OWNING OURSELVES: WHY THE AMERICAN NOTION OF PRIVACY DEMANDS A REGULATORY ANSWER TO THE GDPR AT THE FEDERAL LEVEL

CHRISTOPHER T. COLLUM*

ABSTRACT

The European Union's General Data Privacy Regulation—which took effect in 2018—is widely thought of as the world's leading data privacy law. Although some aspects of the law are quintessentially European, its core principles are concomitant with fundamental American legal conceptions of private property, privacy, and liberty more generally. This Note provides a jurisprudential argument for a general data privacy bill at the federal level in the United States. In doing so, this Note also briefly addresses key provisions of the European law, as well as American copycat laws at the state level, and public policy rationales for heightened statutory protections for data privacy.

INTRODUCTION

In late May of 2018, consumers in the United States and worldwide might have noticed a sudden inundation of messages in their email inboxes with titles like "We're Updating Our Privacy Policy" or "Improving Our Privacy Policies."[1] Most consumers likely ignored these emails, whether from their bank or from a website they hadn't logged in to for several years, allowing their Gmail account to filter them out and languish

* Editor-in-Chief, *Washington University Jurisprudence Review*, Vol. 13. J.D. Candidate, Washington University School of Law, Class of 2021.

1. Alfred Ng, *The GDPR Privacy Law Happened, and All I Got Were These Lousy Emails*, CNET (May 26, 2018, 5:00 AM), https://www.cnet.com/news/eu-gdpr-privacy-law-happened-and-all-i-got-were-these-lousy-emails/ [https://perma.cc/TRS4–5FKV].

indeterminately.[2] Any consumers who clicked on one of the emails were probably greeted with a polite, upbeat message full of business buzzwords and hyperlinks, which in turn led to pages of legalese on the company's website.[3] It seems unlikely that even a curious consumer who made it this far would read beyond the first sentence or so of a several-pages-long corporate document; most consumers probably moved on by the time the words "a Delaware corporation" inevitably appeared in the first line.[4] But a keen-eyed, albeit disinterested, consumer would probably have at least noticed a seemingly omnipresent acronym, particularly if they explored more than one or two of these form emails and the links that they contained: "GDPR."

The "GDPR," short for "General Data Privacy Regulation," is a European Union ("EU") regulation that took effect on May 25, 2018—explaining the timing of the email influx.[5] The framework created by the GDPR was hailed as "the world's toughest rules to protect people's online data."[6]

While the GDPR may appear quintessentially European, scholars note that the core of GDPR contains strands of American law.[7] Although EU law may be ahead of American law with respect to data privacy,[8] American law does contain protections for personal data, albeit in a more

---

2. A very unscientific Twitter poll conducted by Entrepreneur.com suggests that very few users actually read these data privacy update emails, as 86% of the 1,361 total respondents said they did not read any of the emails they received. Entrepreneur (@Entrepreneur), TWITTER (May 29, 2018, 11:57 AM), https://twitter.com/Entrepreneur/status/1001507746615881731 [https://perma.cc/XPG5-GCXM].

3. *See generally Glassdoor Privacy and Cookie Policy*, GLASSDOOR (last updated Sept. 3, 2020), https://www.glassdoor.com/about/privacy.htm?utm_source=campaign&utm_medium=email&utm_content=&utm_campaign=2018_GDPR [https://perma.cc/U32Z-FRH6].

4. *Id.*

5. Lydia Belanger, *Here's Why Your Inbox Is Filled With Privacy Policy Emails*, ENTREPRENEUR (May 29, 2018), https://www.entrepreneur.com/article/314170 [https://perma.cc/AAX9-NN62].

6. Adam Satariano, *G.D.P.R., a New Privacy Law, Makes Europe World's Leading Tech Watchdog*, N.Y. TIMES (May 24, 2018), https://www.nytimes.com/2018/05/24/technology/europe-gdpr-privacy.html [https://perma.cc/V7G8-YQVY].

7. Chris Jay Hoofnagle et al., *The European Union General Data Protection Regulation: What It Is and What It Means*, 28 INFO. & COMM. TECH. L. 65 (2019), https://www.tandfonline.com/doi/full/10.1080/13600834.2019.1573501 [https://perma.cc/C5VT-GF3W]. "[T]he GDPR is the most consequential regulatory development in information policy in a generation. The GDPR brings personal data into a complex and protective regulatory regime. That said, the ideas contained within the GDPR are not entirely European, nor new. The GDPR's protections can be found – albeit in weaker, less prescriptive forms – in U.S. privacy laws and in Federal Trade Commission settlements with companies." *Id*. at 66.

8. Satariano, *supra* note 6.

fragmented form than in the GDPR.[9] Despite this, no sweeping regulatory framework exists in the United States at the federal level. Two states, however, have passed legislation similar to the GDPR in the years after the EU law came into effect. California lawmakers passed the "California Consumer Privacy Act" ("CCPA") in 2018, which has drawn comparisons to the GDPR.[10] The CCPA was further augmented by the California Privacy Rights Act ("CPRA"), which was passed as a ballot initiative in the November 2020 election and even more closely aligns Californians' data privacy rights with EU citizens' under the GDPR.11 The following year, Virginia passed the Consumer Data Protection Act ("CDPA"), which is similar to the CCPA and also has drawn comparisons to the GDPR.12 Although states like Maine, Nevada, and Washington have passed smaller privacy bills in recent years,[13] none of those laws are as comprehensive as the California or Virginia laws.[14]

---

9. Neil M. Richards et al., *Understanding American Privacy, in* RESEARCH HANDBOOK ON PRIVACY AND DATA PROTECTION LAW: VALUES, NORMS AND GLOBAL POLITICS, (Gloria González Fuster, et al., eds.) (forthcoming), https://ssrn.com/abstract=3256918 [https://perma.cc/36YZ-LNTZ]. "Unlike its European counterparts . . . the United States does not have a federal omnibus privacy or data protection law. Instead, the federal government has taken a sectoral approach by enacting laws that regulate privacy and data security by focusing on a particular sector of the economy, or particular groups of people . . . ." *Id*. at 10.

10. Issie Lapowsky, *California Unanimously Passes Historic Privacy Bill*, WIRED (June 28, 2018, 5:57 PM), https://www.wired.com/story/california-unanimously-passes-historic-privacy-bill/ [https://perma.cc/9QZC-LZ5X]. "The new [California] legislation . . . . [is] similar to the General Data Privacy Regulation that went into effect in the European Union last month, but adds to it in crucial ways." *Id*. One trivial thing that the CCPA certainly has in common with the GDPR is that it also produced a barrage of legal notices flooding users' inboxes—this time in the weeks leading up to the CCPA effective date on January 1, 2020. *See* Katy Murphy, *Wild West: Firms Interpret California's Privacy Law as They See Fit*, POLITICO (Jan. 8, 2020, 6:27 PM), https://www.politico.com/states/california/story/2020/01/08/choose-your-own-adventure-firms-interpret-californias-privacy-law-as-they-see-fit–1242362 [https://perma.cc/RK6J-QAV8].

11. Michael Bahar et al., *California's New Privacy Law, the CPRA, Was Approved: Now What?*, LEXOLOGY (Nov.November 9, 2020), https://www.lexology.com/library/detail.aspx?g=5a7edce9–26af–487c–8877–7a815945954d. CPRA "builds on the existing framework of the CCPA, expands consumer privacy rights to more closely align with the EU's GDPR, imposes additional obligations on businesses, and establishes the nation's first agency dedicated to privacy regulation and enforcement . . . ." *Id.*

12. Sarah Rippy, *Virginia Passes the Consumer Data Protection Act*, INT'L ASS'N PRIVACY PROFESSIONALS (Mar. 3, 2021), https://iapp.org/news/a/virginia-passes-the-consumer-data-protection-act/.

13. Cynthia Brumfield, *12 New State Privacy and Security Laws Explained: Is Your Business Ready?*, CSO (Dec. 28, 2020 2:00 AM PST), https://www.csoonline.com/article/3429608/11-new-state-privacy-and-security-laws-explained-is-your-business-ready.html.

14. *See* Sarah Rippy, *US State Comprehensive Privacy Law Comparison,* INT'L ASS'N PRIVACY PROFESSIONALS (Mar. 22, 2021), https://iapp.org/resources/article/state-comparison-table/.

This Note argues that federal lawmakers in the United States should adopt a sweeping regulatory scheme like the GDPR. A GDPR-style regulation would be a welcome development in American privacy law for four reasons. First, such a law would advance fundamental American notions of property rights, rooted in natural law theory as understood by the Founders. Second, such a law would be consistent with the privacy law jurisprudence that the Supreme Court has developed in the last half-century. Third, in light of high-profile data breaches occurring with increasing frequency, a GDPR-like law is necessary from a public-policy standpoint, in order to protect consumers. Finally, in light of the CCPA—and the high likelihood that other state-level privacy laws will be enacted—a GDPR-style law at the federal level avoids the risk of a patchwork regulatory scheme negatively impacting the tech industry, along with other sectors of the American economy.

Part I of this Note outlines the history of the GDPR and discusses the key provisions enacted by the regulation. Part II outlines the philosophical underpinnings of the American understanding of private property rights—an understanding that has its roots in the writings of natural law theorists who influenced the founding fathers, with special attention given to John Locke. It is from these centuries-old ideas about private property that I develop an argument that corporate entities should not use personal information for profit without consumers' express permission—and certainly not without consumers' knowledge. Part III examines relevant case law in the privacy realm, which is an area of law that the Supreme Court has extensively developed in the last hundred years. Part IV examines both recent data breaches and business sector attitudes towards the GDPR, before synthesizing these two phenomena to develop a public policy argument for a GDPR-like scheme in the United States. Part V outlines what a proper GDPR-like scheme would look like in the United States, including explaining ways in which a US regulatory scheme would need to (or should) be different than the EU one, as well as ways the scheme should resemble and depart from the CCPA and other state laws mentioned above. Part V also addresses arguments against the adoption of a GDPR-like scheme in the US.

