps puzzling in light of the rhetoric of "Take Back Control," and this Article assesses it against its models of preference change. In Part III, the focus is on future tensions in the relationship around data protection law between the EU and the UK and how concepts of preference change may help predict the UK's future behavior.

I. Data Privacy and Preference Change

In thinking about how the data privacy law of one legal system might change the preferences in a different legal order, there are a number of factors that might play a role. With particular reference to the UK, this Article considers two time spans in assessing this issue. The first is the period in the 1980s during which the UK first adopted EU-style data protection law. The second

11 Herman Melville, Moby Dick, ch. 90 (1851).

12 Agatha Christie, Murder on the Orient Express (1934).

Electronic copy available at: https://ssrn.com/abstract=3895999

concerns the time of Brexit. We now consider five potential models for possible preference change.

A. Law and Preferences: Theoretical Models

Under the first approach, Cooter's theory, EU data protection would have changed individual preferences in the UK. This result follows from the law encouraging and shaping better behavior and individuals internalizing the lesson.[13] Under such "Pareto self-improvement," people change themselves to be better off as measured by both their old and new preferences, and such "socialization is an essential, necessary effect of law."[14] Legal sanctions can prompt a rational person to modify her preferences as part of this process.[15] Like Cooter, and from a similar perspective, Ariel Porat has proposed that the law can maximize social welfare by changing preferences.[16]

It is an appropriate extension of Cooter's theory to apply it not to a person, but to a legal system. The idea here is to look at the actions of leaders of law and policy, and not at the preferences of the mass population. Indeed, the idea of the "common law working itself clean" suggests, as Cooter writes, that the common law itself evolves toward efficiency as "judges selectively enforce social norms."[17] Extended to a legal system, the modified Cooter idea would be that a foreign law might change the underlying preferences in the target nation's legal order. Thus, the existence of EU data protection law might have modified UK legal preferences. This process would reflect a rational choice for improvement of the UK legal system regarding its data privacy law.

Here, as noted above, this Article draws a distinction with Cooter's attention to individuals. It focuses on the decision-making in a legal system, that is, it looks to legal elites and influential policymakers and explores the preferences resulting within the UK legal system itself. One can posit that a legal system might find that a foreign approach aligns with its own regulatory wishes and choose to follow it. Perhaps the most famous example of such an adoption is Japan's decision in 1896 to adopt the German Civil Code, the *Bürgerliches Gesetzbuch*, and to do so even before that law took effect in Germany. It did

---

13 *See* Cooter, *supra* note 3.

14 *Id.* at 919.

15 *Id*.

16 Ariel Porat, *Changing People's Preferences by the State and the Law*, 22 Theoretical Inquiries L. 215 (2021).

17 Cooter, *supra* note 3, at 910.

Electronic copy available at: https://ssrn.com/abstract=3895999

so under the rubric of "modernization" and because of a desire to follow Western legal models.[18]

Like Professor Cooter, however, privacy law has typically focused on individual preferences rather than those of the legal system or legal elites. Regarding attention to public opinion, Samuel Warren and Louis Brandeis in their famous article, *The Right to Privacy*, raised a warning about printed gossip in newspapers. In their concise conclusion, "[T]he supply creates the demand."[19] Writing in 1890, Warren and Brandeis were worried that a new supply of trashy reporting was stimulating a public demand for more of it. The two authors advocated for a new tort, a right of privacy, to stop the "lowering of social standards and of morality."[20] This tort was to change and improve personal preferences. In correspondence to his future wife, in the same year as the publication of *The Right to Privacy*, Brandeis observed, "All law is a dead letter without public opinion behind it. But law and public opinion interact — and they are both capable of being made."[21] This process of interaction between law and public opinion also can be international in scope, with foreign legal models increasingly available today for scrutiny and adoption.

Privacy law itself relies on the views of the public, most famously in its use of the test of "highly offensive" in three of the four privacy torts. One of these torts requires a jury to find, for example, that an invasion on seclusion is "highly offensive to a reasonable person." Through this test, the privacy tort integrates the views of the public into law and reflects evolving social norms regarding "rules of civility," as Robert Post has explained.[22] In other areas, however, there may be a divide between the preferences of the legal system and those of the public. Hence, the Cooter model can be used to introduce a novel idea into privacy law, which is that a legal system might change its privacy preferences through Pareto self-improvement.

Second, under the alignment model, a concept that this Article develops, the UK's preferences in this area might have already been in sync with those in the EU in the 1980s. Two strangers can discover similar tastes in movies,

---

18 Zentaro Kitagawa, *Development of Comparative Law in East Asia*, *in* The Oxford Handbook of Comparative Law 237, 240 (Mathias Reimann & Reinhard Zimmermann eds., 2008).

19 Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 Harv. L. Rev. 193, 196 (1890).

20 *Id.*

21 Louis D. Brandeis, *Letter of December 28, 1890*, *in* 1 Letters of Louis D. Brandeis 97 (Melvin I. Urofsky & David W. Levy eds., 1971).

22 Robert Post, *The Social Foundations of Privacy: Community and Self in the Common Law Tort*, 77 Cal. L. Rev. 957 (1989).

Electronic copy available at: https://ssrn.com/abstract=3895999

music, or food, which might even be a good basis to start a friendship. Pursuant to this explanation, the UK adopted EU privacy law because it reflected underlying or immanent values in the UK, which its domestic law had not yet successfully expressed.

As a related third model, UK law may have internalized the model of EU law *after* adoption due to a process of "persuasion or acculturation." Ideas and ideology have power and, with or without a heavenly light, scales can fall from eyes, and minds can change. As a result, by the time of Brexit, the UK may have come to accept EU privacy law. As for the internal mechanism of such an alteration of preferences, Ryan Goodman and Derek Hinks have developed a useful legal theory of "persuasion" and "acculturation."[23] In the explanation of Goodman and Hinks, whereas "persuasion requires active assessment of the merits of an idea," acculturation involves tacit acceptance due to a "degree of identification" between "the target audience and some group."[24] The two processes can be tied to each other. Goodman and Hinks write, "[A]cculturation may serve as the cultural predicate for all acts of persuasion."[25] Under this third model, the UK might have experienced preference change due to the power of data protection as a value system. For example, Steven Weber and Bruce Jentleson describe a global competition of ideas "built around an evolving digital infrastructure that increasingly connects everyone to everyone."[26] Weber and Jentleson present this competition as "an essential ingredient of international politics."[27] EU data protection law in the 1980s might have seemed a peerless point of reference for the UK.

This Article's fourth model is Bradford's Brussels Effect. Bradford has identified factors that underpin the EU's global influence. In her view, "[T]he EU remains an influential superpower that shapes the world in its image."[28] What are the elements of Bradford's Brussels Effect? First, the Brussels Effect will become prevalent based on a large domestic market, a relative amount of regulatory capacity in the area, and the political will to create stringent rules. Moreover, the Brussels Effect depends on the presence of inelastic markets, such as a consumer market as opposed to a capital market. As an additional element of Bradford's model, EU standards become powerful only if a company's service or product is non-divisible — that is, when it is more beneficial for the

---

23 Goodman & Jinks, *supra* note 8, at 621-31.

24 *Id.* at 643.

25 *Id.* at 644.

26 Steven Weber & Bruce W. Jentleson, The End of Arrogance: America in the Global Competition of Ideas 12 (2010).

27 *Id.* at 8.

28 Bradford, *supra* note 9, at xiii.

Electronic copy available at: https://ssrn.com/abstract=3895999

company to adhere to a single standard rather than to customize for different markets.[29] Interestingly enough, Bradford separates the "normative power" of EU rules from the Brussels Effect. For her, the attractiveness of EU rules can nonetheless increase their appeal as a "virtuous example."[30]

Further, Bradford points to two categories of Brussels Effect: "de facto" and "de jure." A "de facto" one occurs when companies shape global production and conduct to follow EU regulations, and a "de jure" Brussels Effect takes place when "foreign governments are emulating EU regulations domestically."[31] For Bradford, moreover, the example of strong EU data protection is a prime example of the influence of the EU. She observes, "data protection [is] a powerful manifestation of the Europeanization of the global regulatory environment."[32] Applied to Brexit, Bradford's theory posits that market forces would drive the adoption of EU standards in this area. Yet, the UK had long adopted and practiced EU data protection law *before* Brexit. Hence, this Article must analyze the initial period of the emergence of UK data protection, which culminated in the enactment of that country's first data protection law in 1984.

One remaining model for preference change remains. Our fifth factor is the extent to which a foreign legal model is accessible. In his work on "legal transplants," that is, "the moving of a rule or a system of law from one country to another," Alan Watson has emphasized the importance of accessibility in whether or not a foreign jurisdiction will adopt another country's law. By being able to take over an available legal rule or system, the borrower is spared "the awful labor of thought."[33] This search for efficiency means that the more accessible a potential legal transplant might be, the greater its chances of adoption. One can imagine all or some of the four preceding models initially serving as catalysts for preference change, and the fifth model then serving as a gatekeeper or "reality check" as to whether the sought-after foreign law could be transplanted easily. In other words, accessibility makes a transplant more likely by making it appear "doable."

Consider the adoption of the common law in the United States. For Watson, it was immeasurably assisted by the presence of numerous abridged editions of Blackstone for students. This volume "covered all the law" and "was comprehensive, cheap, and convenient for slipping into saddlebags."[34] Accessibility also matters under federalism. In the United States, where

---

29 *Id.* at xvii-xvii.
30 *Id.* at 81.
31 *Id.* at xviii.
32 *Id.* at 132.
33 Alan Watson, *Aspects of Reception of Law*, 44 Am. J. Comp. L. 335 (1996).
34 Watson, *Legal Transplants*, *supra* note 10, at 94.

Electronic copy available at: https://ssrn.com/abstract=3895999

certain matters are reserved to the states, a first-mover state has a built-in advantage by presenting a model that can be copied. In their detailed survey of privacy bills, for example, Anupam Chander, Margot Kaminski, and William McGeveran find that the recently enacted California Consumer Privacy Act is already exerting a strong influence on other states.[35]

As a caveat regarding these five models, they are ideal types, and one can expect overlap among them in the real world. Beyond the interplay of these factors, there is another useful suggestion from Watson, who stresses how chance can play a significant role in legal change due to the unplanned interaction of various influences. He asks, "What would have been the impact on American law if Chancellor Kent had read German?"[36] Had that been the case, Watson believes that the Continental influence on U.S. common law would have been greater. Indeed, Louis Brandeis did read German, and he relied on the Continental model of "personality rights" in developing his idea of the "right to privacy."[37]

Watson points to a further aspect of how chance can affect the adoption of foreign legal systems. While he believes that "patterns of development can be discerned," Watson remains skeptical about the ability of model-makers to predict the future. As a country singer once put it more dramatically, "There's no future in the past."[38] Bygone events only offer limited help in identifying the shape of times yet to come. This Article now explores the process by which the UK initially adopted EU data protection in the 1980s. Put differently, we begin by considering the available choices before UK decision-makers at that time. In other words, what was the available "inventory" of data privacy law among which the UK could choose?

