Planting in a Walled Garden: Data Portability Policies To Inform Consumers How Much (if any) of the Harvest is Their Share

Whitney Nixdorf

INTRODUCTION

"The goal of the Web is to serve humanity. We build it now so that those who come to it later will be able to create things that we cannot ourselves imagine." —Tim Berners-Lee[1]

As creator of the World Wide Web, Tim Berners-Lee envisioned a world where "any person could share information with anyone else, anywhere."[2] In the last decade, the information-sharing capabilities of the Internet and accompanying devices and "things" has exploded, enabling vast amounts of data to be collected, processed, and used to draw inferences, make connections, and solve problems.[3] We have only just begun to explore the possible uses for data on such an enormous scale, and important issues arise in the context of personal data about individuals.

Much of the information being aggregated is generated by people, about themselves, and as such, they have certain expectations about ownership and privacy regarding "their" data.[4]

However, Berners-Lee and other experts are concerned that increased centralization by tech giants like Facebook, Google, and Apple fragments the Web by "locking in" user data into information "silos," which keep users from exercising control over the information they provide to the service.[5] Each company amasses a "treasure trove of content" which it chooses to share only with select services.[6] This "walling off" of data has increasingly become the norm as tech giants seek to become one-stop shops for users, enticing (maybe even coercing) them to stay within a carefully tended and personalized garden for all their social interactions, shopping, and even news consumption.[7] It is true that the open Web is full of misinformation, spam, and even criminal actors, and walled gardens may be "generally nice places to hang out"—but what happens when the price users pay for a pleasant experience is a service

---

[1] Tim Berners-Lee, *Long Live the Web*, 303 SCI. AM. 80, 80 (2010).

[2] *Id.* at 80.

[3] *See, e.g.*, Omer Tene & Jules Polonetsky, *Big Data For All: Privacy and User Control in the Age of Analytics*, 11 NW. J. TECH. & INTELL. PROP. 239, 240 (2013).

[4] *See, e.g.*, *id.* at 269.

[5] Berners-Lee, *supra* note 1, at 82.

[6] Ryan Holmes, *From Inside Walled Gardens, Social Networks Are Suffocating The Internet As We Know It*, FASTCOMPANY (Aug. 9, 2013), https://www.fastcompany.com/3015418/from-inside-walled-gardens-social-networks-are-suffocating-the-internet-as-we-know-it.

[7] *Id.*

so proprietary that, once they invest their time and data, they cannot get it back or use it anywhere else?[8]

About 91 percent of U.S. residents feel that they have lost control over their personal data and how it is used.[9] Many feel that the time has come to shift our thinking about the control and flow of personal data by moving from the silo model to something more like what Berners-Lee imagined. After all, freely shared data has given us many useful innovations like Yelp and Airbnb, and the possible uses for individuals' aggregated data are tremendous: what if users could take data from all their social networking systems and combine it with data from their calendars, fitness trackers, and smart home devices?[10] It seems that access to such cross-platform data would prompt robust innovation, as software developers and entrepreneurs would rush to create new tools to help people get meaningful use out of their information.[11] In the financial sector, consumers are able to make use of their account data to benefit from services such as personal financial management tools, automatic savings programs, budget analysis, bill payment, and identity theft protection.[12] But in the largely unregulated area of social networking, for example, consumers lack knowledge about the value and utility of their data.[13] Furthermore, there are legal constraints on the concept of data portability—the ability to access one's data and "port" it to another website, platform, or service provider.[14]

In Europe, however, the General Data Protection Regulation (GDPR) creates a fundamental right to data portability for EU citizens.[15] This right allows EU data subjects to receive information that they provided to a controller, "in a structured, commonly used and machine-readable format," or have it transferred to another data controller.[16] Legislators have expressed

---

[8] *Id.*

[9] Letter from Joseph Jerome, Center for Democracy & Technology, *Response to Office of Science and Technology Policy Request for Information Regarding Data Portability* 5 (2016).

[10] *See id.* at 3; *see also* Holmes, *supra* note 6.

[11] *See, e.g.*, Tene & Polonetsky, *supra* note 3, at 267 ("The entire 'app economy' is premised on individuals accessing their own data for novel uses, ranging from GPS programs and restaurant recommendations to self-tailored financial and health services.").

[12] BUREAU CONSUMER FINANCIAL PROTECTION, No. CFPB-2016-0048, REQUEST FOR INFORMATION REGARDING CONSUMER ACCESS TO FINANCIAL RECORDS, 10–12 (Nov. 14, 2016).

[13] Jerome, *supra* note 9, at 8 (stating that it is the responsibility of industry to set standards, provide transparency, and create interoperable formats to help consumers use their data).