I. HISTORY AND CONTENT OF THE GDPR

A. Pre-GDPR EU Privacy Regulation Attempts

The history of the GDPR begins thirty-seven years before it became law, when the Council of Europe approved a treaty called the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data ("Convention"), made available for member-state

ratification on January 28, 1981.[15] The Convention described itself as "the first binding international instrument which protects the individual against abuses which may accompany the collection and processing of personal data and which seeks to regulate at the same time the transfrontier [sic] flow of personal data."[16] Although the Convention was ratified by enough member states to enter into force by 1985,[17] the Council of Europe continued to work towards a directive with the goal of creating uniformity for data regulation across its member states, replacing the regulatory patchwork still existent in the mid–1980s despite the Convention.[18]

These efforts bore fruit in the form of the European Union's 1995 Data Policy Directive ("Directive").[19] The first draft of what became the Directive was produced in July of 1990, and the European Parliament approved a slightly-altered version of this draft on March 11, 1992.[20] As opposed to previous EU actions concerning privacy regulation described above, (which were subject to voluntary enforcement by member states) the Directive was a much stronger regulation, binding member states to implement their own regulatory schemes that complied with the Directive's principles.[21] Just like the Convention that came before it, the Directive was rooted in seven fundamental principles of privacy protection:

> (1) Subjects whose data is being collected should be given notice of such collection.
> (2) Subjects whose personal data is being collected should be informed as to the party or parties collecting such data.
> (3) Once collected, personal data should be kept safe and secure from potential abuse, theft, or loss.
> (4) Personal data should not be disclosed or shared with third parties without consent from its subject(s).

---

15. Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, *opened for signature* Jan. 28, 1981, 1496 U.N.T.S. 65.

16. *Id.*

17. *Id.*

18. Robert R. Schriver, *You Cheated, You Lied: The Safe Harbor Agreement and its Enforcement by the Federal Trade Commission*, 70 FORDHAM L. REV. 2777, 2783 (2002), http://ir.lawnet.fordham.edu/flr/vol70/iss6/29 [https://perma.cc/JQP5-NCJN].

19. Council Directive 95/46/EC, O.J. (L 281) 31.

20. Schriver, *supra* note 18, at 2783–84, 2786.

21. Nate Lord, *What is the Data Protection Directive? The Predecessor to the GDPR*, DIGITAL GUARDIAN (Sept.September 12, 2018), https://digitalguardian.com/blog/what-data-protection-directive-predecessor-gdpr. [https://perma.cc/J53D-Q2FW].

> (5) Subjects should [be] granted access to their personal data and allowed to correct any inaccuracies.
> (6) Data collected should be used only for stated purpose(s) and for no other purposes.
> (7) Subjects should be able to hold personal data collectors accountable for adhering to all seven of these principles.[22]

All of these principles are seen not only in the Directive, but also would come to influence the GDPR some decades later.[23] This Note advocates these principles should influence an American answer to the GDPR.

The final version of the 1995 Directive was passed by the EU on October 24, 1995 and took effect three years later on October 25, 1998.[24] The seven principles outlined above became enshrined in the regulation.[25] Although these protections on the usage of personal data were obviously important, how the Directive defined what qualified as "personal data" was at least as impactful as the regulatory aspects of the Directive itself.[26] The Directive's definition of personal data, as discussed below, has had far-reaching consequences in other jurisdictions around the world since its promulgation.[27]

The Directive became law in the EU and naturally had the most direct effect on persons and entities operating there, but its effects extended beyond the EU in two primary ways. First, the Directive's broad definition of personal data meant that its protections applied not only to entities operating within the EU, but also to all foreign entities that processed personal data of persons within the EU.[28] Second, Article 25 of the Directive attempted to ensure enforcement of the Directive's provisions by closing a loophole in the Convention's regulatory scheme.[29] Prior to the

---

22. *EU Data Protection Directive (Directive 95/46/EC)*, TECHCRUNCH (last updated Jan. 2008), https://whatis.techtarget.com/definition/EU-Data-Protection-Directive-Directive–95–46-EC [https://perma.cc/CUV2-F86Mhttps://perma.cc/CUV2-F86M] (numbering added). These seven principles are often referred to as "notice," "purpose," "consent," "security," "disclosure," "access," and "accountability." *See generally* Lord, *supra* note 21.

23. *The Principles*, INFO. COMMISSIONER'S OFF. https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/ [https://perma.cc/A7W9-FT82] (last visited Jan. 25, 2020).

24. Schriver, *supra* note 18, at 2784.

25. Lord, *supra* note 21.

26. *Id.* Article 2a of the Directive defines personal data as "any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity." *Id.*

27. *See generally* Schriver, *supra* note 18, at 2786–87.

28. Lord, *supra* note 21.

29. Schriver, *supra* note 18, at 2785.

Directive, EU member states would commonly allow the electronic transmission of personal data to non-EU countries for "processing" as a way of avoiding more-stringent EU privacy laws.[30] The Directive closed this loophole by prohibiting the electronic transfer of personal data to any country that didn't possess an "adequate level" of privacy protection in its laws.[31]

The Directive was structured such that each individual EU member state had to create its own internal data privacy policies and regulation, in keeping with the tenets of the Directive.[32] This structure naturally led to slight transnational differences in privacy regulation under the Directive, according to how particular member states chose to implement the its principles in their substantive law.[33] The Directive was successful because it not only strengthened protections concerning data usage within the EU, but also encouraged other, non-European jurisdictions to pass their own data privacy regulations—or at least to negotiate agreements with the EU concerning transnational data usage.[34] For example, while the Directive did not encourage the United States to enact its own sweeping data privacy law, it did spur the United States to create the bilateral Safe Harbor Agreement, which was certified—after several rejected drafts—by the European Commission on July 26, 2000.[35] The Safe Harbor Agreement was supposed to certify to European regulators and consumers that US companies that processed EU consumers' private data were in compliance with the Directive.[36] Unfortunately, in practice, the Safe Harbor Agreement was not as successful as EU regulators had hoped, because the Safe Harbor agreement was voluntary, and many US companies chose not to participate.[37] Further, US officials continued to publicly express

30. *Id.*

31. *Id.* The main problem with Article 25, however, was that it did not specify what constitutes an "adequate level" of privacy protection, and some speculated that "the whole world" did not possess the necessary protection at the time the law took effect. *Id.* at 2785–86. Even a country like Switzerland, which had its own privacy laws which were fairly similar to the EU model at the time, was considered by EU regulators to be noncompliant with the Directive by default. *Id.* at note 82.

32. *EU Data Protection Directive*, THOMSON REUTERS PRACT. L., https://uk.practicallaw.thomsonreuters.com/6–501–7455?transitionType=Default&contextData=(sc.Default)&firstPage=true&bhcp=1 [https://http://perma.cc/F4RZ-UI1P] (last visited Jan. 12, 2020).

33. *Id.*

34. Schriver, *supra* note 18, at 2786–87.

35. *Id.* at 2789.

36. *Id.* at 2789–94.

37. *Id.* at 2792–93.

misgivings about the wisdom of the Safe Harbor Agreement while European member-state officials rarely carried out enforcement actions against US companies.[38]

Even setting aside concerns about US compliance with the Directive, as the internet changed rapidly in the years that followed institution, it became inevitable that the Directive would have to be updated, if not fundamentally altered, to meet modern data privacy needs.[39] With the progression of the 21st century, new risks inherent to consumers' ever-increasing internet use have arisen that EU regulators did not foresee in the 1990s.[40] One of these inherent risks—the ease with which consumers' personal data can be transmitted across international borders—was partially foreseen by EU regulators, as evidenced by their attempts to create the Safe Harbor Agreement with the US, but has become even more pressing in the years since.[41] Hoping to bring both EU data privacy law fully into the 21st century—and to create a single, EU-wide law that would be more extensive than the Directive—in January of 2012, the European Commission proposed a first draft of the law that would become the GDPR.[42]

B. History of the GDPR

In December of 2015, nearly four years after the EU set out to update the Directive and institute more stringent requirements for usage of its citizens' personal data, EU officials reached a tentative agreement about what this new law would contain.[43] The final version of the GDPR—completed a few months after the tentative agreement—was quite extensive, containing eleven chapters and ninety-one articles,[44] and was

---

38. *Id.*

39. *See* Mira Burri & Rahel Schär, *The Reform of the EU Data Protection Framework: Outlining Key Changes and Assessing Their Fitness for a Data-Driven Economy*, 6 J. INFO. POL'Y 479, 480 (2016).

40. *Id.*

41. *Id.*

42. *See generally* Lord, *supra* note 18.

43. Jeremy M. Mittman, *EU Officials (Finally) Agree on New Data Protection Regulation*, PROSKAUER PRIVACY L. BLOG (Dec. 17, 2015), https://privacylaw.proskauer.com/2015/12/articles/european-union/eu-officials-finally-agree-on-new-data-protection-regulation/ [https://perma.cc/98HA-BYC6]. It is worth noting that at this nascent stage in the regulation's development, specific details concerning the GDPR were not publicly available, but it was clear even at this point that the GDPR would contain such provisions as a "right to be forgotten" and very strong fines for non-compliance, that featured in the final version of the law. *Id.*

44. Juliana De Groot, *What Is the General Data Protection Regulation? Understanding & Complying with GDPR Requirements in 2019*, DIGITAL GUARDIAN (Sept. 30, 2020),

passed by the European Council on April 8, 2016.[45] Twenty-seven member states voted in favor of the GDPR, with only Austria voting against.[46] On April 14, 2016, the European Parliament passed the GDPR, cementing its status as EU law, and ending the years-long process to improve and replace the Directive.[47] Although the GDPR "entered into force" shortly thereafter, it was not directly applicable until some two years later, allowing member states the interim to "transpose the provisions of the directive into national law."[48] The GDPR finally became fully effective on May 25, 2018.[49]

The central idea of the GDPR is that individuals should have ownership and control of their private data, not the corporations, organizations, or web entities with which they interact.[50] This ethic of self-ownership of data is of vital importance in thinking about all EU privacy regulation, not just the GDPR, as the seven principles implicitly suggest the idea of self-

---

https://digitalguardian.com/blog/what-gdpr-general-data-protection-regulation-understanding-and-complying-gdpr-data-protection [https://perma.cc/YL8K-R2XM].

45. *Regulation of the European Parliament and of the Council on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC*, VOTEWATCH EUR., https://term8.votewatch.eu/en/term8-regulation-of-the-european-parliament-and-of-the-council-on-the-protection-of-natural-persons-with-r.html [https://perma.cc/44FF-XL2M] (last visited Jan. 13, 2020).