B. Data Privacy Law: The EU and U.S. Approaches

In his comparative law scholarship, Günter Frankenberg uses the metaphor of a "constitutional Ikea," where "shoppers" can select finished products from another legal system, or pick elements from foreign law to put together

---

35 Anupam Chander et al., *Catalyzing Privacy Law*, 105 Minn. L. Rev. 1733, 1781 (2021).

36 Watson, *Aspects*, *supra* note 33, at 350.

37 Warren & Brandeis, *supra* note 19, at 207. At the age of 16, Brandeis' family moved to Europe, and young Louis Brandeis attended the Annen-Realschule in Dresden, Germany for three terms, during which he took "twelve courses at a time." Melvin I. Urofsky, Louis D. Brandeis: A Life 22 (2012).

38 Vince Gill, No Future in the Past (MCA Records 1992).

Electronic copy available at: https://ssrn.com/abstract=3895999

themselves and integrate into their national law.[39] In deciding on a data privacy system in 1984, the UK was faced with a "privacy Ikea," that is, there were different established approaches in the EU and in the U.S. Despite the UK's shared common law background with the U.S., it decided to follow the path of EU data protection rather than U.S. information privacy. In analyzing why the UK made this choice, this Article begins by sketching the chief differences between the EU and U.S. regarding data privacy.

In the EU, data protection is based on a human-rights perspective.[40] The EU engages in a right-focused legal discourse that is centered on the individual whose data are processed.[41] Data protection is a fundamental right anchored in interests of dignity, personality, and self-determination.[42] European judicial institutions both within and outside of the EU protect these rights. The key institutions are the Court of Justice of the European Union (CJEU) and the Council of Europe's European Court of Human Rights (ECtHR).[43]

Beyond these courts, other important institutions play an essential role in EU data protection. These organizations include national data protection commissions in each EU member state. In its *Schrems I* decision, the CJEU found that the independence of these officials was constitutionally safeguarded.[44] The European Data Protection Supervisor and the European Data Protection Board fulfill important institutional roles in data protection. A so-called "omnibus law," the GDPR, provides the central legislative element of EU data protection. This regulation binds both the public and private sectors and is further supplemented by more specific EU and national laws, such as the

---

39 Günter Frankenberg, Comparative Constitutional Studies: Between Magic and Deceit 125 (2018).

40 Paul M. Schwartz & Karl-Nikolaus Peifer, *Transatlantic Data Privacy Law*, 106 Geo. L.J. 115 (2017).

41 *Id.* at 138-40.

42 *Id.*

43 These are two different courts that are part of two different political entities. The EU terms itself a "unique economic and political union between 27 EU Countries that together cover much of the continent." *The EU in Brief*, Eur. Union, https://europa.eu/european-union/about-eu/eu-in-brief_en. Among the tasks of the CJEU is to interpret EU law to make sure it is applied uniformly by EU member states, and to settle disputes between EU institutions and national governments. The Council of Europe seeks to promote human rights and has 47 member states. The ECtHR oversees the implementation of the Convention of Human Rights by its signatories, which are all the Council of Europe's member states. European Union Agency for Fundamental Rights, Handbook on European Data Protection Law 22-27 (2018).

44 Case C-362/14, Schrems v. Data Prot. Comm'r, 2015 E.C.R. 1-1, at 96-98.

Electronic copy available at: https://ssrn.com/abstract=3895999

Data Protection Law Enforcement Directive, and the ePrivacy Directive, which is now slated to be replaced by an ePrivacy Regulation. In areas left open to the member states, national data privacy laws fill in significant gaps.

In the U.S., information privacy law is anchored in the marketplace. While the EU uses the term "data subject" for the object of its protection, U.S. law generally envisions a "privacy consumer," and one not protected by any strong right to data privacy.[45] The privacy consumer of the U.S. participates in a series of free exchanges of her personal data. In this legal universe, the rhetoric of bilateral self-interest holds sway. Personal information is another commodity in the market, and the focus of information privacy is policing fairness in exchanges of personal data.[46]

As for its legal framework, the U.S. lacks an omnibus privacy law. It has long proceeded through a patchwork of sectoral laws limited to a specific industry or to specific categories of personal data. The following examples will demonstrate the gaps that occur in this system. Through HIPAA,[47] U.S. information privacy law regulates healthcare information processed by healthcare providers or insurers, but not data collected by fitness trackers.[48] FERPA[49] regulates educational records if stored by schools or universities that receive federal funding, but does not reach a variety of edtech software and devices.[50] The Gramm-Leach-Bliley Act[51] regulates personal data use by "financial institutions," a term of art statutorily defined, which leaves at least

---

45 Schwartz & Peifer, *supra* note 40, at 115.

46 *Id.*

47 Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936 (codified as amended in scattered sections of 18, 26, 29, and 42 U.S.C.).

48 The personal data protected by HIPAA is called "protected health information" (PHI), which is defined as information that "is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse" and "relates to the past, present, or future physical or mental health or condition of any individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual." 45 C.F.R. §160.103.

49 Family Educational Rights and Privacy Act of 1974, Pub. L. No. 93-380, 20 U.S.C. §1232g.

50 FERPA defines "[e]ducation records" as "those records, files, documents, and other materials which contain information directly related to a student; and are maintained by an educational agency or institution." 20 U.S.C. § 1232g(a)(4)(A).

51 Gramm-Leach-Bliley Act of 1999, Pub. L. No. 106-102, 15 U.S.C. §§ 6801-6809.

Electronic copy available at: https://ssrn.com/abstract=3895999

some fintech organizations outside its regulatory scope.[52] As for constitutional law in the U.S., it plays a comparatively small role in protecting information privacy.[53] For one thing, U.S. constitutional rights generally limit only "state action," and leave the private sphere outside of their reach when it comes to information privacy.[54]

Finally, regarding institutions, the U.S. lacks a mandated data protection authority, although the Federal Trade Commission (FTC) has assumed the mantle of the nation's leading privacy cop. Established in 1914, the FTC is an agency tasked with consumer protection as well as oversight over competition issues. As a functional matter, the FTC falls short of the classic role of an EU data protection authority. For one thing, it cannot generally impose penalties for privacy violations unless a company is already under an FTC order for previous misbehavior.[55] In the context of information privacy, the FTC typically issues these orders as part of a settlement with an offending organization. It has also, on occasion, litigated privacy matters when unable to reach a settlement agreement with the offending party.[56] Moreover, there is no general federal data privacy law for the FTC to enforce. There are also substantial limits on its jurisdiction and on its general rulemaking authority for privacy and security.

C. The Rise of the UK Data Protection Act: the 1984 Statute

As a historical matter, the UK developed its data protection regime relatively late. Colin Bennett has noted how the enactment of the Data Protection Act of

---

52 *See* 15 U.S.C. § 6809(3)(A).

53 In *Whalen v. Roe*, 429 U.S. 589, 598-600 (1977), the Supreme Court extended its substantive due process privacy protection, holding that the "zone of privacy" protected by the Constitution encompasses the "individual interest in avoiding disclosure of personal matters." *See* Daniel J. Solove & Paul Schwartz, Information Privacy Law 585-89 (7th ed. 2020) (discussing the reluctance of the Supreme Court to further develop this right to information privacy in subsequent cases).

54 *See Whalen*, 429 U.S. at 598 n.23 (noting that the right of privacy is grounded in the Fourteenth Amendment's concept of personal liberty, which means that the Constitution's restriction of its protections to state action will apply).

55 On the limitations on the FTC's power, see Chris Jay Hoofnagle, Federal Trade Commission Privacy Law and Policy 334-35 (2016); Jessica Rich, *Give the F.T.C. Some Teeth to Guard Our Privacy*, N.Y. Times (Aug. 12, 2019), https://www.nytimes.com/2019/08/12/opinion/ftc-privacy-congress.html.

56 *See, e.g.*, LabMD v. Federal Trade Commission, 894 F.3d 1221 (11th Cir. 2018); FTC v. Wyndham Worldwide Corporation, 799 F.3d 236 (3d Cir. 2015).

Electronic copy available at: https://ssrn.com/abstract=3895999

1984 was preceded by "procrastination and controversy not seen to the same extent elsewhere" in the world.[57] Two British advisory groups, the Younger (1970) and Lindop committees (1978), first examined issues of privacy before Parliament enacted its first data protection law in 1984.[58] This statute appeared over a decade after continental Europe had its first wave of data protection lawmaking, and the UK's adoption of this law was a direct response to these foreign law developments, in particular to the threat of data embargo orders.

The UK Data Protection Act became law in George Orwell's titular year of 1984. Elsewhere in the world, early trends of computerization and concerns about the processing of personal information led to a wave of data privacy laws in the 1970s.[59] One might imagine that the UK joined the data privacy club at last in 1984 because of its rising consciousness of surveillance issues. But, more than any other factor, Parliament enacted the Act because it was concerned about the economic consequences of *not* having a data protection regime. In the concise conclusion of Bennett, "The economic motive was predominant."[60]

The UK legislated against a background of emerging national data protection laws in Europe and a Council of Europe Convention that allowed nations to block data transfers to countries without adequate protection. It was less worried about privacy than about the economic impact of data embargo orders from Europe.[61] First-generation laws in Europe had taken different approaches to stopping international transfers of the personal information of their citizens, but shared a basic policy decision to keep these transmissions from weakening domestic privacy protections. In an age of international data flows, national measures for individual privacy would be doomed to failure if their reach ended at the borders of each country. As a result, the data protection laws of most European nations by 1984 required an equivalent level of protection in a recipient nation before permitting an international data transfer to it.[62] As Rosemary Jay notes in her treatise on UK data protection law,

> There were rumblings from some of those states which had adopted data protection controls in the 1970s which suggested that they might

---

57 Colin J. Bennett, Regulating Privacy 82 (1992).

58 *Id.* at 40-90.

59 For an account of the developments during this period, see Simits et al., *Einleitung [Introduction]*, *in* Datenschutzrecht: DSGVO mit BDSG 179-180 [Data Protection Law: GDPR with BDSG] (2019) (Ger.).

60 *Id.* at 42.

61 *Id.*

62 Paul M. Schwartz, *European Data Protection Law and Restrictions on International Data Flows*, 80 Iowa L. Rev. 471, 474-75 (1995).

Electronic copy available at: https://ssrn.com/abstract=3895999

> seek to restrict the movement of data about their citizens, to ensure that such data remained within jurisdictions in which the legal systems provided protection for their subjects' "informational freedoms."[63]

Thus, national data protection laws on the Continent threatened the UK's access to personal data, and, in turn, risked a negative impact on its service industry and IT sector.

Then, in 1981, the Council of Europe's Convention 108 took a decisive step to encourage blocking of international data transfers in the absence of data protection in the recipient nation. Convention 108 is a treaty that requires signatory nations to establish domestic data protection legislation that gives effect to its principles.[64] It contains a core set of privacy principles that are to govern data processing. This treaty also permits, but does not require, signatory nations to restrict transborder flows of personal data to nations that do not "provide an equivalent protection."[65] Note, too, that the Convention predates the EU's own involvement in data privacy, which began with the 1995 Data Protection Directive. This legal act took effect in 1998 and required EU member states to implement its requirements into their national law.