46. *Id.* Austria voted against adoption of the GDPR because, in Austria's view, the law's "level of data protection . . . falls short of that provided by [the Directive]." *Statement by Austria*, COUNCIL OF THE EUROPEAN UNION GENERAL SECRETARIAT (April 8, 2016), https://www.europarl.europa.eu/cmsdata/99614/Procedure_ecrite_GDPR_EN.docx [https://perma.cc/RLC6-UEAC]. Much of Austria's concern revolved around the ambiguous standard for data controllers' usage of personal data—including international transfer of data—under the "legitimate interest" avenue of the GDPR. *Id.* This "legitimate interest" standard is briefly discussed below and is only one way for a data controller to justify usage of personal information under the GDPR. *See* Ben Wolford, *What Are the GDPR Consent Requirements?*, GDPR.EU, https://gdpr.eu/gdpr-consent-requirements/ [https://perma.cc/ZLQ6–9GLR] (last visited Jan. 25, 2020).

47. *Data Protection Reform – Parliament Approves New Rules Fit for Digital Era*, EUROPEAN PARLIAMENT (Apr. 14, 2016, 12:11 PM), https://www.europarl.europa.eu/news/en/press-room/20160407IPR21776/data-protection-reform-parliament-approves-new-rules-fit-for-the-digital-era [https://perma.cc/6WRG–9UC7].

48. *Id.*

49. De Groot, *supra* note 44.

50. For example, Margrethe Vestager, a European Union official involved in implementation of the GDPR, has repeated in interviews that the concept that "we all own our own data" is fundamental to the philosophy underpinning the GDPR. Jennifer Baker, *Vestager on the Intersection of Data and Compliance*, INT'L ASS'N PRIVACY PROFESSIONALS (Oct. 30, 2018), https://iapp.org/news/a/vestager-on-the-intersection-of-data-and-competition/?mkt_tok=eyJpIjoiTkRoa09HRmhNelJoWVdaaSIsInQiOiIzSWFlN0JUQVhwRDVaaEtXRExRZ20zbzJqZXcrenNDUGVlV1pwQXhSZzlKdTg4Z1RxS1VybHduRnZhXC9NTWtXR1d5VnBCXC9KWnk4bjdRN05nWlhJaHBFMGpGd1ZTdWRwK2dRTGc1TlkwN0dsU1lmT1ZwVURQUWJkRkFFZHFSVENHIn0=. [https://perma.cc/8B8Y-RA4J].

ownership of data.[51] With this fundamental notion of self-ownership of data in mind, let us briefly address the core substantive aspects of the GDPR.

C. Core Aspects of the GDPR

Although a law as vast as the GDPR contains a host of provisions of potential interest, this Note focuses on nine core aspects of the GDPR. This will by no means constitute a comprehensive treatment of the GDPR, but rather will serve to introduce the reader to some of the regulation's more-impactful provisions. The paragraphs below will address each of the nine aspects individually.

The first aspect of the GDPR worth discussing is the regulation's extraterritorial applicability.[52] As mentioned above about the Directive and the attempted Safe Harbor Agreement with the United States, concerns regarding the potential applicability of EU privacy laws beyond the EU's physical borders have existed both for EU officials and other governments' officials for decades.[53] Although the original text of the GDPR made its provisions applicable only to personal data usage by organizations (hereinafter, "data controllers") "established" within the EU, subsequent decisions by the Court of Justice of the European Union ("CJEU") have broadly interpreted the applicability of the GDPR.[54] This expansive understanding of the law's applicability brought about by the CJEU's rulings has subsequently been explicitly incorporated into the text of the GDPR.[55] Currently, under Article 3 of the GDPR, the law applies to data controllers that process EU citizens' personal data even if the data controller is not established within the EU, so long as the data usage is either related to "the offering of goods and services to individuals in the

---

51. *See generally EU Data Protection Directive (Directive 95/46/EC)*, *supra* note 22.

52. Alexander Garrelfs, *GDPR Top Ten #3: Extraterritorial Applicability of the GDPR*, DELOITTE, https://www2.deloitte.com/ch/en/pages/risk/articles/gdpr-extraterritorial-applicability.html# [https://perma.cc/H8N3-N255] (last visited Jan. 14, 2020). With the GDPR, "the territorial scope has been broadened so that EU privacy rules now also can apply to data controllers outside the EU." *Id.*

53. *See generally* Schriver, *supra* note 18, at 2789–90.

54. Bertram Burtscher & Gernot Fitz, *The Extra-territorial Scope of the EU's GDPR*, FRESHFIELDS BRUCKHAUS DERINGER, https://www.freshfields.com/en-us/our-thinking/campaigns/digital/data/general-data-protection-regulation/ [https://perma.cc/3QXG-PKNH] (last visited Jan. 14, 2020). "The CJEU ruled that 'any real and effective activity – even a minimal one – being exercised through stable arrangements' may suffice to qualify as an establishment in European data privacy law." *Id.*

55. *Id.*

EU" [56] or is somehow otherwise related to "monitor[ing] the behavior of individuals in the EU."[57] This significantly extends the scope of EU privacy law relative to the Directive and other prior attempts at regulation, and means that the aspects of the GDPR enumerated below are applicable to a host of non-EU data controllers not subject to prior EU regulations.[58]

The next important aspect of the GDPR, is the law's fairly stringent consent requirements.[59] Under the GDPR, for a data controller to lawfully process a user's data: the user's consent must be freely given; the user must consent to a specific, unambiguous usage of data; the consent must be fully informed; and the user must be able to revoke their consent at any time.[60] Although these strict consent requirements are an important component of the GDPR, a data controller does not always need a user's consent before using or processing their personal data.[61] Article 6 of the GDPR enumerates six different ways a data controller may lawfully use or process a consumer's personal data, with consent being only one possible avenue for valid processing data usage.[62] However, of the six legal bases for data usage, consent is the one most often used by data controllers. This is because consent empowers the data controller to extensively use the user's data, and because it can be definitively satisfied fairly simply.[63] The consent requirement contained in the GDPR is more stringent than any requirement of the Directive, as the seven principles merely required

---

56. *EDPB Publishes Guidelines on Extraterritorial Application of the GDPR*, HUNTON ANDREWS KURTH: PRIVACY & INFO. SEC. L. BLOG (Nov. 27, 2018), https://www.huntonprivacyblog.com/2018/11/27/edpb-publishes-guidelines-on-extraterritorial-application-of-the-gdpr/ [https://perma.cc/LM8E-BPC2].

57. *Id.*

58. Garrelfs, *supra* note 52.

59. Ann Bevitt, *GDPR – Do I Need Consent to Process Personal Data?*, COOLEY GO, https://www.cooleygo.com/gdpr-do-i-need-consent-to-process-personal-data/ [https://perma.cc/L2H2–6N28] (last visited Jan. 14, 2020) (explaining that "valid consent can be difficult to obtain").

60. *Id.*

61. Wolford, *supra* note 46.

62. *Id.* The other five legal bases for data processing besides consent are: "(1) Processing is necessary to satisfy a contract to which the data subject is a party. (2) You need to process the data to comply with a legal obligation. (3) You need to process the data to save somebody's life. (4) Processing is necessary to perform a task in the public interest or to carry out some official function. (5) You have a legitimate interest to process someone's personal data." *Id.*

63. *Id.* Some of the other legal bases are either too narrow (for example, "need to process the data to save somebody's life") or too broad and ambiguous (for example, "have a legitimate interest to process someone's personal data") to be as useful for data controllers as user consent is. *Id.*

notice of usage of personal data, not affirmative consent by the consumer that their data be used.[64]

The next important aspect of the GDPR is one that has received a significant amount of attention in United States press:[65] the so-called "right to be forgotten."[66] This right is originally derived from the 2014 *Google Spain* case[67] in which the European Court of Justice ruled that EU citizens possess a right to have commercial search engines like Google remove their personal information from search engine results.[68] Although the *Google Spain* case was decided under the Directive,[69] the right was formally codified in Article 17 of the GDPR.[70] Even under the GDPR, however, the right to be forgotten is not absolute and is only applicable in certain circumstances, such as when the data controller's usage of personal data was premised upon the user's valid consent, and the user has chosen to withdraw that consent.[71] There are also a number of instances in which a data controller's desire to use or process personal data can override a user's right to be forgotten.[72] Some of these carve-outs are ambiguous, such as allowing a data controller to override a user's desire to have information erased when "the data is being used to exercise the right of freedom of expression and information."[73] Finally, the ECJ clarified recently that the right to be forgotten does not extend beyond the physical

---

64. *See generally EU Data Protection Directive (Directive 95/46/EC)*, *supra* note 22.

65. *See, e.g.*, James Eng, *Consumer Watchdog: Google Should Extend 'Right to Be Forgotten' to U.S.*, NBC NEWS (July 7, 2015), https://www.nbcnews.com/tech/internet/consumer-watchdog-google-should-extend-right-be-forgotten-u-s-n388131[https://perma.cc/SN6E–7HQZ]; *see also* Farhad Manjoo, *'Right to Be Forgotten' Online Could Spread*, N.Y. TIMES (Aug. 5, 2015), https://www.nytimes.com/2015/08/06/technology/personaltech/right-to-be-forgotten-online-is-poised-to-spread.html [https://perma.cc/QW79-PGFD].

66. Ben Wolford, *Everything You Need to Know About the 'Right to Be Forgotten'*, GDPR.EU, https://gdpr.eu/right-to-be-forgotten/ [https://perma.cc/6MAT–7F2Y] (last visited Jan. 25, 2020).

67. Case C–131/12, Google Spain SL v. Agencia Española de Protección de Datos, 2014 E.C.R. 317.

68. *The Right to Be Forgotten (Google v. Spain)*, ELECTRONIC PRIVACY INFO. CTR., https://epic.org/privacy/right-to-be-forgotten/ [https://perma.cc/D8EX-Z9T2] (last visited Jan. 14, 2020).

69. Case Comment, *Google Spain SL v. Agencia Española de Protección de Datos* 128 HARV. L. REV. 735, 735 (2014), https://harvardlawreview.org/2014/12/google-spain-sl-v-agencia-espanola-de-proteccion-de-datos/ [https://perma.cc/2DHW–7VZQ].

70. Wolford, *supra* note 66.

71. *Id.*

72. *Id.*

73. *Id.* This limitation is particularly relevant to this Note given the concerns expressed by some American legal scholars that a "right to be forgotten" could not work in American law because invocations of the right to be forgotten could potentially infringe upon First Amendment freedom of speech rights. *See generally* Andrea Gallinucci-Martinez, *Is the European Right to Be Forgotten Viable in the Land of the First Amendment?*, 122 PENN STATE L. REV. PENN STATIM 1.

boundaries of the EU's twenty-eight member states, meaning that EU residents likely cannot demand worldwide removal of their information.[74]

Somewhat similar to the right to be forgotten is the next important provision of the GDPR, namely "the right not to be profiled."[75] Defining what exactly constitutes "profiling" a user is not at all clear-cut, and was one of the difficult aspects of the GDPR-drafting process.[76] The current definition of "profiling" contained in the GDPR is less broad than some definitions that were proposed during the drafting process.[77] Per Article 4 of the GDPR, data processing becomes profiling when automated data processing is used to "evaluate certain personal aspects relating to a natural person."[78] Article 22 of the GDPR gives consumers the right not to be subjected to a decision based upon data profiling "which produces legal effects" on the user or "similarly significantly affects" the user.[79] This standard of when a decision is unlawfully made based upon profiling is nebulous on its face, and subsequent attempts at clarification by EU officials have failed.[80] How this provision affects online advertisers is

---

74. Mary Samonte, *Google v CNIL Case C–507/17: The Territorial Scope of the Right to be Forgotten Under EU Law*, EUR. L. BLOG (Oct. 29, 2019), https://europeanlawblog.eu/2019/10/29/google-v-cnil-case-c–507–17-the-territorial-scope-of-the-right-to-be-forgotten-under-eu-law/ [https://perma.cc/2A3E-LJZZ].

75. *What Does the GDPR Say About Automated Decision-Making and Profiling?*, INFO. COMMISSIONER'S OFF., https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/automated-decision-making-and-profiling/what-does-the-gdpr-say-about-automated-decision-making-and-profiling/ (last visited Jan. 14, 2020).

76. Rita Heimes, *Top 10 Operational Impacts of the GDPR: Part 5 – Profiling*, INT'L ASS'N PRIVACY PROFESSIONALS (Jan. 20, 2016), https://iapp.org/news/a/top–10-operational-impacts-of-the-gdpr-part–5-profiling/ [https://perma.cc/PL84-DG5D].

77. *Id.*

78. *Id.*

79. Eduardo Ustaran & Victoria Hordern, *Automated Decision-Making Under the GDPR – A Right for Individuals or a Prohibition for Controllers?*, HOGAN LOVELLS CHRON. DATA PROTECTION (Oct. 20, 2017), https://www.hldataprotection.com/2017/10/articles/international-eu-privacy/automated-decision-making-under-the-gdpr-a-right-for-individuals-or-a-prohibition-for-controllers/ [http://perma.cc/4PL5-LWHV].

80. *Id.* "[T]he position that the data protection authorities have taken on this provision in their draft guidelines generates considerable uncertainty." *Id. See also* Lee Matheson, *WP29 Releases Guidelines on Profiling Under the GDPR*, INT'L ASS'N PRIVACY PROFESSIONALS (Oct. 18, 2017), https://iapp.org/news/a/wp29-releases-guidelines-on-profiling-under-the-gdpr/ [http://perma.cc/88M7-BMQX]. "The WP29 clarifies the GDPR's use of 'legal' or 'similarly significant' effects. . . . 'Similarly significant' effects need not necessarily be legal ones — the working party suggests that threshold is the significance of the decision's impact on the data subject — so to qualify, the processing 'must be more than trivial … the decision must have the potential to significantly influence the circumstances, behavior, or choices of the individuals concerned.'" *Id.* Despite this attempt to clarify what constitutes "similarly significant" effects for the purpose of the right to not be profiled, it seems plain that the definition given by the working party is still fraught with ambiguity.

clearer, however, as the data processing that drives online advertising cannot begin "making decisions that significantly affect individuals" based solely upon profiling.[81]

Another crucial aspect of the GDPR is that it enshrines in Article 20 a right to "portability." This means that users must be allowed to "port," or move their data from one platform or data controller to another if they so desire.[82] The user must be able to receive an electronic copy of their personal data, as well as any pieces of data they have transmitted to the data controller, in a "machine readable format."[83] The user must then be able to transfer—or "port"—that data to another data controller if they wish to do so.[84] Since this provision of the GDPR is a bit abstract, a practical example is helpful. Suppose a Yahoo! Mail user has developed an intricate organization system of folders and keyword filters using their Yahoo! Mail account. This system would likely be a mixture of data that the user has "transmitted" to Yahoo! (e.g., naming a folder "Work") and personal data that Yahoo's algorithms have collected about the user. Under the GDPR's portability requirements, if the user wanted to switch to using Gmail, Yahoo! must provide that user's data to them in a format that could be used by Gmail to recreate the user's organization system in their new Gmail account.[85] While portability seems like a natural, consumer-friendly innovation of the GDPR, implementation has proven difficult, and the portability provision of the GDPR has received significant push-back from businesses that handle users' data.[86] Some commentators also question whether the portability model the GDPR creates will actually work as well for users in practice as it does in

---

81. Ustaran, *supra* note 79.

82. *GDPR – Data Portability*, PWC, https://www.pwc.co.uk/who-we-are/regional-sites/north-west/insights/gdpr---data-portability.html [http://perma.cc/6D24–45UU] (last visited Jan. 14, 2020).

83. *Id.*

84. *Data Portability Under the GDPR: The Right to Data Portability Explained*, I-SCOOP, https://www.i-scoop.eu/gdpr/right-to-data-portability/ [http://perma.cc/QE23–5SK5] (last visited Jan. 14, 2020).

85. Another oft-cited example is that of a user who wishes to move their Spotify library of playlists and recently listened tracks to a competitor like Apple Music. *Id.*

86. *GDPR – Data Portability*, *supra* note 82. "This aspect of the GDPR created consternation among entities with a business model that rely on personal data collected from customers and which view the manipulation and structural format of that data to be one of their main commercial assets." *Id.*

theory.[87] Even if its implementation has not been perfected, however, portability remains an important facet of the GDPR.

Although the core aspects of the GDPR discussed thus far have been designed primarily to benefit consumers and their rights, one aspect of the GDPR, the "one-stop shop" provision, is designed mostly to aid businesses.[88] Instead of dealing with a patchwork of different regulatory agencies often with diverse perspectives and goals concerning how the GDPR's substantive provisions should be implemented and enforced, the one-stop shop allows industry to have a single regulatory body with which to deal for all GDPR matters.[89] Given the disparate national laws that enforce the GDPR in various member states, this provision was designed to help facilitate compliance for organizations engaging in commerce throughout the EU.[90] However, despite the one-stop shop principle's efficacy in theory, in practice, individual member states' legal and regulatory bodies have so far proved reticent to relinquish control over data controllers when the one-stop shop principle should be applicable. This is not altogether surprising given these bodies' hesitancy at the inclusion of the one-stop shop rule in the first place.[91] This reticence was on display, for example, when the *Commission nationale de l'informatique et des libertés* ("CNIL") (the French data regulation agency) fined Google 50 million euros on January 21, 2019,[92] even though the CNIL probably should not have exercised jurisdiction over the matter according to the one-stop shop mechanism.[93]

---

87. *See generally* Robert Madge, *GDPR: Data Portability Is a False Promise*, MEDIUM (July 4, 2017), https://medium.com/mydata/gdpr-data-portability-is-a-false-promise-af460d35a629 [http://perma.cc/4ZJS-FRG6].

88. Lokke Moerel, *What Happened to the One-Stop Shop?*, INT'L ASS'N PRIVACY PROFESSIONALS (Feb. 21, 2019), https://iapp.org/news/a/what-happened-to-the-one-stop-shop/ [http://perma.cc/8ZP2–9BVC].

89. *Id.*

90. Nuria Pastor, *Understanding the One-Stop-Shop Principle*, FIELDFISHER: PRIVACY, SECURITY & INFO. (Jan. 30, 2017), https://privacylawblog.fieldfisher.com/2017/understanding-the-one-stop-shop-principle [http://perma.cc/J29T–6HCZ].

91. Moerel, *supra* note 88.

92. *The CNIL's Restricted Committee Imposes a Financial Penalty of 50 Million Euros Against Google LLC*, CNIL (Jan. 21, 2019), https://www.cnil.fr/en/cnils-restricted-committee-imposes-financial-penalty–50-million-euros-against-google-llc [http://perma.cc/RW58-MYYG].

93. Moerel, *supra* note 88.

Another key aspect of the GDPR is its strict requirements concerning notifying consumers about data breaches.[94] Under the GDPR, data controllers have a legal duty to report a breach—or in some instances even just a potential breach— of consumers' information to the relevant supervisory body within seventy-two hours of the breach's occurrence.[95] If the breach is "likely to result in a high risk of adversely affecting individuals' rights and freedoms," then the consumer victims of the breach must be notified "as soon as possible."[96] Breaches that require consumer notice often involve medical or financial records, but can also include other types of breaches.[97] A simple breach of consumers' contact information, on the other hand, would perhaps not trigger the consumer notification requirement, as it would be unlikely to adversely affect any of the victim consumers' individual rights or freedoms.[98]

The GDPR also institutes heavy fines for non-compliance with the regulation.[99] The GDPR creates two levels of possible fines, based upon the severity of the non-compliance incident.[100] At the lower level, the maximum fine a data controller can receive is either 10 million euros or 2% of the corporation's worldwide revenue from the previous year, whichever is greater.[101] At the upper level of fine, the maximum fine doubles, going up to 20 million euros or 4% of worldwide revenue, whichever is greater.[102] Violations that can trigger the upper range of fines include violations of the consent or non-profiling requirements.[103] Information technology industry analysts have described these fine ranges

---

94. *Personal Data Breaches*, INFO. COMMISSIONER'S OFF., https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/personal-data-breaches/ (last visited Jan. 14, 2020).

95. *Id.*

96. *Id.*

97. Andy Green, *GDPR Data Breach Guidelines*, VARONIS (last updated June 19, 2020), https://www.varonis.com/blog/guide-eu-gdpr-breach-notification-rule/ [perma.cc/87GQ-AJBK]. Other types of breaches that could require consumer notification include breaches involving information about children, breaches involving the consumer's racial or psychological characteristics, or potentially any other large-scale accidental release of data. *Id.* This is largely context-dependent and also dependent on the number of users affected: for example, an accidental release of simple contact information is likely not serious enough to trigger the GDPR's consumer notification requirement standing alone, but if a massive number of consumers' contact information was released, that could trigger the requirement. *Id.*

98. *Id.*

99. *Fines and Penalties*, GDPR EU.org https://www.gdpreu.org/compliance/fines-and-penalties/ [http://perma.cc/YSA4-NXV8] (last visited Jan. 14, 2020).