These elements of the Council of Europe Convention 108 and national data protection law proved decisive to the stalled UK policy discussion. In the UK, a Conservative government led by Prime Minister Margaret Thatcher, building on the work of the two advisory groups and a legislative proposal from the recently toppled Labor government, quickly enacted the Data Protection Act. As Jay writes, "[T]he threat of trade barriers galvanized the government of the day into action" and led to the enactment of the 1984 law.[66]

The resulting statute was one squarely in the European mold. It is an omnibus law that established a group of eight principles that all data processors were to follow.[67] The 1984 statute set up a series of rights for "data subjects," and required special protection for "sensitive" data. As is typical of the European approach, it also prohibited processing of personal data without a legal basis for doing so.

As further evidence of its following the European path, the UK Data Protection Act of 1984 required data registration by data processing entities.[68] Some first-generation data protection laws took this approach, others did not.

---

63 Rosemary Jay, Data Protection Law and Practice 7 (4th ed. 2012).

64 Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Jan. 28, 1981, E.T.S. No. 108.

65 *Id.* at Art. 12(3)(a). For a discussion, see Schwartz, *supra* note 62, at 478.

66 Jay, *supra* note 63, at 10.

67 For a discussion of the 1984 Act, see *id.* at 12-13.

68 Jay, *supra* note 63, at 382-386.

Electronic copy available at: https://ssrn.com/abstract=3895999

The French Data Protection Act of 1978 is the leading example of a registration law; the German laws from the same period, state and federal, did not require registration.[69] Here is another example of how the UK deviates from the orientation of U.S. information privacy law. A requirement of registration with a governmental agency before the processing of personal data would be entirely inconsistent with free speech traditions in the United States.[70]

Finally, the UK law of 1984 establishes a process for governmental issuance of "transfer prohibition notices." It permits such data embargo orders when personal information is to be transferred out of the UK and "the transfer is likely to contravene, or lead to a contravention of, any of the data protection principles."[71] Here, too, the UK was placing itself into the European camp. U.S. information privacy law has never contained such a requirement for the transfer of personal data outside the U.S.

D. Preference Formation in the UK's Initial Adoption of EU Data Protection Law

How then does the UK's adoption of EU data protection law look when assessed with the different models of preference formation? Regarding its enactment of a European-friendly statute in 1984, the UK was acting due to market considerations. First-generation data protection laws in Europe had created potential trade barriers, and the UK joined the club of European data protection nations to guarantee access to a lucrative consumer market with rich personal data.

First, regarding the Cooter model, the EU had not changed the underlying values in the UK through a process of Pareto self-improvement by individuals. Unlike a smoker who turns against his old habit, the Data Protection Act of 1984 did not reflect a change in underlying beliefs about data privacy. Rather, there was a fear that "the country's computers would stand idle because of a new nontariff trade barrier imposed by [the UK's] trade partners."[72] European law cannot be said to have altered internal UK domestic values regarding privacy.

---

69 Current French law has largely abolished its filing requirements, but UK data protection law to this day contains a registration requirement. *See Data Protection Laws Of The World: Registration*, DLA Piper, https://www.dlapiperdataprotection.com/index.html?t=registration&c=FR&c2=GB (last visited July 18, 2020).

70 *See* NAACP v. Alabama, 357 U.S. 449 (1958) (unanimous opinion invalidating an Alabama requirement that the NAACP share its membership list as part of the process of doing business in the state).

71 Data Protection Act 1984, c. 35, § 12(2) (UK).

72 Bennett, *supra* note 57, at 91.

Electronic copy available at: https://ssrn.com/abstract=3895999

Second, regarding alignment, the UK legal system did not follow EU data protection law because it already had a preference for the values it expressed. The UK did not, for example, decide that the human rights approach to data privacy was an idea inherent in British data privacy yet unexpressed in domestic law. It chose to synch its law with the European because of economic benefits regarding continuing access to personal data from the continent.

As for the third model, there also is a lack of evidence of a process of "acculturation" or "persuasion" prior to the period of adoption. In accounts of this period, key British policymakers do not express support for the values of European data protection. In addition, parts of the UK political establishment at the time already had an uneasy relationship with the larger European human rights regime. We return to this point below, as this reluctance towards fundamental rights from the continent continues to this day among UK elites.

Fourth, as for the Brussels Effect, the adoption of European data protection by the UK *predated* the EU's own involvement in this area. Influential member states of the EU had enacted national data protection laws, but the European Data Protection Directive did not appear until 1995 and would not take effect until 1998. And the GDPR would not see the light of day until 2016 and would not enter into force until 2018. Strictly speaking, therefore, the UK's adoption of the Data Protection Act in 1984 might be considered the result of a "pre-Brussels Effect," or a "Strasbourg Effect." The UK Data Protection Act was enacted in response to strong market forces in Europe; the presence of economically valuable non-divisible services or products on the continent; and laws in individual member states and a treaty from the Council of Europe that permitted the imposition of data embargos to countries with insufficient national privacy protections.

For more on the concept of a "Strasbourg Effect," we can reference recent scholarship by Lee Bygrave. In 2020, Bygrave looked back at the enactment of the Council of Europe's Convention on Data Protection of 1981 and found that the Council "has been enormously influential in shaping regulatory discourse in the field, primarily within Europe but also beyond."[73] For Bygrave, the Strasbourg Effect is primarily an expression of the Council of Europe's "promotion of human rights," which is the core of the Council's mission.[74] Bygrave also argues that while Bradford's Brussels Effect "is fundamentally a market-powered process," the Strasbourg Effect "is fundamentally a treaty-

---

73 Lee Bygrave, *The "Strasbourg Effect" on data protection in light of the "Brussels Effect,"* Computer L. & Sec. Rev. (Oct 2020), at https://www.sciencedirect.com/science/article/pii/S0267364920300650.

74 *Id.*

Electronic copy available at: https://ssrn.com/abstract=3895999

based process with relatively scant opportunity to leverage off market power."[75] Looking to the future, he predicts that "hard-nosed economic factors, such as being able to promote consumer spending or access a lucrative market, will play a significant role in getting many governments and businesses outside Europe to pay heed to" the Convention 108 in its modernized format.[76]

The 1981 Convention did play an important role in the UK's adoption of European data protection law. This Article also proposes a modest correction to Bygrave's notion of the Strasbourg Effect as historically driven by a human rights discourse. The Strasbourg Effect always had a dimension beyond the Council's promotion of human rights. The UK chose to follow European data protection law in 1984 as an early example of a market-driven influence, and one that tracks Bradford's Brussel Effect. Moreover, as Spiros Simitis has observed, the 1981 Convention played a decisive role in the future development of European data protection law. It summarized the most important fundamental principles present then in national data protection statutes, and "burst the framework of isolated, national reactions" regarding the necessary creation of "legally binding regulation for the processing of personal data."[77] In the future, each of the Convention's principles was to be regarded as "a part of internationally accepted rules of conduct."[78]

Finally, there is the question of the accessibility of EU data protection law. Compared to the patchwork of U.S. privacy law, European data protection statutes in their first generation and beyond have offered an attractive model for adoption. One might take the French statute of 1978 as an example. This law covered public and private sector data processing while occupying only five pages, albeit in small print and double columns, as published in the *Journal Officiel de la République Française*.[79] In enacting a similarly concise piece of legislation, the UK could in one fell swoop have a functioning statute for data privacy. In contrast, were the UK to transplant the U.S. approach, it would be obligated to enact several laws, and still be left with many sectors of troubling personal data use free of regulation. Another flaw of the U.S. path in

---

75 *Id*.

76 *Id.*

77 Spiros Simitis, *Einleitung: Geschichte – Ziele – Prinzipien [Introduction: History – Goals – Principles]*, *in* Bundesdatenschutzgesetz [Federal Data Protection Act] 81, 137 (Spiros Simitis ed., 8th ed. 2014) (Ger.).

78 *Id.*

79 Loi no 78-17 du 6 janvier 1978 relative a l'informatique, aux fichiers et aux libertes [Law 78-17 of Jan. 6, 1978 on Information Technologies, Data Files and Civil Liberties] 110 Journal Officiel[J.O] [Official Gazette of the French Republic], Jan. 7, 1978, P. 227-231 (Fr.).

Electronic copy available at: https://ssrn.com/abstract=3895999

the 1980s was that the UK could not find a model of effective oversight in the U.S. At that time, the FTC had yet to involve itself in the area of data privacy.[80]

In sum, the rise of the UK Data Protection Act reflects a market-based decision and the superiority of EU data protection as a model for transplantation. It reflects neither individual Pareto self-improvement by individuals; nor an existing alignment of values between the EU and UK; nor a deep-seated "acculturation" or "persuasion" regarding a human rights approach to privacy. We now turn to the time of Brexit, which occurred decades after this initial period, and raised a new issue, namely the merits not of *adoption*, but of *rejection* of EU data protection.

II. Brexit and the GDPR

In departing the EU after forty-seven years of membership, the UK generated a host of questions about the future legal relationship between the two entities. Upon Brexit, the UK also became a "third country" for purposes of EU data protection and faced the same questions regarding adequacy of protection as any country outside the EU that lacks a formal adequacy finding. As a member of the EU, the UK was considered to have adequate data protection and could receive transfers of personal information from any EU member state. Once outside this circle, however, as a "third country," the UK would not receive these transfers without fulfillment of additional requirements and additional scrutiny.

Faced with looming "third country" status, the UK decided that it needed to meet the overarching policy goal of ensuring flows of data post-Brexit between the UK and the EU. The government announced that its policy would be to ensure that these flows were "unhindered and uninterrupted."[81] This goal required a careful coordination of different legal mechanisms to anchor the GDPR into UK law before, during, and after Brexit. This Part examines these actions and analyzes the elaborate steps taken in the UK to adopt the GDPR. It then returns to this Article's models of preference change and assesses them against Brexit.

---

80 In his authoritative account of the FTC as a privacy regulator, Christopher Hoofnagle located the start of the FTC's activities in this area to a 1995 policy statement from it. The first FTC enforcement actions followed then a few years later. Hoofnagle, *supra* note 55, at 145.

81 European Union Comm., House of Lords, Brexit: The EU Data Protection Package 50 (2017).

Electronic copy available at: https://ssrn.com/abstract=3895999

A. The Mechanisms of Brexit and UK Data Protection

As it faced becoming a "third country" for data protection, the UK decided to become the non-EU nation that most closely follows EU data protection. Its goal was to make clear that the EU data protection regime and the GDPR would be as binding the day *after* Brexit as it was the day *before*. It also took extensive steps to create an international transfer regime regarding its own data exports that would integrate with the EU's approach. What is most striking about these extensive legal efforts is that they were not taken to further the development of a uniquely British approach to data protection. To return to Watson's observation about transplants seeking to avoid "the awful labor of thought," the UK legal system during Brexit did exhibit considerable thought and engage in arduous lawmaking concerning data protection law. Almost all of these efforts were made, however, to remain in close alignment with EU data protection law. It will be useful at this juncture to survey the full extent of this labor on the part of the UK legal system. A rich description of these steps will further this Article's subsequent analysis of the applicability of its different models of preference change.