100. *Id.*

101. *Id.*

102. *Id.*

103. *Id.*

as "sky high," but have also noted that maximum fines so far seem to be rare.[104]

The final provision of the GDPR warranting discussion is how the law deals with data controllers seeking to process the personal data of minors.[105] In cases where the legal basis for processing information is consent, data controllers need parent or guardian consent to process the information of minors below the age of consent.[106] Although the GDPR suggests sixteen as the age of consent for purposes of the regulation,[107] Article 8 allows member states to set the age of consent anywhere between thirteen and sixteen.[108] This has led to variance in the age of consent from country to country: several member states use thirteen, fourteen, or fifteen as their age of consent. [109] Over a third of all member states, however, do use the GDPR's suggested age of sixteen as their age of consent.[110] Not only do these age of consent provisions only apply when consent is the legal basis for a data controller processing information, but they also only apply when businesses offer information services *directly* to children.[111]

Having discussed in detail these nine core aspects of the GDPR, this Note will now examine how personal data could fit into the American property law scheme, before returning to the idea of how an American federal answer to the GDPR could incorporate the nine aspects above.

II. HISTORY AND PHILOSOPHY OF PROPERTY RIGHTS IN AMERICA

What does the American notion of "property" entail? What core philosophies influence this notion of what property is and is not?

---

104. Michelle Drolet, *GDPR Fines: How Much Will Non-Compliance Cost You?*, CSO (Oct. 23, 2017, 8:07 AM), https://www.csoonline.com/article/3234685/gdpr-fines-how-much-will-non-compliance-cost-you.html [http://perma.cc/Q6FY-V3WG].

105. *Minors and the GDPR*, IUBENDA, https://www.iubenda.com/en/help/11429-minors-and-the-gdpr [http://perma.cc/6DN7–5BT5] (last visited January 14, 2020).

106. *Id.*

107. *Id.*

108. International Association of Privacy Professionals, *EU Member States' Age of Consent Under GDPR*, INTERNATIONAL ASSOCIATION OF PRIVACY PROFESSIONALS, https://iapp.org/resources/article/age-of-consent-in-the-gdpr-updated-mapping/ [https://perma.cc/TCB9–35N4] (last visited: January 14, 2020).

109. Ingrida Milkaite and Eva Lievens, *Status Quo Regarding the Child's Article 8 GDPR Age of Consent for Data Processing Across the EU*, BETTER INTERNET FOR KIDS (Dec. 20, 2019), https://www.betterinternetforkids.eu/en_US/web/portal/practice/awareness/detail?articleId=3017751 [https://perma.cc/TZ4Z-DPF6].

110. *Id.*

111. *Id.*

Furthermore, how does American law protect the American notion of property? Because of the quietly revolutionary notion that the GDPR promulgates concerning self-ownership of data,[112] thereby giving EU citizens a property interest in their own data, it is necessary to address the three questions above when considering what an American data privacy law could or should look like. By briefly examining the most fundamental tenets that undergird the American theory of property rights, we will be able to examine both the capacity of the American body of law to incorporate a regulation like the GDPR, as well as the wisdom of an American legal answer to the GDPR.

Any basic legal discussion of what property is begins with the notion that property ownership is akin to a "bundle of rights," including, among other rights, the right to derive income from the property and the right to enforce property rights against others.[113] Because American laws have long protected intangible property as fiercely as tangible property, consumer data—like that protected by the GDPR—can inarguably be considered "property," and must be owned by someone.[114] Many non-European consumers would likely be shocked to learn that they are not in fact owners of their own private data, do not have the right to derive income from their private data or enforce their right to that private data, and that ownership is instead claimed by corporations and internet advertising agencies.[115] It is in keeping with the distinctly American

---

112. *See* Baker, *supra* note 50.

113. *See* Denise R. Johnson, *Reflections on the Bundle of Rights*, 32 VERMONT L. REV. 247, 247 (2012), https://lawreview.vermontlaw.edu/wp-content/uploads/2012/02/johnson2.pdf [http://perma.cc/7C3X-UKNP].

> The modern legal understanding of property ownership in the United States is expressed through a metaphor as a 'bundle of rights' or a 'bundle of sticks.' This is an abstract notion that analytically describes property as a collection of rights vis-à-vis others, rather than rights to a 'thing,' like a house or a piece of land.

Id. However, some legal theorists have increasingly begun to reject the notion of the "bundle of rights" theory as a good method of conceptualizing property rights. *See* Simon Douglas and Ben McFarlane, *Defining Property Rights in* PHILOSOPHICAL FOUNDATIONS OF PROPERTY LAW 219, 219–20 (James Penner & Henry E. Smith, ed., 2013) "[T]he 'bundle of rights' analysis has come under sustained critical pressure." *Id.*

114. There is no direct property rights analogy for self-ownership of data in current American law. However, the most-analogous concept in the realm of intellectual property law would be the idea of "moral rights" that eventually evolved into intellectual property rights statutes. This could help provide the antecedent American legal property law notion for instituting self-ownership of private data under a United States GDPR-like law. *See generally* BARLOW BURKE, ET AL., FUNDAMENTALS OF PROPERTY LAW 873 (4th ed., 2015).

115. *See generally* Eyal Iffergan, *Who Owns Personal Data? GDPR vs. USA*, HyperionGP Research (Feb. 12, 2018) https://insights.hgpresearch.com/who-owns-personal-data-gdpr-vs-usa [http://perma.cc/MEG9-P82N] ((“The new EU standard is a dramatic departure from how American

understanding of individual property rights—rooted in natural law theory—that the rightful owner of information about a consumer must be the consumer themselves. While lay consumers may not be able to succinctly and accurately describe all the personal data that they would have an ownership claim to under a GDPR-like law, it is not any more difficult for a consumer to conceptualize having a right to exclude data controllers from using their information for profit than it is for them to understand the idea of excluding a person or entity from using, for example, their vehicle, home, or image and likeness for commercial profit without permission.[116] With this in mind, let us turn to a brief consideration of the philosophy of American property rights, in the modern and historical contexts.

A. Natural Law and Influential Thinkers

When considering the fundamental aspects of property rights, we must begin with the question: Where does property come from? In answer to this question, there are two general frameworks helpful for distinguishing between different thinkers' methods of defining property. This section will briefly distinguish between two schools of thought about property rights, before considering in more detail the theories of a seminal political philosopher who had a heavy influence on the American founders: John Locke.

Before turning to Locke specifically, we must distinguish between these two schools of thought about property rights. The first school of thought is the "top down approach," which holds that property rights are disseminated from the government "down" to the individual property-holders.[117] Thinkers such as Thomas Hobbes—with his "state of nature" theory—would fall into the category of "top down" thinkers with respect

companies typically treat the billions of bytes of data that they collect each day . . . for American corporations, there are no explicit data privacy protection mandates....") . . . .").

116. This is a fairly straightforward application of the "bundle of rights" method of framing property rights in terms of the owner's relationship with others, rather than with the thing over which ownership is claimed. *See* Johnson, *supra* note 113, at 247.

117. Jeremy Waldron, *'To Bestow Stability Upon Possession' Hume's Alternative to Locke, in* PHILOSOPHICAL FOUNDATIONS OF PROPERTY LAW 1, 1 (James Penner & Henry E. Smith, ed., 2013). ("Property rights [in a top down system] are arbitrary assemblages of rights that the state creates for its own instrumental purposes, and which it can undo almost at will for the same instrumental ends.") (quoting Richard A. Epstein, DESIGN FOR LIBERTY: PRIVATE PROPERTY, PUBLIC ADMINISTRATION, AND THE RULE OF LAW 63 (2011)).

to property rights.[118] According to this "top down" way of thinking about property rights, no individual has any sort of claim on property before the state exists; in other words there are no "pre-political" rights.[119]

On the contrary, other thinkers believe in a "bottom up" conception of private property rights.[120] Although this conception is typically associated with Locke, other influential thinkers such as Hume, Rousseau, and Marx espoused variations of what can generally be considered "bottom up" theories of property rights.[121] Under a "bottom-up" theory of property rights, the rights originate with the individual rather than with the state. [122] Under this sort of theory, "[p]roperty rights are not a gift of the state . . . they have legal standing quite apart from legal rule."[123] Although either a "bottom up" or "top down" schema of private property rights could perhaps support a data privacy approach resembling the one advocated in this Note, the Lockean "bottom up" approach was more embedded in the minds of the constitutional framers, and that framework, therefore, is the one that this Note will primarily reference.

Turning to the writings of John Locke, many of Locke's lasting thoughts about property rights were found in his *Second Treatise of Government* which, despite the title, surveyed a broad range of areas including but not limited to government. Locke believed in so-called inalienable "rights of man," and included property among these inalienable rights. In support of this notion, in his *Second Treatise of Government*, Locke writes:

> For the preservation of property being the end of government, and that for which men enter into society, it necessarily supposes and requires that the people should have property, without which they must be supposed to lose that by entering into society which was the

---

118. *See* Waldron, *supra* note 121, at 6.

119. *Id.* at 1.

120. *Id.*

121. *Id.* at 6. *See also, e.g.*, David Hume, *A Treatise of Human Nature*, PROJECT GUTENBERG (November 10, 2012). Available at: https://www.gutenberg.org/files/4705/4705-h/4705-h.htm#link2H_4_0089. [http://perma.cc/4PW6-RZ5T]. In Book III, Part II, § II of this work (entitled "Of the Origin of Justice and Property"), Hume describes his understanding of property rights:

> No one can doubt, that the convention for the distinction of property, and for the stability of possession, is of all circumstances the most necessary to the establishment of human society, and that after the agreement for the fixing and observing of this rule, there remains little or nothing to be done towards settling a perfect harmony and concord.

Id. Note that this statement by Hume presupposes the existence of property, imagining the role of society vis-à-vis property rights as merely establishing a "rule" that recognizes the preexisting natural order.