At the time of Brexit, the UK took considerable initiative and exhibited great ingenuity in order to keep its data protection law in synch with EU law. This alignment was not present in 1984, at the time of the initial enactment of UK data protection law, but something had happened in the meantime, a transformation which this Part will seek to explain. As a technical matter, the UK government took two steps to meet its goal of unobstructed data flows. As a first step, it dutifully enacted a new national data protection statute, the Data Protection Act of 2018, to implement the GDPR.[82] The timeline of the UK's long goodbye to the EU had implications for its data protection regime: the Brexit referendum occurred in June 2016; the initial date for withdrawal was March 2019; and the actual withdrawal took place on January 31, 2020. Due to this timetable, the GDPR became directly binding in May 2018 in Britain as it did throughout the EU. In an admirable display of zeal, the UK became one of the first countries to pass the required implementing legislation. Its Data Protection Act of 2018 took effect on May 23, 2018, that is, two days before GDPR Day.

After passing its implementing legislation, the UK took a second step to protect unobstructed data flows from the EU. It enacted a "UK GDPR," which took effect at the start of 2021, that is, at the end of the Brexit transition period. The UK GDPR amended the British Data Protection Act of 2018. Here, it becomes necessary to understand certain aspects of the internal mechanisms

82 Data Protection Act 2018, c.12 (Eng.).

Electronic copy available at: https://ssrn.com/abstract=3895999

of UK law post-Brexit. To smooth the legal consequences of the departure from the EU, the UK enacted the European Union (Withdrawal) Act (EU(W)A).[83] This domestic UK statute is not to be confused with the similarly named agreement between the EU and the UK that set the terms for Brexit pursuant to Article 50(2) of the Treaty on the European Union. As a matter of domestic UK law, the EU(W)A repeals the European Communities Act of 1972 and thereby extinguishes the ability of EU institutions to legislate for the UK after Brexit. But this British law also provides for legal continuity by creating a new category of domestic UK law, namely, "retained EU law."[84] The rough analogy that will occur to Americans is the idea of the "reception statute." This term applies to a statutory law by which a former British colony adopts or receives the English common law. In the U.S., after the American Revolution, states adopted English common law through reception statutes as well as by judicial recognition and state constitutional provisions.

The concept of "retained EU law" transforms certain categories of existing EU law into UK law. Among its multiple approaches to deciding which EU law will be adopted into UK law, the EU(W)A in its Section 3 identifies as retained law all enacted EU legislation with a direct effect in the UK. In other words, the EU(W)A took a snapshot of all EU law that *directly applied* in the UK on the day of Brexit and made it part of the UK's legal framework. As an EU regulation, as opposed to a mere directive, the GDPR is clearly such "direct EU legislation." For the purposes of data protection, therefore, the impact of the EU(W)A is clear. The GDPR falls squarely within the category of retained EU law. Like all EU regulations, it was directly applicable in the UK and, as a regulation that entered into force in May 2018, it was in effect before Brexit Day.

Under the EU(W)A, the GDPR would continue to have effect in the UK upon Brexit. Nonetheless, a simple word-for-word retention of it as blackletter UK law would raise difficulties. Some GDPR provisions if enacted directly into UK law would no longer make sense in the post-Brexit context. For example, the GDPR contains provisions regarding the duties and responsibilities for EU data protection institutions, such as the European Data Protection Board. This language would not belong in a statute enacted by a non-EU nation.[85]

---

83 European Union (Withdrawal) Act 2018, c.16 (Eng.).

84 Info. Comm'r's Office, An Overview of the Data Protection Act 2018, at 7 (2d ed. 2019).

85 The Data Protection Act of 2018, as originally enacted, was based on an assumption of the UK's continuing membership in the EU. As an illustration of an incoherent detail post-Brexit, the Data Protection Act of 2018 detailed the duties of the UK as an EU Member State.

Electronic copy available at: https://ssrn.com/abstract=3895999

Fortunately, the EU(W)A authorized the UK government to amend retained law through so-called "statutory instruments" to ensure their effective operation. The government has made use of this power through the "Exiting the European Union Data Protection Electronic Communication Regulations of 2019" (EU Exit Regulations). It is this document that creates a "UK GDPR" and alters the Data Protection Act of 2018.[86] Technically, this law falls in the British legal category of a "statutory instrument." A statutory instrument is a form of legislation that allows Parliament to enact a law that can be brought into force at a later date without Parliament having to act again.

The result of the amended Data Protection Act and the UK GDPR is to preserve EU data protection law as part of the UK's domestic law. In particular, the UK has committed itself to an international transfer regime that is compatible with the one in the EU. In their Revised Political Declaration of October 19, 2019, a nonbinding document, the EU and UK agreed to ensure "a high level of personal data protection to facilitate" data flows and exchanges.[87] In the Revised Political Declaration, the EU also committed to starting its adequacy assessment of the UK "as soon as possible after the United Kingdom's withdrawal."[88]

Beyond the Revised Political Declaration, the UK took action to create an international transfer regime that would work smoothly with the EU's approach. The key documents in this regard are the UK GDPR and the amended UK Data Protection Act. To enable an uninterrupted flow of data with the EU, the UK GDPR's redline of the original GDPR keeps the UK's data protection framework closely oriented with that of the EU. For example, it permits data transfers from the UK only to countries with "adequate" data protection. The UK GDPR then recognizes all EU member states as "adequate" and adopts the existing European Commission list of adequate countries outside the EU. It also recognizes the existing mechanisms for achieving adequacy outside a formal European Commission determination; these are the Binding Corporate Rules and the Standard Contractual Clauses. Finally, the UK GDPR permits the Secretary of State to have parallel authority to the European Commission regarding future UK findings of adequacy.

---

86 Helpfully, the UK government has also issued redlined versions of both the GDPR and Data Protection Act of 2018; these so-called "Keeler Schedules" identify the changes in these laws.

87 European Comm'n, Political Declaration Setting Out the Framework for the Future Relationship Between the European Union and the United Kingdom 8 (2019).

88 *Id.*

Electronic copy available at: https://ssrn.com/abstract=3895999

B. The Disconnect with "Take Back Control" and the Adoption of the GDPR

There is a marked disconnect between the UK's stated reasons for leaving the EU and its policy approach to data protection. Voices for remaining in the EU during the referendum stressed the benefits of membership, both for economic growth and for Britain's global status. Those who advocated leaving the EU summed their views with the rallying cry of "Take Back Control." These individuals argued that red tape from the EU and onerous decisions from the CJEU had robbed the UK of its sovereignty. As Boris Johnson summed up this overarching concern, it was about the ability of the British people "to pass laws independently and in the interests of the people of this country . . ."[89] Beyond this goal of legislative independence, other major points of concern were immigration policy, UK funding of the EU, and fishing rights in the North Atlantic.[90] The attention to the fishing industry is particularly puzzling considering the existence of far more important industries, such as "the UK's financial services industry, which is worth more than 300 times the fishing trade."[91] According to one estimate, the UK has lost thousands of jobs in the financial services industry due to Brexit, the biggest winners for these positions being Dublin, Luxembourg, and Frankfurt.[92] In addition, over $1.6 trillion of assets have been transferred by these firms from the UK to the EU.[93] But the small UK fishing industry relates to an atavistic, near-mystical idea of the UK as an island-nation that should be free to chart its own path in a messy 21st -century world of international trade and global interconnections.

---

89 Letter of Resignation from Boris Johnson, Sec'y of State for Foreign Affairs, to Theresa May, Prime Minister of Britain (July 9, 2018), https://www.reuters.com/article/us-britain-eu-johnson-resignation-letter/boris-johnsons-resignation-letter-to-british-pm-theresa-may-idUSKBN1JZ2FJ.

90 For an analysis of how fishing rights came to be a key factor in "symbolic sovereignty" despite the small size of the British fishing industry, see Matt Seaton, *What's Brexit to Do with the Price of Fish?*, N.Y. Rev. Books (Dec. 24, 2020), https://www.nybooks.com/daily/2020/12/24/whats-brexit-to-do-with-the-price-of-fish/.

91 *Id.* Regarding the problems in the final Brexit agreement for UK financial services, see Peter Walker, *Boris Johnson admits Brexit deal falls short for financial services*, Guardian (Dec. 27, 2020), https://www.theguardian.com/politics/2020/dec/27/boris-johnson-admits-brexit-deal-falls-short-for-financial-services.

92 Viren Vaghela, *Brexit Prompts 7,500 City Jobs, $1.6 Trillion to Leave U.K.*, Bloomberg Wealth (Sept. 30, 2020), https://www.bloomberg.com/news/articles/2020-09-30/brexit-prompts-7-500-finance-jobs-1-6-trillion-to-leave-u-k.

93 *Id.*

Electronic copy available at: https://ssrn.com/abstract=3895999

At any rate, such was the sense of urgency for Brexit among its proponents that some favored following at all costs the two-year deadline triggered in March 2017 even if it meant suffering the costs of a "hard Brexit." In this view, Britain could not "tolerate being subject to EU laws (and financial demands) for a moment longer."[94] The current global pandemic did not weaken this resolve. The complex trade negotiations between the EU and the UK were made more difficult by the world outbreak of COVID-19, which, for a period, kept the two sides from negotiating in person.[95] Nonetheless, as the *New York Times* noted regarding the December 31, 2020 deadline, "the British government is adamant about sticking to that forbidding timetable, even at the risk of heaping more economic damage on nations reeling from the impact of lockdowns."[96]

With the insistence by the UK on a rapid Brexit, one might also expect efforts in the UK to enact a next-generation British data protection statute to terminate the reign of EU data protection. Here would be a chance to "take back control." In the political debate around Brexit, data protection also had potential to provide additional ammunition regarding supposedly burdensome red-tape from Brussels that harmed the British people. At times, the Conservative party attempted to raise this issue: Boris Johnson occasionally mentioned data protection as an area in which the UK would seek to "develop separate and independent policies."[97] Instead, Britain chose to follow EU data protection before, during, and after Brexit.[98] Its unexpressed motto might be summed up as, "Keep Calm and Follow the GDPR."

A clear contrast can be drawn with the UK's approach to immigration, and its actions to end "free movement," which its EU membership had required.

---

94 David M. Herszenhorn et al., *Brexit frustration as May offers EU leaders nothing new*, Politico (Apr. 19, 2019 1:34 AM), https://www.politico.eu/article/brexit-shrug-from-eu-european-council-leaders-as-theresa-may-offers-nothing-new.

95 Raf Casert & Jill Lawless, *Brexit Trade Negotiations Suspended Because of COVID-19 Case*, AP News (Nov. 19, 2020), https://apnews.com/article/international-news-brexit-michel-barnier-david-frost-f13d86639da482638a4226715055d742.

96 Stephen Castle & Mark Landler, *Britain is Sticking to Brexit Plans Despite Virus Upheaval*, N.Y. Times (Apr. 24, 2020), https://www.nytimes.com/2020/04/24/world/europe/virus-U.K.-brexit.html.

97 Danny Palmer, *On data protection, the UK says it will go it alone. It probably won't*, ZDNet (Feb. 14, 2020), https://www.zdnet.com/article/on-data-protection-the-uk-says-it-will-go-it-alone-it-probably-wont/.

98 David Smith, *Data Protection and Brexit – Clearing Up Some Misunderstandings*, Allen & Overy Digital Hub (Jan. 23, 2020), https://aodigitalhub.com/2020/01/23/data-protection-and-brexit-clearing-up-some-misunderstandings/.