122. Waldron, *supra* note 117, at 1.

123. *Id.*

> end for which they entered into it; too gross an absurdity for any man to own.[124]

This understanding of property rights—as not only existing in a pre-political context but also being the reason for which political associations are formed in the first place—would prove to be influential on the American founders.[125]

B. The Views of the Founders

The Declaration of Independence guarantees all individuals the unalienable rights of "life, liberty, and the pursuit of happiness."[126] Although the Declaration of Independence is not a binding legal document, it is still helpful when attempting to analyze what exactly the founders believed about fundamental rights at the instant of the founding. "Life, liberty and the pursuit of happiness," unlike Locke's "life, liberty, and property" does not imply that natural law property rights were less important to the Founders than they were to Locke.[127] On the contrary, this statement was in some ways just a reframing of Locke's basic theories. "We hold these truths to be self-evident" seems clearly rooted in the same natural law concepts that drove Locke, and Thomas Jefferson was influenced by Locke.[128] In fact, any fundamental disagreement between Locke and Jefferson would likely be about what precisely "self-evident" meant and not whether property rights are a fundamental aspect of natural law theory.[129]

---

124. John Locke, *Second Treatise of Government* at §138.

125. *See generally* Don L. Doernberg, *'We the People': John Locke, Collective Constitutional Rights, and Standing to Challenge Government Action*, 73 CALIF. L. REV. 52 (1985); *contra* Chester James Antineau, *Natural Rights and the Founding Fathers—the Virginians*, 17 WASH. & LEE L. REV. 43, 65 (1960) ("When Thomas Jefferson omitted from the Declaration of Independence the third in the triumvirate of Locke's natural rights . . . he rather clearly indicated that to him property was not a highly significant natural right.").

126. National Archives, *Declaration of Independence: A Transcription*, NATIONAL ARCHIVES https://www.archives.gov/founding-docs/declaration-transcript. [http://perma.cc/UFV8-D7HM] (last visited: Jan. 26, 2020).

127. *Contra* Antineau, *supra* note 125.

128. Robert Curry, *Jefferson, Locke, and the Declaration of Independence*, CLAREMONT REVIEW OF BOOKS (Mar. 17, 2017), https://www.claremont.org/crb/basicpage/jefferson-locke-and-the-declaration-of-independence/https://www.claremont.org/crb/basicpage/jefferson-locke-and-the-declaration-of-independence/ [http://perma.cc/3ZR3-LKF3].

129. *Id.*

In addition to Thomas Jefferson, founder Thomas Paine also wrote and thought about property rights. Paine's *Common Sense* shows that he is a proponent of the natural rights theory, much like Locke, and includes a fundamental notion of a right to property.[130] In *Common Sense*, he writes of "securing freedom and property to all men" as the goal of the colonial revolutionaries of his day.[131] Thomas Paine's *Agrarian Justice*, in which Paine argued that private property is necessary so long as all inhabitants of the earth are adequately provided for, also shows Paine's beliefs about property rights and their integral role in his philosophy.[132] "Equality of natural property is the subject of this little essay," Paine writes in *Agrarian Justice.*[133] "Every individual in the world is born therein with legitimate claims on a certain kind of property, or its equivalent."[134]

The work of founders John Jay, Alexander Hamilton, and James Madison in *The Federalist Papers* are also at times indicative of how the founders' thoughts about property rights. For example, in Federalist #10, although primarily issuing a warning about the dangers of factions, Madison takes care to recognize the primacy of private property rights—for better or worse—in a democratic constitutional scheme.[135] This Lockean analysis is heavily rooted in natural law concepts.[136] Likewise, in Federalist #54, Madison writes, "Government is instituted no less for the protection of the property than of the persons of individuals."[137] Although this perhaps muddies the waters a bit by introducing terminology that gestures in the direction of a top down theory of property rights,[138] it is

---

130. Thomas Paine, *Common Sense*, BILL OF RIGHTS INST., https://billofrightsinstitute.org/founding-documents/primary-source-documents/common-sense/ [http://perma.cc/9UP9-BMV9] (last visited January 26, 2020).

131. *Id.* In addition to the quote given, Paine mentions "property" ten other times in the short pamphlet.

132. *See generally* Thomas Paine, *Agrarian Justice*, PARIS SCHOOL OF ECONOMICS, http://piketty.pse.ens.fr/files/Paine1795.pdf [https://perma.cc/DZT7-B69N] (last visited January 26, 2020).

133. *Id.* at iii.

134. *Id.*

135. As Madison writes in Federalist #10:

> The diversity in the faculties of men, from which the rights of property originate, is not less an insuperable obstacle to a uniformity of interests. The protection of these faculties is the first object of government. From the protection of different and unequal faculties of acquiring property, the possession of different degrees and kinds of property immediately results; and from the influence of these on the sentiments and views of the respective proprietors, ensues a division of the society into different interests and parties.

THE FEDERALIST NO. 10 (James Madison).

136. *See* Locke, *supra* note 121128.

137. THE FEDERALIST NO. 54 (James Madison).

138. *See generally* Waldron, *supra* note 121.

still possible to infer a Lockean understanding of property rights from the Federalist papers. This is because if government must exist to protect property, then property must be existent prior to the state. Therefore, private property rights must be fundamental, not a construction of the state.

Next, in Federalist #79, Hamilton writes that "[i]n the general course of human nature, a power over a man's subsistence amounts to a power over his will."[139] This statement cuts both ways, suggesting that humanity retains some fundamental right to that which provides its subsistence, a Lockean proposition, but one that also echoes the Hobbsian"state of nature".[140] Regardless, it is clear from these excerpts that natural law theory played a role in defining the constitutional framers' thinking about private property rights.

Lastly, to learn what the framers of the Constitution thought about private property rights, and about privacy more broadly, we can look to the text of the Constitution itself. We can look to the Fourth and Fifth Amendments primarily. The Fourth Amendment clearly respects a fundamental—albeit penumbral[141]—notion of private property rights, rooted in natural law, when it provides for "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures."[142] Within the Fifth Amendment, the Due Process Clause is relevant, with its notion that no citizen may be "deprived of life, liberty, or property, without due process of law,"[143] which again clearly is undergirded by a fundamental natural law notion of private property rights, as it presupposes that property must have existed before the state.[144] Finally, the Takings Clause also supports this notion, as it protects against the taking of "private property" for public use without just compensation.[145]

---

139. THE FEDERALIST NO. 79 (Alexander Hamilton).
140. *See* Waldron, *supra* note 114 at 6.
141. Griswold v. Connecticut, 381 U.S. 479, 484 (1965).
142. U.S. Const. amend. IV.
143. U.S. Const. amend. V.
144. *See generally* Waldron, *supra* note 114121.
145. U.S. CONST. amend. V.

C. Owning Ourselves: Data as Property

The above analysis of the concepts that undergird the American scheme of private property rights is important to the purposes of this Note because it shows that private property rights are fundamental to the American legal and constitutional scheme. This matters because, given how much data we generate as modern consumers, it doesn't make sense for something so ubiquitous and deeply personal as data to *not* be considered property, given how important personal property rights are in our society and in our laws, and how much Americans value owning property. Furthermore, our legal system has shown a willingness to extend property rights to other intangible interests, so it is not too much of a leap to extend property rights to personal data.[146]

With these important fundamental characteristics of American property rights in mind, as well as how they might apply to self-ownership of personal data, this Note next briefly turns to how these property rights have been expanded by the Supreme Court into the area of privacy.

III. THE U.S. SUPREME COURT'S PRIVACY LAW PRECEDENT

Although it is an open question as to exactly how a legislature would implement a GDPR-like regulation enshrining a digital right to privacy in the United States and incorporate it into the body of American statutory law, the idea of a constitutional right to privacy is far from a new one. The American notion of a right to privacy is often traced back to an 1890 law review article co-authored by then-future Supreme Court Justice Louis Brandeis.[147] "The principle which protects personal writings and any other products of the intellect or of the emotions," the article reads, "is the right to privacy, and the law has no new principle to formulate when it extends this protection to the personal appearance, sayings, acts, and to personal relation, domestic or otherwise."[148] The year after that article was published the Supreme Court echoed its core tenets by finding that a woman injured while traveling on a railcar could not be forced to submit to a physical examination of her injuries by the railroad company.[149]

---

146. *See generally* BURKE, ET AL., *supra* note 114 at 873.

147. Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890).

148. *Id* at 213.

149. Union Pacific R. Co. v. Botsford, 141 U.S. 250 (1891). "No right is held more sacred...than the right of every individual to the possession and control of his own person, free from all restraint or interference of others, unless by clear and unquestionable authority of law." *Id.* at 251.

Furthermore, once Justice Brandeis was on the Court decades later, he was able to vindicate his views about privacy expressed in the article (albeit in dissent) as he wrote of the "indefeasible right of personal security, personal liberty and private property."[150]

The Court's privacy jurisprudence picks up in earnest several decades later, with the line of cases begun with *Griswold v. Connecticut*.[151] In upholding the right of a married couple to use contraception, Justice Douglas, writing for the Court, used the word "privacy" twelve times, finding that even though the Constitution does not use the word privacy, the "penumbra"[152] of the First and other amendments clearly imply the privacy right.[153] The *Griswold* Court held that the privacy right was furthermore implied by the First, Third, Fourth, Fifth, and Ninth Amendments.[154] In the years since *Griswold*, the Court has frequently returned to the right to privacy to justify a host of developments of substantive law, including the right to be free from a government wiretap in a public phone booth,[155] a woman's right to receive an abortion,[156] the right to engage in homosexual activity in the privacy of one's own home,[157] and—in a case that cited Justice Brandeis' *Olmstead* dissent—to uphold citizens' right to be free from unreasonable searches of cell phone record and data.[158]

Although these cases do not cohere into a seamless framework of what the American notion of privacy encompasses, they illustrate how the idea of privacy has seeped into otherwise disparate areas of American jurisprudence. Given this expansion, it would be no great logical leap to extend the right to privacy to consumers' daily interactions with dozens of apps and websites. Just as the right to privacy has mutated in the past to meet advances in technology, so too can it shift to fit a 21st-century understanding of the risks posed to privacy by misuse of personal data. As discussed in the next section, stronger protections against data misuse are

---

150. Olmstead v. United States, 277 U.S. 438, 474–75 (1928) (Brandeis, J., dissenting).
151. 381 U.S. 479 (1965).
152. "Penumbra" comes from the Latin word for "shadow." *See* William Safire, *On Language; The Penumbra Of Desuetude*, N.Y TIMES MAGAZINE (Oct. 4, 1987), https://www.nytimes.com/1987/10/04/magazine/on-language-the-penumbra-of-desuetude.html.
153. 381 U.S. at 484.
154. *Id.*
155. Katz v. United States, 389 U.S. 347 (1967).
156. Roe v. Wade, 410 U.S. 113 (1973).
157. Lawrence v. Texas, 539 U.S. 558 (2003).
158. Carpenter v. United States, 138 S. Ct. 2206 (2018).

not only supported by American legal precedent but is also mandated by current American policy needs.