Electronic copy available at: https://ssrn.com/abstract=3895999

As a policy statement from the UK Government explains, the UK will enact legislation to "take back control of our borders" through a new "point-based system."[99] The Parliament is now in the process of approving this extensive overhaul of immigration rules. The legislation introduces "a firm and fair points-based system that will attract . . . high-skilled workers."[100] The new system assigns points to characteristics of an applicant, such as the offer of a job by an approved sponsor, a job at the appropriate skill level, the ability to speak English at the required level, and whether or not the employment is in a "shortage occupation."[101]

This drastically new approach to immigration differs in scope and conception from the UK's effort to stay in alignment with EU data protection. Its goal for the latter was to replace the GDPR with the GDPR. The acceptance of the GDPR was a rare fixed point in the midst of the otherwise chaotic and improvised UK process of withdrawal from the EU. After all, even the previously controversial idea of permitting a customs border between Northern Ireland and the mainland of the UK was ultimately accepted by Johnson's government as part of its negotiations with the EU.[102] In contrast, there was agreement on the UK-side throughout the Brexit process about the need to retain EU data protection law. This policy decision remained unchanged from Theresa May's stint as Prime Minister to Boris Johnson's.

The UK accepted the GDPR as a necessary price for participation in the digital economy. The Queen's Speech in 2017 touched on this theme. This traditional address, which sets out the government's agenda for the coming year, explained that the adoption of EU data protection rules pre-Brexit would "put the UK in the best position to maintain our ability to share data with other EU member states and internationally after we leave the EU."[103] As a further matter, and in a detailed briefing paper, the House of Lords explained the necessity of continued life under the GDPR in the UK:

---

99 HM Gov't, The UK's Points-Based Immigration System: Policy Statement 3 (2020), https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/866744/CCS0120013106-001_The_UKs_Points-Based_Immigration_System_WEB_ACCESSIBLE.pdf.

100 *Id.*

101 *Id.* at 6.

102 The British voting public then affirmed this path by providing a strong level of support for Johnson and the Tories in the general election in December 2019. *See UK general election 2019: Who won and what happens now?*, BBC (Dec. 13, 2019), https://www.bbc.com/news/world-europe-50746464.

103 Prime Minister's Office, The Queen's Speech and Associated Background Briefing (2017).

Electronic copy available at: https://ssrn.com/abstract=3895999

> When the UK leaves the EU, it will cease to be bound by the EU's data protection laws. But there is no prospect of a clean break: the legal controls placed by the EU on transfers of personal data outside its territory will apply when data is transferred from the EU to the UK.[104]

This language soberly acknowledges the intertwined nature of the EU and UK economies, and the importance of the flow of personal data from the EU to the UK.

This perspective on EU data protection as a necessary price for participation in the digital economy is deep-seated in the UK. As we have seen, the UK enacted its first data privacy law, the British Data Protection Act of 1984, "for economic rather than for civil libertarian reasons."[105] At that time, over a decade before the EU Data Protection Directive of 1995, a handful of data protection authorities in Europe already had the power to restrict data exports to countries without sufficient privacy safeguards.[106] By the time of Brexit, the UK had even greater grounds to fear a weakening of elements of the essential parts of its economy that relied on digital data. Following enactment of the first British data protection law in 1984, the UK's economy became even more linked to the EU's. The UK now has forty-three percent of its exports with EU member states; the EU has only eight percent of its exports with the UK.[107]

Here, we see a certain paradoxical element at the core of Brexit. It represented a desire for change, but those negotiating Brexit also wished to minimize disruption. Moreover, data privacy was not directly implicated by the Leave vote, and was therefore a prime area where matters might be left unaltered. As noted in the preceding section, the Leave movement was primarily driven by immigration policy, UK funding of the EU, fishery issues, and a wish for legislative independence. There was also no shortage of inchoate emotion behind the plebiscite. As Geoffrey Wheatcroft explains, "the vote against 'Europe' was an expression of the general and perfectly understandable resentment of so many people in post-industrial England who felt ignored and disdained by their leaders."[108] Craig Oliver, a media advisor to Prime

---

104 Brexit: The EU Data Protection Package, *supra* note 81, at 7.

105 Bennett, *supra* note 57, at 91.

106 Schwartz, *supra* note 62, at 474-77.

107 Matthias Matthijs, *Europe After Brexit*, Foreign Affairs 85 (Jan.-Feb. 2017), https://www.foreignaffairs.com/articles/europe/2016-12-12/europe-after-brexit.

108 Geoffrey Wheatcroft, *The Opportunist Triumphant*, N.Y. Rev. Books, Feb. 13, 2020, at 32, 34. In a different account, the declining industrial north "voted as though it were seeking revenge on an elite it felt had forgotten it." Swati Dhingra, *Salvaging Brexit*, Foreign Affairs 90, 96 (Nov.-Dec. 2016).

Electronic copy available at: https://ssrn.com/abstract=3895999

Minister David Cameron, came to the same conclusion regarding the Leave voters in his postmortem on the plebiscite:

> I suspect that for many of them the referendum was more than a straightforward question of whether or not it made sense to remain in the European Union. Instead it was a cipher that, encouraged by a cynical Leave campaign, allowed them to put whatever was worrying or angering them on the ballot paper: immigration, feeling let down, ignored, betrayed, a life that didn't turn out as it should have done . . .[109]

Data protection law was not an issue that mattered in this debate, and, hence, the policy response for the UK government was to nail down compliance with EU requirements in this area, and to turn to other matters.

There is also a certain internal logic present here. Much of Brexit was driven by a fear of immigrants from the EU. The Leave campaigners made this argument about not just the number of foreigners coming to the UK, but also about the supposedly negative impact of immigrants on the British economy and public services. Post-Brexit, the UK has even established detention centers for visitors from the EU who are suspected of entering Britain to work. The *Guardian* has reported on cases of Bulgarian, Czech, French, German, and Italian citizens being held at UK airports overnight before being transferred to these centers.[110] In enacting the GDPR into UK law, the UK demonstrated that it wanted to receive personal information from EU member states — but not to be obliged to live with the EU residents to whom the data referred.

III. Preference Formation in the UK's Brexit and EU Data Protection Law

How then did the GDPR affect existing preferences in the UK? We now return to the puzzle of law and preferences before concluding this Part with thoughts regarding the future relationship of the UK and EU data protection regimes. The next section explores how its five models provide a *Murder on the Orient Express* solution; each of these perspectives offers a different contribution to understanding why the UK stuck with EU data protection law during Brexit.

---

109 Craig Oliver, Unleashing Demons: The Inside Story of Brexit 403 (2017).

110 Giles Tremlett & Lisa O'Carroll, *Hostile UK border regime traumatises visitors from EU*, Guardian (May 14, 2021), at https://www.theguardian.com/politics/2021/may/14/hostile-uk-border-regime-traumatises-visitors-from-eu; Giles Tremlett & Lisa O'Carroll, *EU citizens arriving in UK being locked up and expelled*, Guardian (May 13, 2021), at https://www.theguardian.com/politics/2021/may/13/eu-citizens-arriving-in-uk-being-locked-up-and-expelled.

Electronic copy available at: https://ssrn.com/abstract=3895999

A. Law and Preferences

An initial question is whether the UK's period of EU membership caused it to modify its preferences regarding data protection law. Turning back to our first model, Cooter's idea of Pareto self-improvement, it requires an assessment of whether the law altered internal preferences. The evidence here is inconclusive as to the public at large. Polling data shows confusion and ambivalence among the UK public about the GDPR. For example, a YouGov poll showed that 72% of British adults had not heard of GDPR in May 2018, the month of its adoption.[111] A year after the GDPR took effect, a TrustArc survey showed that only a small minority of Britons said that they had exercised rights under it. As one account of this poll explained, "[c]onsumers are confused and relatively few of them are taking advantage of personal data protections."[112]

Nonetheless, the presence of the GDPR did make a difference in the UK's policy-making environment regarding data protection during Brexit. To some extent then, there was "law-driven preference change," in Professor Cooter's phrase. In thinking about the Cooter model of preference change, however, one does not see individual self-improvement towards a Pareto optimal result. But the UK legal system did change its preferences for privacy regulation through a kind of Pareto self-improvement driven by market factors. Having adopted EU data protection law, the UK faced the question under Brexit as to whether it would "untransfer," or reject it. Or to build on Watson's concept of the "legal transplant," the question was whether to "untransplant" EU law. Here, this Article's modification of the Cooter approach, applying it beyond individuals to a legal system, demonstrates the general merit of the idea of Pareto self-improvement. The choice to keep EU data protection reflected a high-level internalization of the GDPR by the UK legal system. As will be developed below, the preferences that EU law helped generate in the UK were for stability of an EU-style regime of data protection law and for continuing access to the rich market in personal data of the EU.

The UK's adoption of EU data protection law dates back to 1984 and its enactment of the first British law in this area. Despite the costs of compliance with the GDPR, a clean break with it was entirely unappealing at the time

---

111 Ben Glanville, *72% of Brits haven't heard about GPDR*, YouGov (Mar. 1, 2018), https://yougov.co.uk/topics/politics/articles-reports/2018/03/01/72-brits-havent-heard-about-gdpr.

112 Greg Sterling, *Only 36% of UK consumers have greater trust in companies after GDPR, survey finds*, Marketing Land (May 23, 2019), https://marketingland.com/only-36-of-uk-consumers-have-greater-trust-in-companies-after-gdpr-survey-finds-261502.

Electronic copy available at: https://ssrn.com/abstract=3895999

of Brexit. Such a step would have required the reformulation of an entire field of law, the retraining of privacy professionals, and a steep hill to climb in convincing the EU of the new system's "adequacy" for international data transfers. One can also doubt whether legal capacity in the UK existed for developing such a new approach to data privacy in the midst of all the other demands that Brexit placed and continues to place on its legal order. The regulatory transaction costs for a new start for its data privacy law would have been enormous.

Moreover, the business community in the UK had made clear its preference for continuing with the existing data protection legal order. For example, the Confederation of British Industry, the country's "most influential business lobby," flatly stated, "Once we leave the EU, businesses want to retain similar standards so that firms can continue to digitally trade and innovate."[113] The UK Department for Digital, Culture, Media and Sort adopted a similar perspective. In its ministerial analysis of the UK Data Protection Act, it stated that maintaining the status quo of European data protection law would "minimise burdens to businesses while also eliminating any transition costs."[114] A modified model one therefore proves helpful in explaining the retention of EU data protection law. From the viewpoint of the UK legal system, it would be optimal to maintain the GDPR and to find ways to embed it as deeply as possible in domestic British law so that this law would survive Brexit intact.

The second model of preference change looks to alignment. While the UK legal system was not in synch with the EU in 1984 regarding data privacy, matters had changed by the time of Brexit. By then, the UK had taken on all the attributes of a standard data protection nation, including a national data protection commission. Its lawyers were versed in this system, and, as noted above, the costs of retraining would be great. By the time of Brexit, moreover, the alignment was not only in one direction. EU data protection law itself had come to reflect decades of input from the UK. The UK had participated in EU privacy institutions, such as the Article 29 Working Party, and played an important role in EU privacy policymaking. As a House of Lords report noted in 2017, the "UK has a track record of influencing EU rules on data protection and retention."[115] On this same note, testimony at this time

---

113 *U.K. Privacy Chief Urges EU Privacy Link After Brexit*, Bloomberg L. Priv. & Data Sec. L. News (Mar. 7, 2017), https://news.bloomberglaw.com/privacy-and-data-security/uk-privacy-chief-urges-eu-privacy-link-after-brexit?context=search&index=0.

114 Dept. for Culture, Media and Sport, Impact Assessment: Data Protection Bill 2017/18 32 (2017).

115 Brexit: The EU Data Protection Package, *supra* note 81, at 14.

Electronic copy available at: https://ssrn.com/abstract=3895999

before the House of Lords observed that the UK had provided a "pragmatic, moderating voice" in the development of EU data protection law.[116] Moreover, the UK was active in the Council of the European Union's Working Party on Information Exchange and Data Protection (DAPIX), which concentrates on implementation of legislation and development of policy relating to information exchange in law enforcement among EU member states.

There are many examples of this influence of the UK on the development of EU data protection law. During the debate around the nascent GDPR, the UK and Ireland successfully introduced a limited judicial exemption from the GDPR's requirements into the emerging text.[117] The UK also took an important role in bringing a risk-based approach to data protection into the GDPR. In sum, the contribution of the second model to this Article's examination of Brexit is to highlight that the UK had over decades aligned its privacy practices with those of the EU and exercised influence in shaping EU data protection to follow its views in at least some areas. The accord created through this mutual process of lawmaking weighed in favor of remaining with the existing EU system by the time of Brexit.

As for "acculturation or persuasion," the third model, it supplies a further perspective on the retention of EU data protection law in the shadow of Brexit. Acculturation into EU data protection had occurred within the EU legal system. As already noted, the UK had an entrenched EU-style system, including a data protection commission, the Information Commissioner's Office (ICO). The powers of this authority in the UK extended further than in some EU member states to include the ability to obtain search warrants and "to commence prosecutions in the criminal courts if a data controller or third party commits any one of a number of criminal offences created by the Act."[118] The exercise of these powers reached an apex of sorts with the ICO's seven-hour raid on the London Offices of Cambridge Analytica in 2018. Photographs of the action showed members of the ICO in FBI-style blue nylon jackets labeled "ICO Enforcement."[119]

---

116 *Id.* at 26.

117 *See* GDPR, *supra* note 1, at Recital 20(2) ("The competence of the supervisory authorities should not cover the processing of personal data when courts are acting in their judicial capacity, in order to safeguard the independence of the judiciary in the performance of its judicial tasks, including decision-making.").

118 Jay, *supra* note 63, at 707.

119 Hannah Summers & Nicola Slawson, *Investigators Complete Seven-hour Cambridge Analytica HQ Search*, Guardian (Mar. 24, 2018), https://www.theguardian.com/news/2018/mar/23/judge-grants-search-warrant-for-cambridge-analyticas-offices.

Electronic copy available at: https://ssrn.com/abstract=3895999

The greatest impact of "acculturation or persuasion" on UK data protection may have come by an indirect route. In these models, there is either an identification between different groups (acculturation) or active assessment of the merits of an idea (persuasion). The EU's idea of "privacy as a human right" is now favored by important officials at major corporations, including Apple, Microsoft, and Google. The leaders of these organizations have indicated, at varying levels of generality and specificity, their approval of the EU data protection regime.[120] Tim Cook of Apple is one of the most outspoken advocates of this perspective. On Data Privacy Day 2021, Cook renewed his call for a "universal, humanistic response" in privacy law to "create ripples of positive change across the industry as a whole."[121] The adoption of this worldview by these technology companies made it that much easier for the UK to stick with EU data protection. There has been a global competition around data privacy, and the success of the EU data protection reflects the appeal of high standards for the use of personal information. But instead of Bradford's view of the EU as hegemon, it has not singlehandedly imposed its regime on other nations, but reached important actors, such as major technology companies, through the force of appealing ideas — as well as a range of negotiating tactics.[122]

Thus far, this section has identified analytical contributions from the first three models. As for the fourth model of preference change, the Brussel's Effect, it provides an especially potent account of the retention of EU data protection law under Brexit. First, the EU is a large commercial market, and the UK's IT sector, like the UK export sector in general, is highly dependent on data transfers from the EU. Moreover, the EU has an impressive regulatory capacity for data protection, and one exercised by numerous institutions.[123] As for the ability of the private sector to create different data-driven services for different markets, this issue proves highly contextual depending on a company's services, internal resources, and other factors. Some companies benchmark different aspects of their use of personal data throughout the world using the GDPR as their critical measure.[124] Such global decisions may be driven by

---

120 *See* Schwartz, *supra* note 2, at 773.

121 C. Velazco, *Tim Cook takes aim at Facebook's practices during privacy conferences*, ENGADGET (Jan. 28, 2021), https://www.engadget.com/tim-cook-privacy-cpdp-2021-slams-facebook-184333398.html.

122 *See* LEE A. BYGRAVE, DATA PRIVACY LAW: AN INTERNATIONAL PERSPECTIVE (2014) ("[I]t is far from the case that the EU has been able to impose unilaterally its regulatory vision on the USA and other countries.").

123 Schwartz, *supra* note 2, at 807-08.

124 Microsoft provides a good example in this regard. Julie Brill, the company's Chief Privacy Officer and a former FTC Commissioner, has written: "[W]hen Europe's GDPR went into effect in May, Microsoft announced that we were extending

Electronic copy available at: https://ssrn.com/abstract=3895999

a combination of political, policy, or ideological reasons, however, and not merely because underlying services or products are non-divisible. Nonetheless, it is probable that many global companies have found it beneficial to adhere to EU privacy standards rather than customize for different markets.

As a related matter, and as noted above, the acceptance of EU data protection by companies like Apple, Google, and Microsoft made it easier for the UK to remain with the bandwagon rather than try a new direction upon Brexit. The result was both a "de facto" and "de jure" Brussel's Effect. It was "de facto" because companies emulated EU regulations worldwide. As a result, there would be some likelihood that these organizations would follow it post-Brexit within the UK. The impact of this behavior as well as other influences contributed to a "de jure" Brussels Effect in which the UK adopted EU law domestically.

The fifth factor, accessibility, also helps explain the UK's acceptance of the GDPR in the shadow of Brexit. Watson writes of the appeal of the English common law in the early days of the United States as being heightened by its ready availability. This quality was embodied by the popular edition of Blackstone that could fit into a saddlebag. European data protection law was, in fact, more than accessible; it was the existing law of the UK at the time of Brexit. At that point, the transaction costs of exit from that legal framework would have been high, and, during Brexit, the UK chose to pick its battles. There is no other data privacy model as easily accessible as EU data protection, and the conceptual costs of starting from zero were — and are — daunting. Put differently, some "exits" within the overall Brexit were more important than others, and regarding data protection law, there was no desire in the UK to undertake change, especially in light of the high costs of doing so.

In sum, there is no single winning model of preference change in explaining the retention of EU data protection by the UK. All five models help explain different elements of this outcome. To recap, beginning with the first model, the public at large did not engage in Pareto self-improvement. Applying a modified Cooter model, however, one can say that the UK legal system had many reasons to decide against a clean break and formulation of a new data privacy order. Regarding the second model, alignment, the UK had not only adopted EU data protection, but this area of EU law also reflected decades

---

Data Subject Rights — the rights at the heart of GDPR that give people in the EU greater control of their data — to all of our consumer customers around the world." Julie Brill, *Millions use Microsoft's GDPR privacy tools to control their data – including 2 million Americans*, Microsoft on the Issues (Sept. 17, 2018), https://blogs.microsoft.com/on-the-issues/2018/09/17/millions-use-microsofts-gdpr-privacy-tools-to-control-their-data-including-2-million-americans/.

Electronic copy available at: https://ssrn.com/abstract=3895999

of UK influence. Here was also a factor in favor of remaining with EU data protection law post-Brexit. The third model, acculturation or persuasion, also took place within the UK, not only through the training of UK lawyers into the Weltanschauung of EU data protection law, but also through the adoption of its ideas by leading corporations. To skip to the fifth model, accessibility, the UK was already fluently speaking the language of data protection — it was available and understood.

Ultimately, however, market forces played the most significant role in the decision of the UK government to accept the GDPR. The Brussels Effect, the fourth model, is especially illuminating in this regard. Indeed, Bennett's comment regarding the UK Data Protection Act of 1984 remains true for the GDPR in 2018: "Some in Britain feared that the country's computers would stand idle because of a new nontariff trade barrier imposed by her European partners."[125] A similar comment could be made almost four decades later about the UK's attitude towards the GDPR. In a sense, Britain took the various complex and arduous steps to adopt the GDPR because of a massive "Fear of Missing Out," or FOMO. This sentiment was directed towards the economy of the EU, and especially its digital data.

B. The Future: Storm Clouds Ahead?

The strategy of the UK in light of the "adequacy" requirement was to adopt EU data privacy law. Although this policy goes against the Brexit motto of "Take Back Control," there was a broad consensus in the UK that this approach to data protection was the best one. Looking ahead, however, there are possible storm clouds on the horizon and, here as well, one might turn to this Article's models regarding the path of possible preference change in light of challenges ahead. Of these models, two prove of particular assistance in thinking about the future of the UK-EU relationship around data privacy.

In particular, three issues threaten the status quo for data protection in the UK. First, the constitutional status of data protection law in the UK will be different post-Brexit, which will leave the British public without the current protections of the EU's fundamental rights. Second, the Conservative government is already speaking of its future ambition to diverge from EU data protection. Third, a new set of EU institutions will now be evaluating the UK's surveillance activities and may do so in a critical fashion.

As for the constitutional landscape, following Brexit, the UK is no longer bound to follow the decisions of the CJEU, the highest court for determining EU law, or to respect the Charter of Fundamental Rights of the European Union.

---

125 Bennett, *supra* note 57, at 91.

Electronic copy available at: https://ssrn.com/abstract=3895999

Andrew Murray concluded on the impact of this aspect of Brexit, "[W]hen the UK leaves the EU, and thereby the EU Charter, UK citizens (and EU citizens looking to enforce in the UK) will lose their right to data protection as found in Article 8 of the Charter."[126] The Charter contains an explicit right to data protection in its Article 8, and there is an extensive case-law from the CJEU interpreting its scope.[127] Today, the chief constitutional pillar of the EU data protection system is no longer applicable in the UK.

The case-law of the CJEU regarding data protection is extensive and expanding, and despite Brexit, the UK is not outside its reach. Consider in this regard the *Schrems II* (2020) decision. In it, the CJEU invalidated the Privacy Shield between the EU and U.S. This agreement had provided the main basis for international data transfers among these two jurisdictions.[128] *Schrems II* also developed complex constitutional requirements for standard contractual clauses, another important means for international data transfers. Data Protection Authorities and judges in member states apply and interpret EU data protection in accord with the CJEU's developing jurisprudence, but there is no mechanism post-Brexit in UK law for keeping its data protection law in accord with EU law. At the same time, however, like the U.S. after *Schrems II*, the UK is dependent on the judgment and good graces of the CJEU if it is to continue to receive personal data transfers from the EU. If the UK deviates too far from providing a system of data protection law for data transfers from the EU, one that is consistent with European constitutional requirements, it will no longer be "adequate," a standard which requires an "essentially equivalent" level of protection.