IV. PUBLIC POLICY AND PUBLIC OPINION CONSIDERATIONS SUPPORTING A GDPR-LIKE SCHEME

A. Prominent Data Use Scandals Demonstrate the Policy Need for a GDPR-Like Scheme

A growing number of significant, often highly publicized instances of data breach or misuse scandals underscore the need for a federal regulation like the GDPR. It would be impossible to outline all these scandals, so this Note will briefly reference a few illustrative ones, merely to show that data breaches are a serious enough concern to American consumers to justify a GDPR-like regulation. A very significant data breach involving consumers' personal financial information, the Equifax breach, affected some 147 million consumers and involved a settlement with regulators valued at up to $700 million.[159] Similarly, the Yahoo! data breach, which also involved a settlement that allows the affected users to file a monetary claim, although that settlement was much smaller in total than the Equifax one, valued at $117.5 million in total, or $358 per consumer.[160] Other data breaches might be smaller in scale, but involve such sensitive information that they still cause concern for consumers. For example, in 2020 Walgreens disclosed that its mobile pharmacy app malfunctioned and allowed an undisclosed number of users to view other users' private health information—including names of drugs prescribed to individuals.161 Finally, in early 2021 the menstruation and fertility tracking app Flo received a large fine from the FTC for sharing users' data with third-

159. *See* Tara Siegel Bernard, *Equifax Breach Affected 147 Million, but Most Sit Out Settlement*, N.Y. TIMES (Jan. 22, 2020), https://www.nytimes.com/2020/01/22/business/equifax-breach-settlement.html [https://perma.cc/8P82-TMG9].

160. Scottie Andrew, *Yahoo Could Pay You $358 for Its Data Breach Settlement*, CNN (Oct. 15, 2019), .https://www.cnn.com/2019/10/15/business/yahoo-data-breach-settlement-trnd/index.html.https://www.cnn.com/2019/10/15/business/yahoo-data-breach-settlement-trnd/index.html [https://perma.cc/BSY3-WAN8].

161. Jessica Davis, *Walgreens Reports Data Breach from Personal Mobile Messaging App Error*, HEALTH IT SECURITY (Mar. 2, 2020), https://healthitsecurity.com/news/walgreens-reports-data-breach-from-personal-mobile-messaging-app-error. [https://perma.cc/H6P9-E758]. Although this data breach involved health data, the app is not regulated by the Health Insurance Portability and Accountability Act (commonly known as "HIPAA"), so it is still a data issue that requires a GDPR-like general data privacy law in order to be regulated. *See id.*

parties (like Facebook and its advertisers) despite promising users it would not do so.[162]

B. Business Community's Growing Openness to a Federal Privacy Law

Data privacy has become a salient issue of public policy (and of law) as data breaches have become a regular occurrence in corporate America. Although not all—or perhaps not even most—data breaches are a result of poor data management policies, the lack of transparency about how companies use private data has become an increasingly important area of consumer protection. Furthermore, despite increasingly frequent breaches, corporations that make use of "big data" continue to reap significant profits from use of consumers' data.[163]

A need for greater transparency and regulation concerning data usage is apparent not only to consumer protection advocates, but also to some within the tech industry itself. The co-founder and then-CEO of Salesforce, Marc Benioff, recently published an op-ed in *Politico* advocating for a nationwide data privacy law.[164] Although Benioff stopped short of advocating for consumer protections as strong as the GDPR, It is likely that more and more tech executives will begin to see the benefits of a nationwide data privacy law, both to preserve good will with consumers as public trust in big tech companies continues to fall, and to avoid a patchwork of state-by-state regulations.

The problem of patchwork regulation is already becoming reality, because, as mentioned above, beginning with California's passage of the CCPA in the summer of 2018, multiple states have begun state-level

---

162. Natasha Lomas, *Flo Gets FTC Slap for Sharing User Data When It Promised Privacy*, TECHCRUNCH (Jan. 13, 2021), https://techcrunch.com/2021/01/13/flo-gets-ftc-slap-for-sharing-user-data-when-it-promised-privacy/. [https://perma.cc/Q6JX-THF8].

163. *See generally* Jori Hamilton, *Big Data Means Big Money*, DATAFLOQ (Sep. 27, 2019), https://datafloq.com/read/big-data-means-big-money-businesses-profitable/6930https://datafloq.com/read/big-data-means-big-money-businesses-profitable/6930 [perma.cc/U3D5–4BG9].

164. Marc Benioff, *Time for Silicon Valley to Get Behind a National Privacy Law*, POLITICO (June 19, 2018), https://www.politico.com/agenda/story/2018/06/19/silicon-valley-national-privacy-law–000679.https://www.politico.com/agenda/story/2018/06/19/silicon-valley-national-privacy-law–000679 [perma.cc/R2HJ-JW25]. Salesforce is a large cloud-based software company, founded in 2001 and publicly traded on the New York Stock Exchange since 2004. Jason Compton, *Salesforce.com IPO Raises $110 Million,* DESTINATION CRM (June 23, 2004), https://www.destinationcrm.com/Articles/CRM-News/Daily-News/Salesforce.com-IPO-Raises-$110-Million–44252.aspx [https://perma.cc/H2FG-VBGD].

passing privacy laws.[165] Those laws will force tech companies to be more transparent about their use of consumer data and will grant users far more control over how their personal information is or isn't used than consumers currently possess.[166] However, there is concern that, given the strength of the tech lobby in California, tech firms might be able to undermine or thwart the CCPA's effectiveness,[167] despite the fact that any businesses that are deemed to be non-compliant under CCPA face stiff penalties.[168] The requirements for what businesses are covered by the California law additionally make it unlikely that any company will be surprised by the regulation, as any company regulated by the law is almost certain to have a large compliance department, making any non-compliance truly intentional.[169] However, the privacy situation in California is still fluid, as evidenced by the passage of the CPRA, which strengthened California consumers' privacy rights beyond what the CCPA provided.[170]

---

165. *See generally* Murphy, *supra* note 10.

166. *See generally* Jill Cowan and Natasha Singer, *How California's New Privacy Law Affects You*, NEW N.Y. TIMES (Jan. 3, 2020), https://www.nytimes.com/2020/01/03/us/ccpa-california-privacy-law.html. [https://perma.cc/E8ME-JQES].

167. *See* Los Angeles Times, *Editorial: Keep California's New Privacy Protections Safe from Tech Company Meddling*, L.A. TIMES (August 16, 2019 2:54 P.M.) https://www.latimes.com/opinion/story/2019–08–26/california-online-privacy-law-data-collection-ccpa [https://perma.cc/523S-WX45].

> Arguing that some key provisions are unworkable, industry lobbyists have pushed to allow more types of data to be excluded from the law's protections and allow more information to be sold. Meanwhile, privacy groups have sought to hold companies accountable for every violation and to give individuals the right to sue companies that run afoul of the law.

Id.

168. *See* Kevin Smith, *California Consumer Privacy Act Will Impact Businesses that Collect and Receive Personal Data*, THE ORANGE COUNTY REG. (Sept. 3, 2019), https://www.ocregister.com/2019/09/03/california-consumer-privacy-act-will-impact-businesses-that-collect-and-receive-personal-data/ [https://perma.cc/9ARP-SVLG].

169. Smith, *supra* note 139.

> The law will apply to a business if it, or an entity it controls or that controls it, collects or receives personal information from California residents, either directly or indirectly, and meets one or more of the following criteria: (1) Has annual gross revenue that exceeds $25 million; (2) Annually receives, buys, sells or shares directly or indirectly the personal information of 50,000 or more California residents, households or devices; (3) Half or more of its annual revenue comes from the sale of personal information about California consumers.

Id. (numbering and punctuation added).

170. Allison Grande, *Calif. Voters Back Bid to Toughen Consumer Privacy Law*, LAW360 (Nov. 4, 2020), https://www.law360.com/articles/1324594/calif-voters-back-bid-to-toughen-consumer-privacy-law. [https://perma.cc/R5KR-YWS8].

V. MOVING FORWARD: WHAT THE NEXT LEGAL STEPS COULD AND SHOULD LOOK LIKE

A. Basic Proposal: Institute a GDPR-Like Scheme

This Note advocates that US lawmakers should adopt a law like GDPR that also incorporates the changes made to the GDPR by the California Privacy Act,[171] except for the CCPA's provision that data controllers do not automatically need a legal basis for processing user data.[172] That provision of the CCPA is vastly different from the GDPR's requirement that processing of user data must be grounded in consent or another legal basis explicitly provided by the law.[173] Otherwise, this Note advocates that in all other aspects the US regulatory framework should adhere as closely to the EU one as possible, adopting each of the nine core tenets of the GDPR described in this Note.[174] The law would likely need to pre-empt the CCPA in order to be effective and avoid patchwork regulation.[175]

The impetus to pass federal legislation in this area is growing rapidly, as other states besides California consider passing legislation similar to the CCPA. For example, in early 2021, Virginia passed the Consumer Data Protection Act, which is similar to the CCPA and also has drawn comparisons to the GDPR.176 This Note maintains that these different state-by-state privacy laws popping up across the country are all the more reason to pass a federal privacy law as soon as possible. In the interim,

---

171. *See generally* Carol A.F. Umhoefer & Tracy Shapiro, *CCPA vs. GDPR: The Same, Only Different*, DLA PIPER (April 11, 2019), .https://www.dlapiper.com/en/us/insights/publications/2019/04/ipt-news-q1–2019/ccpa-vs-gdpr/https://www.dlapiper.com/en/us/insights/publications/2019/04/ipt-news-q1–2019/ccpa-vs-gdpr/ [https://perma.cc/4MTJ-Q5NQ].

172. *Id.* "Most crucially, the CCPA does not require businesses to have a 'legal basis' (a justification set forth in GDPR) for collection and use of personal information." *Id.*

173. *See* Wolford, *supra* note 66.

174. Although some technical concessions will likely be necessary given the differences between the American and European legal systems, that is largely beyond the scope of this Note.

175. In addition to the simple fact that it is unwise for a federal law to conflict with a state one, the California Privacy Act would also need to be pre-empted because in some areas commentators have suggested that the California law does not go as far as the policies that this Note advocates would. *See* David Priest, *Google and Facebook Treating Your Data Like Property Would Be Terrible*, CNET (October 4, 2019), https://www.cnet.com/news/google-and-facebook-treating-your-data-like-property-would-be-terrible/ [https://perma.cc/S83D-WPMD] ("Even California's Consumer Privacy Act – the most comprehensive piece of privacy legislation in the US as of 2020 – only protects consumers part way: Companies must inform California citizens of their intent to collect data and they must comply with customer requests to delete said data.").

176. *See* Rippy, *supra* note 12.

however, coordination between federal and state privacy regulators will be of crucial importance, a fact recognized by a bipartisan group of senators who on January 23, 2020, introduced the Cybersecurity State Coordinator Act of 2020,[177] although the bill has yet to become law as of this writing.178

As United States lawmakers consider this weighty issue of consumer data privacy and ponder whether to upend the current patchwork of state-level legislation, the debate over what provisions the law should and should not have is likely to shift rapidly. Some ideas about the law are likely to, for better or worse, come from tech industry leaders. The new US law would likely need to address Facebook founder Mark Zuckerberg's concerns about needing "clear rules on when information can be used to serve the public interest and how it should apply to new technologies such as artificial intelligence."[179] Congress would likely seek input from leaders in the information technology field in order to ensure that the law will be cutting-edge. As with all technology-specific regulations, there is always a concern that by the time the regulation takes effect, the field will have already shifted.

B. Questions About a GDPR-Like Scheme and Potential Arguments Against One

Although this Note advocates that the United States should institute a regulatory framework similar to the GDPR, that position is certainly not without its detractors or questions. While this Note will inevitably be unable to fully address all possible concerns about or counterarguments to the institution of a GDPR-like regulatory framework in the United States, there are some arguments that have sufficient merit to warrant mentioning within the scope of this Note.

---

177. John Rondini, *New Federal Legislation Seeks to Appoint a Cybersecurity Coordinator for Each State*, JD SUPRA (Jan. 23, 2020), https://www.jdsupra.com/legalnews/new-federal-legislation-seeks-to–78994/.https://www.jdsupra.com/legalnews/new-federal-legislation-seeks-to–78994/ [https://perma.cc/75XK-TTTG]. This law would require state cybersecurity coordinators to coordinate with a federal cybersecurity coordinator about various legal matters, especially related to cyberattacks. *Id.*

178. *S.3207 - Cybersecurity State Coordinator Act of 2020*, CONGRESS.GOV, https://www.congress.gov/bill/116th-congress/senate-bill/3207/actions. [https://perma.cc/28SC-CDL2].

179. Mark Zuckerberg, *Four Ideas to Regulate the Internet*, FACEBOOK (Mar. 30, 2019), https://newsroom.fb.com/news/2019/03/four-ideas-regulate-internet/https://newsroom.fb.com/news/2019/03/four-ideas-regulate-internet/ [https://perma.cc/2D49-W6KN].

One concern about a GDPR-like law is regarding what happens when information protected by the law pertains to multiple consumers. In an instance like this it is not necessarily clear which consumer would be the owner, and unless the proposed US law clearly defined the boundaries in this area, some sort of legal test would likely be necessary. Furthermore, it is not at all clear whether multiple consumers would be able to split ownership of personal data, which seems like the logical answer to the concern raised above but raises some tricky and technical property law issues. Joint ownership of intellectual property is allowed under US law,[180] but how could this joint ownership be legally codified when in some instances the data in question might pertain to two users in opposite sides of the country who have never met each other?

Another question that might be raised by the proposed US law, and that is tangentially connected to the question of the preceding paragraph, is if corporations are legally considered to be persons under US law, why should we value the rights of so-called "natural persons" to data over the rights of "corporate persons" to the same data?[181] Would corporate persons be protected as equally as natural persons by the GDPR-like law in the United States? This question is two-fold: first would they be legally required to be equally protected under *Citizens United*, and second, if not required, would it be sound policy for them to be?

There might be questions about the "right to be forgotten" provision of the GDPR, and implementation of this right becomes difficult when that proposed right begins to negatively intersect with the criminal law. Would a right to be forgotten, as is embedded in the GDPR and as this Note advocates should also be embedded in the proposed US law, adversely affect law enforcement proceedings?[182] Another question about the right to

---

180. *See, e.g.*, *Joint Ownership of Intellectual Property: Everything You Need to Know*, UPCOUNSEL, https://www.upcounsel.com/joint-ownership-of-intellectual-property [https://perma.cc/LCL5-WW9D] (last visited Jan. 27, 2020).

181. Citizens United v. Federal Election Commission, 558 U.S. 310 (2010).

182. *See* Jaclyn Jaeger, *TRACE: How the GDPR interferes with anti-corruption compliance*, COMPLIANCE WEEK (May 6, 2019), https://www.complianceweek.com/anti-bribery/trace-how-the-gdpr-interferes-with-anti-corruption-compliance-/27030.article [https://perma.cc/BZ5F-YHU2].

> Article 10 of the GDPR prohibits the processing of personal data relating to criminal convictions and offenses, unless 'carried out only under the control of official authority or when the processing is authorized by [European] Union or [EU] Member State law providing for appropriate safeguards for the rights and freedoms of data subjects.

Id. See also Illya Antonenko, *Conflicts Between GDPR and Corporate Anti-bribery Compliance: OECD Working Group Invites Comments*, THE FCPA BLOG (May 2, 2019 11:48 AM),

be forgotten, from the perspective of industry rather than law enforcement, is whether this new right would encourage fraudulent behavior?[183] Although this is partially just a procedural question that Congress could work out, it is fair to ask whether, if consumers are allowed to sell their personal data to the highest bidder, how explicit and informed their consent would have to be for this transfer to be legally binding? Although that concern is largely procedural, it also goes to the heart of the policy issues the law would seek to address, as well as the fundamental notion that "we all own our own data," discussed in various places in this Note.[184]

Finally, some scholars question whether the right to be forgotten would also have an adverse effect on some persons and entities' First Amendment free speech rights, by allowing persons to make "right to be forgotten" requests simply because they don't like the information reported about them.[185] Although United States courts have not addressed this issue, the Supreme Court heard a case in 2015 that would have required the Court to rule on an issue at the intersection of free speech and a consumer's desire to have their data erased.[186] In the end, however, the Court avoided the substantive data rights issue by finding the plaintiffs lacked standing to sue.[187]

There are also broader policy concerns about what happens when a user decides that they want to allow companies or websites to use their personal data. One proposal is to allow users to then re-sell their data to companies or websites that want to acquire it. Would this free-market solution create perverse incentives and unintended consequences? For example, would access to popular websites include as a pre-condition that the user relinquish all rights to any personal private data that the website collects? Would this perhaps totally undercut the law's substantive regulations?

This again gets to the heart of the reasons for a GDPR-like law, and to the presuppositions that support such a law. If we truly "all own our own data"[188] is there any way to avoid a free market system like this? What

---

https://fcpablog.com/2019/5/2/conflicts-between-gdpr-and-corporate-anti-bribery-compliance [https://perma.cc/KP47-BKSJ]

183. Zac Cohen, *The Fraud Risk Underlying GDPR's 'Right to Be Forgotten'*, TRULIOO (July 3, 2018), https://www.trulioo.com/blog/fraud-risk-gdpr/ [https://perma.cc/R2P3-XHW4]].

184. *See* Baker, *supra* note 50.

185. *See generally* Gallinucci-Martinez, *supra* note 73.

186. Spokeo, Inc. v. Robins, 578 U.S. 330 (2016).

187. *Id.* The case involved a claim under the Fair Credit Reporting Act that alleged that Spokeo had posted incorrect information about a job-seeking plaintiff on their website, but the Court dismissed for lack of injury-in-fact.

188. *See* Baker, *supra* note 50.

would possible alternatives to a free market system be? How would agencies regulate the free market system? Which US agency would have jurisdiction? Perhaps the Federal Trade Commission,[189] but would not both the volume and tiny nature of these transactions make it out of place compared to what the Federal Trade Commission normally governs? In light of this concern, would perhaps a system of full transparency and disclosure be preferable to a system in which users actual "own" their own data?

Despite all these potential pitfalls associated with an American answer to the GDPR, a GDPR-like law is still needed in the US. Also, and perhaps most importantly, none of these concerns are significant enough to override the key concern that without a GDPR-like federal regulation, we are facing a state-by-state patchwork regulatory scheme. Therefore, despite the immense challenges associated with such a law, this Note maintains that the best way forward with respect to consumers' privacy rights is a federal law that largely mirrors the GDPR.

CONCLUSION

As technological development continues at a dizzying pace, it remains vitally important that American law attempt to match technology's pace as much as possible. Concerns about how consumers' data is processed and used by tech companies and advertisers is growing ever stronger, and it is increasingly clear that the regulatory answer to these concerns must come at the federal level. Looking to the examples of the GDPR and the CCPA, the United States Congress should institute a comprehensive regulatory framework that aggressively protects consumers' data privacy rights. Such a scheme would be in keeping with the fundamental American notion of private property rights understood by the founders and by the thinkers who influenced them. In a society as concerned with individual liberty as ours, it should not stretch the American legal or moral consciousness to suggest that each and every one of us should own our own data.

This Note is far from the first attempt to justify the property interest that feels inherent to personal data, and it will likely not be the last. There are as many good philosophical rationales for self-ownership of data as there are policy ones. The ethicist and computer scientist Luciano Floridi

189. *See generally* Richards et al,. *supra* note 9.

gave two examples of these philosophical arguments in a talk he gave in 2018 at Santa Clara University:

> [There are] two ways of looking at personal data. One is in terms of the philosophy of economics. Your data are yours as in 'My data, my house, my car: I own it . . . and if you trespass, you are trespassing the boundaries of my property.' . . . . Then there's another way of looking at personal information, that's got to do not with the philosophy of economics—broadly understood—but with the philosophy of mind—the philosophy of personal identity. My data, or my personal memories, are more like my hand, my liver, my lungs, my heart. It's not that they are mine because I own them; they are mine because they constitute me . . . . Making a copy of my data [is] not taking away that data, but there's something about cloning here, and being intrusive, that's got nothing to do with trespassing, but more like kidnap.[190]

Regardless of which precise philosophical rationale we select, the implication is clear: we should have a personal property interest in our personal data. Exactly how American legislators and regulators could choose to codify that right remains to be seen, but the GDPR is clearly an instructive example. But whatever path lawmakers choose, the time has come for us to own our own personal data—since in our modern society that truly means owning ourselves.

---

190. Irina Raicu, *Do You Own Your Data?*, MARKKULA CTR. FOR APPLIED ETHICS AT SANTA CLARA U. (Aug. 29, 2018), https://www.scu.edu/ethics/privacy/do-you-own-your-data/. [https://perma.cc/YN2V–3DKA].