As a further constitutional complication, under separate legal authority, the UK is obligated to follow the ECtHR, which interprets the European Convention on Human Rights and its right to data protection. The Convention's right to data protection is similar to but not entirely the same as Article 8 of the Charter. Even after Brexit, the UK must meet its obligations under the Convention — although the Conservative party seeks its rejection as a long-term goal and its replacement with a British Bill of Rights.[129] At the same time, the British government has signed on to a revised privacy treaty of the

---

126 Andrew D. Murray, *Data Transfers Between the EU and UK post Brexit?*, 7 Int'l Data Privacy L. 149, 151 (2017).

127 European Union Agency for Fundamental Rights, Handbook, *supra* note 43, at 42-51.

128 Data Prot. Comm'r v. Facebook Ir. Ltd. & Maximillian Schrems, C-311/18 (E.C.J. 2020).

129 *See* Heather Stewart, *Ministers put British bill of rights plan on hold until after Brexit*, Guardian (Dec. 29, 2016), https://www.theguardian.com/law/2016/dec/29/ministers-put-british-bill-of-rights-plan-on-hold-until-after-brexit.

Electronic copy available at: https://ssrn.com/abstract=3895999

Council of Europe, namely the so-called Convention 108+.[130] In short, its ambitions regarding distancing the UK from European data protection are far from consistent.

Regarding the coveted adequacy determination from the EU, the absence of the Charter framework as part of British data protection should not prevent success on this front — at least not in the short term. As Murray observes, in comparing the UK to several other countries that currently have an adequacy decision from the EU, "[I]t is clear the UK will have a much more comprehensive and compliant data protection regime."[131] Longer term, however, there is a possibility that the UK will separate itself from the EU's constitutional regime to an extent that might endanger future adequacy reviews. Indeed, any adequacy assessment by the EU of the UK's level of data protection will predictably be subject to a sunset followed by a mandated, later reassessment. As Ronald Reagan used to comment regarding his negotiations with Mikhail Gorbachev of the Soviet Union, "Trust but verify."

When the European Commission finally released a draft adequacy finding on February 19, 2021, this document demonstrated the wisdom of the UK's strategy of sticking closely to the GDPR. Throughout the proposed Implementing Decision, the Commission noted the presence of myriad identical or mirroring provisions in UK law that track EU data protection.[132] The ultimate judgment of the Commission was that UK law met the "essential equivalent" test first identified by the CJEU in *Schrems I* and then confirmed in *Schrems II*, but it also warned of consequences if actual practices in the UK did not also fulfill this standard.[133] The Commission also limited its adequacy decision to four years, and promised that it would monitor "on an ongoing basis, relevant developments in the United Kingdom after the adoption of this Decision in order to assess whether it still ensures an essentially equivalent level of protection."[134]

---

130 Jennifer Baker, *What does the newly signed 'Convention 108+' mean for UK adequacy*, IAPP Privacy Advisor (Oct 20, 2018), https://iapp.org/news/a/what-does-the-newly-signed-convention-108-mean-for-u-k-adequacy/.

131 Murray, *supra* note 126, at 156.

132 Draft Commission Implementing Decision Pursuant Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate protection of personal data by the United Kingdom (Feb. 19, 2021), https://ec.europa.eu/info/sites/info/files/draft_decision_on_the_adequate_protection_of_personal_data_by_the_united_kingdom_-_general_data_protection_regulation_19_feb_2020.pdf.

133 *Id*. at 45.

134 *Id.* at 84.

Electronic copy available at: https://ssrn.com/abstract=3895999

The draft adequacy decision has now been the subject of a nonbinding opinion from the European Data Protection Board, which concluded that there was "strong alignment between the GDPR framework on certain core provisions."[135] It also noted that "challenges remain" and, in particular, pointed to the risk of "possible future divergence," which "might create risks for the maintenance of the level of protection provided to personal data transferred from the EU."[136] In a similar nonbinding resolution, the Civil Liberties Committee of the Parliament has called for further assessment by the Commission of troubling aspects of the UK data protection regime, and in particular, the UK's broad exemption for the areas of national security and immigration.[137] The Committee also raised concerns about onward transfers of EU citizens' data from the UK to the United States.[138] The Committee's recommendation now goes to the European Parliament for further input. The draft adequacy finding then will be subject to the comitology process of the EU. Comitology permits input on a proposed Commission action from a committee of representatives from all EU countries.

We return to our different models of preference change. The Brussels Effect, our third model, suggests that UK's deviation from the EU's constitutional structure may be limited. Upon Brexit, UK Prime Minister Boris Johnson all but crowed, "We have taken back control of laws and our destiny. We have taken back control of every jot and tittle of our regulation. In a way that is complete and unfettered."[139] This is nonsense; to restrict our comments only to data protection, the UK, like the U.S., must maintain "an essentially equivalent" standard for personal data from the EU. Due to the Brussels Effect, the UK is also unlikely to untether its domestic data protection law completely from the constitutional requirements of the EU.

The second threat to the status quo is the UK's newfound ability post-Brexit to amend its data protection statute in a unilateral fashion. As we have seen,

---

135 European Data Protection Board, Opinion 14/2021 regarding the European Commission Draft Implementing Decision pursuant to Regulation (EU) 2016/679 on the adequate protection of personal data in the United Kingdom 5 (April 13, 2021).

136 *Id.* at 5-6.

137 European Parliament, Data Protection, *MEPs urge the Commission to amend UK adequacy decisions* (May 11, 2021), https://www.europarl.europa.eu/news/en/press-room/20210510IPR03816/data-protection-meps-urge-the-commission-to-amend-uk-adequacy-decisions.

138 *Id.*

139 *Full text: Boris Johnson's Brexit deal speech*, The Spectator (Dec. 24, 2020), https://www.spectator.co.uk/article/full-text-boris-johnson-s-speech-on-the-brexit-trade-deal.

Electronic copy available at: https://ssrn.com/abstract=3895999

the main strategy during Brexit was to adopt the GDPR along with a push to obtain an adequacy finding. Longer term, the Tory party desires to create "separate and independent policies" in data protection, among other areas.[140] Overall, the UK government aspires post-Brexit to deregulate and shift away from the EU model. It points to Singapore as a model for the UK. There is much that might be said about this policy aspiration to become "Singapore of the West" or "Singapore-on-the-Thames."[141] In addition to the heavy involvement of Singapore's government in that nation's economy, one can note that this nation has adopted a data protection regulation that is largely sui generis and seems unlikely to qualify for an adequacy determination.[142]

At any rate, the Conservative government in the UK hopes in the future to gain economic advantages from diverging from EU data protection rules, and, in the words of Prime Minister Johnson, establishing its own "sovereign controls" in this field.[143] Or, as Nicky Morgan, then the UK's digital secretary, stated, the government's goal is to "fully and responsibly unlock the power of data, for people and organisations across the UK."[144] The extent of the UK's future divergence from EU data protection is impossible to predict, and the current political leaders of the UK are unlikely to have formulated detailed strategies in this regard. Some information concerning the aspirations in this area can be gleaned from a March 2021 speech by the UK Minister for Media and Data, John Whittingdale, calling for the development of new "international rules" as well as the formulation of "innovative alternative mechanisms for international data transfers."[145] He also promised, "There is a huge prize to be won here."

Here, too, the Brussels Effect raises doubts regarding this ambition of Tory leaders to develop a bold new approach and deviate in the UK's law from the GDPR. As noted above, the EU's ability to issue and withdraw an adequacy decision will offer a powerful check on further development of UK

---

140 Samuel Stolton, *UK to diverge from EU data protection rules, Johnson confirms*, Euractiv (Feb. 3, 2020), https://www.euractiv.com/section/digital/news/uk-to-diverge-from-eu-data-protection-rules-johnson-confirms.

141 Patrick Wintour, *Why the Singapore model won't work for the UK post-Brexit*, Guardian (Jan 2, 2019), https://www.theguardian.com/politics/2019/jan/02/why-the-singapore-model-wont-work-for-the-uk-post-brexit.

142 Graham Greenleaf, *The Asian Context of Singapore's Law*, *in* Data Protection Law in Singapore 459, 485 (Simon Chesterman ed., 2d ed. 2018).

143 Stolton, *supra* note 140.

144 *Id.*

145 John Whittingdale, *The UK's new, bold approach to international data transfers*, Privacy Laws & Business (March 2021), https://www.privacylaws.com/reports-gateway/articles/uk114/uk114datatransfers/.

Electronic copy available at: https://ssrn.com/abstract=3895999

data protection law. Already, the Draft Adequacy Decision of the European Commission contains a warning to the UK regarding its limited margin for maneuvering away from EU data protection law. The Commission first notes that individuals who seek redress for violations of their privacy interests can seek relief not only before UK courts but, after exhausting national remedies, before the ECtHR.[146] More broadly, in considering the general legal framework of the UK, the Commission stresses that the UK has ratified the European Convention of Human Rights, Convention 108, and Convention 108+. It emphasizes that "continued adherence to such instruments is . . . a particularly important element of the assessment on which this Decision is based."[147]

Beyond the Brussels Effect, the third model, acculturation or persuasion, is potentially important here. With leading tech companies voicing support for the GDPR, there is another important centripetal factor for the UK's remaining close to EU data protection. These entities have already harmonized their practices under the GDPR, and different laws in the UK will impose additional legal compliance costs on them.

Finally, a new set of EU institutions will be evaluating the UK's surveillance activities in a potentially more critical fashion than in the past. Here is the third threat to the current status quo. The UK has a tradition of vigorous international surveillance activities through the General Communications Headquarters (GCHQ), its equivalent to the National Security Agency in the U.S. The UK is also part of the Five Eyes, an Anglophone intelligence community. The other members of this alliance are Australia, Canada, New Zealand, and the U.S. As a member of the EU, the UK's intelligence collection was largely excluded from review by the European Commission, the European Data Protection Board, and the Data Protection Authorities of other member states. At that time, the UK was generally free from scrutiny from these institutions because "internal security" is a matter predominately reserved to the competency of the member states.[148] The UK was obligated, however, to exercise these matters in a constitutional manner, and it fell short of its obligations under the Council of Europe's Convention in many instances according to the case-

146 Draft Commission Implementing Decision, *supra* note 132, at 30.

147 *Id*. at 32.

148 In October 2020, however, the CJEU ruled that in their practices of mass data retention, EU member states were obligated to follow EU law, and were therefore subject to the privacy safeguards of EU law. Privacy International v. Secretary of State, (CJEU, Case C-623/17, Oct. 6, 2020); La Quadrature du Net and Others v. Premier Minister (CJEU, Joined Cases C-511/18 and C-512/18, Oct. 6, 2020). The two cases in question concerned surveillance practices in the UK, France, and Belgium.

Electronic copy available at: https://ssrn.com/abstract=3895999

law of the ECtHR.[149] Nonetheless, its surveillance activities were helpful for other members of the European security community, who benefitted from the UK's data gathering through formal and informal data-sharing arrangements.[150]

Post-Brexit, different EU institutions will evaluate the UK's data collection as part of its adequacy evaluation. From this perspective, the UK's departure from the EU represents a potential shift in power to forces in the EU *and* the UK that are privacy-oriented rather than security-oriented.[151] *Schrems II* sets out the kind of requirements that the EU is to use in evaluating whether a third party's data privacy regime is "essentially equivalent" to that in the EU, and, in particular, whether public authorities in the third-party nation carry out surveillance on transferred data in a fashion that meets the requirements of the principle of proportionality.[152] Here, the portrait by Henry Farrell and Abraham Newman of EU-U.S. data protection relations is helpful for understanding this likely area of tension between the EU and UK after Brexit. For Farrell and Newman, the transatlantic relationship has long been "an ongoing struggle between competing factions hoping to promote privacy or security."[153] They describe how "political factions within each jurisdiction that privilege security or civil liberties" collaborate across the Atlantic towards their policy goals and against groups in their own jurisdiction with different policy goals.[154]

Post-Brexit, entities in the UK that favor data protection will be able to point to the looming adequacy determination and its built-in sunset provision

---

149 *See, e.g.*, Big Brother Watch and Others v. the United Kingdom, ECtHR (2018) (the UK's mass surveillance program violated ECHR Articles 8 and 10 due to inadequate oversight and safeguards); Case of Liberty and Others v. the United Kingdom, ECtHR (2008) (defendant's interceptions of telephone and electronic communications pursuant to the Interception of Communications Act 1985 violated ECHR Article 8 due in part to its broad scope and discretion, and the failure to require a publicly available procedure as to the selection, sharing, storing and destruction of intercepted material).

150 Peter Schaar, a former Data Protection Commissioner of Germany, termed such techniques within the European security community as "competence hopping," or the practice of routing around internal requirements set by national law through international data-sharing arrangements. Paul Schwartz, *Systematic Government Access to Private-Sector Data in Germany*, *in* Bulk Collection 61, 88-89 (Fred Cate & James X. Dempsey eds., 2017).

151 Henry Farrell & Abraham Newman, Of Privacy and Power: The Transatlantic Struggle over Freedom and Security 159 (2019).

152 Data Prot. Comm'r v. Facebook Ir. Ltd. & Maximillian Schrems, C-311/18, at 173–176 (E.C.J. 2020).

153 Farrell & Newman, *supra* note 151, at xv.

154 *Id.*

Electronic copy available at: https://ssrn.com/abstract=3895999

as grounds for strong policies. Indeed, during the transitional period before departure, the British Data Protection Commissioner, the ICO, lost no time in announcing high preliminary fines under the GDPR in several matters then before it.[155] These seemingly strong regulatory moves would be easier to justify today than ever before; a powerful ICO helps furnish proof of the adequacy of UK data protection law.[156]

Yet, these arguments regarding the "adequacy" of data collection by the UK intelligence apparatus will only go so far. In particular, the UK GDPR contains a built-in weakness for an adequacy determination: it omits inclusion of the GDPR's Article 48.[157] In a nutshell, Article 48 limits recognition of foreign judicial opinions that require a transfer or disclosure of personal data to those "based on an international agreement, such as a mutual legal assistance treaty."[158] The situation for the UK is therefore problematic regarding data sharing with the U.S. pursuant to the U.S.'s Foreign Intelligence Surveillance Act (FISA). From the EU perspective, FISA does not represent an "international agreement," but is merely a statute from a third country. By choosing not to follow the requirements of Article 48, the UK opens itself to an argument that its process for transfers to foreign authorities is more lenient than that which is required by *Schrems II* and the GDPR.

---

155 *See, e.g.*, *Scottish company hit with maximum fine for making nearly 200 million nuisance calls*, Info. Comm'r's Office (Mar. 2, 2020), https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2020/03/scottish-company-hit-with-maximum-fine-for-nuisance-calls.

156 The ICO ultimately lowered its announced respective fines against British Airlines and Marriot International. The amount of the Marriott fine was lowered, for example, due to its cooperation in the investigation and to reflect the COVID-19 pandemic's impact on this company. Neil Hodge, *In second drastic reduction, ICO fines Marriott $23.8 million*, Compliance Week (Oct. 30, 2020), https://www.complianceweek.com/regulatory-enforcement/in-second-drastic-reduction-ico-fines-marriott-238m/29674.article.

157 For a discussion, see John Bowman & Jade Nester Gray, *UK's 181 words could start a cross-border GDPR scramble*, IAPP Privacy Perspectives (March 1, 2016), https://iapp.org/news/a/uks-181-words-could-start-a-cross-border-gdpr-scramble/. The UK was permitted to do so based on an opt-out negotiated by the UK and Ireland to the "Treaty on the Functioning of the European Union" in respect to "freedom, security, and justice." Consolidated version of the Treaty on the Functioning of the European Union, Protocol No. 21, O.J. C 202, 295 (June 7, 2016).

158 GDPR, *supra* note 1, § 48. For a discussion, see Christopher Kuner, *Article 48*, *in* The EU General Data Protection Regulation (GDPR) 825 (Christopher Kuner et al. eds., 2020).

Electronic copy available at: https://ssrn.com/abstract=3895999

At the same time, however, security-oriented governmental agencies in the EU and the UK will continue to be part of the policy debate. As part of Brexit, the EU and UK alike have expressed a shared desire for continued information-sharing regarding international and domestic security issues. To enable this data-sharing post-Brexit, the UK GDPR's Part 3 incorporates the requirements of EU Directive 2016/680 on law enforcement data. Moreover, the Withdrawal Agreement speaks of the parties' desire for "a broad, comprehensive and balanced security partnership." Towards this objective, the EU and the UK have agreed that "the future relationship should cover arrangements" that include "data exchange."[159] In particular, the Revised Agreement stated, "Recognising that effective and swift data sharing and analysis is vital for modern law enforcement, the Parties agree to put in place arrangements that reflect this, in order to respond to evolving threats, disrupt terrorism and serious criminality, facilitate investigations and prosecutions, and ensure the security of the public."[160]

Security-oriented agencies in the EU and UK have a shared stake in the adequacy determination from the Commission under the GDPR. Beyond these two stakeholders, the U.S. also has an interest in these transfers. The Draft Adequacy Decision of the Commission plays special attention to the Umbrella Agreement between the U.S. and EU, which permits onward transfers as part of law enforcement cooperation.[161] In finding this agreement to meet the adequacy standard, the Commission noted how it promises "equivalent protections to those provided" by a parallel agreement for law enforcement sharing of personal data already drawn up between the EU and U.S.[162]

---

159 European Comm'n, *supra* note 87, at 16.

160 *Id.* at 17. A further provision saw the parties agreeing to "exchange intelligence on a timely and voluntary basis as appropriate, in particular in the field of counter-terrorism, hybrid threats, and cyber-threats." *Id.* at 20.

161 Draft Implementing Decision, *supra* note 132, at 44-45.

162 *Id.* at 45. As a further demonstration of the stake of security-oriented agencies in continued data transfers from the EU to the UK, on the same day that it published its draft adequacy decision pursuant to the GDPR, the Commission also released an adequacy decision pursuant to the EU's Law Enforcement Directive (LED), which concerns the processing of personal data for "law enforcement purposes." Commission Implementing Decision pursuant to Directive (EU) 2016/680 of the European Parliament and of the Council on the adequate protection of personal data by the United Kingdom (Feb. 19, 2021), https://ec.europa.eu/info/sites/info/files/draft_decision_on_the_adequate_protection_of_personal_data_by_the_united_kingdom_law_enforcement_directive_19_feb_2020.pdf. It found that the UK ensured an adequate level of protection for personal data transferred from

Electronic copy available at: https://ssrn.com/abstract=3895999

The alignment theory, our second model, is particularly promising in thinking about the future situation regarding how institutions will handle privacy and security questions in the UK and EU. The future will be one of competition for power among institutions and entities within the EU and within the UK that favor privacy versus those that privilege data collection and data-sharing for law enforcement and security reasons. The work of Farrell and Newman suggests that the extent of future alignment between the UK and EU data protection will vary depending on policy area and the outcome of collaboration and transnational competition among different groups. Thus, security forces in the EU and UK may be in alignment in a way that pits them against data protection institutions in the EU and UK.

Conclusion

The UK's adoption of EU data protection law before, during, and after Brexit demonstrates the value of different theories of preference change. All five models of preference change in this Part offer useful perspectives on this behavior, with Bradford's Brussels Effect of special value. Regarding Cooter's model of Pareto self-improvement, this Article's first paradigm, there had been, at least to some extent, law-driven preference change for the UK legal system. Facing the choice of whether or not to reject EU data protection, the UK decided that it would be optimal to continue following it rather than bear the regulatory costs of a new start.

The second model of preference change, one that this Article introduces, looks to whether the EU and UK were in alignment by the time of Brexit. Indeed, by this period, the UK had taken on all the attributes of a standard data protection nation, including a national commissioner. A clear contrast can be drawn with the UK's initial adoption in 1984 of EU data protection law. By the time of Brexit, moreover, the alignment was not only in one direction. EU data protection itself reflected decades of input from the UK. This collaboration created another factor weighing on the UK remaining with the GDPR. EU data protection was not a foreign transplant, but one that itself had come to reflect values and input from the UK.

The third model, the Brussels Effect, is extremely helpful. The UK chose to follow the GDPR because of the power of the European market, and the dependence of the UK on it. As for acculturation or persuasion, the fourth model of preference change, it was felt in different ways during Brexit,

---

the EU to public authorities in the UK "responsible for prevention, investigation, detection, or prosecution of criminal offences." *Id*. at 49.

Electronic copy available at: https://ssrn.com/abstract=3895999

including indirectly. By the time of Brexit, leading technology companies were advocates for a human rights approach to data privacy. The final model concerns accessibility. EU data protection was highly accessible to the UK legal system; it was the existing law of the UK at the time of Brexit.

Looking to the future, there are possible storm clouds regarding the status quo for UK data protection. The three matters of concern are the constitutional status of data protection law in the UK; the possible ambition of the UK government, led by the Tories, to diverge from EU data protection in hopes of new efficiencies; and new and perhaps heightened scrutiny by EU institutions of the UK international surveillance apparatus. This Article's models of preference change suggest that there will be centripetal forces limiting the path of UK data protection away from EU law. Despite the claims of the UK government post-Brexit to have regained total independence, the imperative need for the UK of continuing access to personal data from the EU will limit the scope of legal change in the UK in its privacy law. A former Irish diplomat, Bobby McDonaugh, observed that "National control over trade is a contradiction in terms. Absolute control over trade stops at Dover and Heathrow. There is only one way to achieve such control. Don't export anything."[163] One can add: the UK cannot engage in data trade with the EU without having essentially equivalent data protection, which limits its control over its data privacy law.

163 Bobby McDonaugh, *Somebody needs to explain sovereignty to Johnson before it is too late*, Irish Times (Nov. 23, 2020), https://www.irishtimes.com/opinion/somebody-needs-to-explain-sovereignty-to-johnson-before-it-is-too-late-1.4416087.

Electronic copy available at: https://ssrn.com/abstract=3895999