[14] *See, e.g.*, Tene & Polonetsky, *supra* note 3, at 268 (stating that data portability is a "contentious concept," which may conflict with intellectual property and antitrust principles); *see also* Facebook v. Power Ventures, 844 F.3d 1058 (9th Cir. 2016) (holding that, although defendant social networking website had permission from Facebook users to access their information, defendant violated Computer Fraud and Abuse Act after Facebook sent cease and desist letter).

[15] Council Regulation 2016/679, 2016 O.J. (L 119) 1 [hereinafter *GDPR*].

[16] *Guidelines on the Right to Data Portability*, Article 29 Data Protection Working Party, 3 (Apr.

that the purpose of the regulation is to provide consumers with greater choice, control, and empowerment, and to "re-balance" the relationship between consumers and data controllers.[17] While many people are concerned about the GDPR's scope and implications for U.S. companies that must also contend with potentially conflicting U.S. laws, U.S. businesses which process or control the information of EU "data subjects" must demonstrate compliance.[18]

The challenge for the United States is to determine what role data portability will play in the evolution of the Internet, and how technology companies will balance their own interests with those of consumers to make use of the vast and growing stores of personal data and all of its still-untapped potential. This Article argues that rather than a blanket mandate of data portability, the requirement of data portability policies for businesses that collect personal data would create beneficial incentives, foster innovation, and balance the need for consumer control with businesses' legitimate rights and responsibilities.[19]

Part I examines the concept of data portability, including its origins and development, and seeks to answer the question, by exploring a variety of legal frameworks, of whether there is a right to data portability in the United States. Part II introduces the right to data portability under the EU's GDPR and addresses its benefits and drawbacks. Part III emphasizes the problems with the GDPR, arguing that as it is written, the regulation will not give consumers the intended portability benefits, and although many U.S. businesses are required to comply with the GDPR, the inadequacies in the regulation will cause businesses to circumvent the mandate. Finally, Part IV offers a solution by suggesting that a GDPR-style mandate is not the best way to solve the problems that data portability seeks to fix, and that the United States should require companies that handle personal data to maintain data portability policies, which—much like privacy policies—would operate within the existing privacy law framework.

This regulatory adjustment will benefit businesses and consumers alike. After all, walled gardens can be nice places where users readily "lend[] . . . their data to the sites and their eyeballs to advertisers," but only until the walls start to feel restrictive.[20] Too much restriction on data access and

---

5, 2017), https://ec.europa.eu/newsroom/document.cfm?doc_id=44099.

[17] *Id.* at 3–4.

[18] *See generally* Peter Swire & Yianni Lagos, *Why the Right to Data Portability Likely Reduces Consumer Welfare: Antitrust and Privacy Critique*, 72 MD. L. REV. 335 (2013).

[19] Elias Bizannes, *Why Every Site Should Have A Data Portability Policy*, TECHCRUNCH (June 23, 2010), https://techcrunch.com/2010/06/23/data-portability-policy.

[20] Holmes, *supra* note 6.

movement will eventually cause frustrated users to abandon a site or app. Opening communication through disclosure, however, will allow consumers to make informed choices about where to invest their time and data, and will allow businesses to cultivate trust with their users and have the opportunity to differentiate themselves by how they handle issues like privacy, transparency, and portability.[21]

I. THE CONCEPT OF DATA PORTABILITY IN THE UNITED STATES

Data portability is a relatively new idea compared with more traditional information governance concerns like privacy, security, and even access and transparency. The term "portability," meaning the ability to move personal data across different services without hindering its usability, does not really appear in legislation or case law until the 1996 passage of the Health Insurance Portability and Accountability Act.[22] And while there are sector-specific laws regulating the transfer of data in the consumer credit and financial industries,[23] U.S. law in general does not provide direct guidance on the issue of portability.[24] However, a close examination reveals how the law treats the subject and provides some clues about how to move forward.

A. Emergence of Data Portability

Most consumer protection measures related to data have been focused on privacy and security—with a more recent push for access and transparency—and narrowly protect only particular industries or specific types of information.[25] The Fair Credit Reporting Act (FCRA) was passed in 1970 to protect consumers from having inaccurate information used against them; the Electronic Communications Privacy Act (ECPA) of 1986 sought to protect citizens' private electronic communications from unauthorized government access; and in 1996, the Health Insurance Portability and Accountability Act (HIPAA) set standards to regulate the disclosure of

---

[21] *See* Bizannes, *supra* note 19 ("[A]s users become more knowledgeable about how sites might control their data without their knowledge, the websites that are transparent about data use will stand in the best stead with the public.").

[22] *See* Health Insurance Portability and Accountability Act ("HIPAA") of 1996, Pub. L. No. 104–191, 110 Stat. 1936 (1996) (codified as amended in scattered sections of 42 U.S.C. and 29 U.S.C.).

[23] *See* Fair Credit Reporting Act, 15 U.S.C. § 1681g–j (2019); Dodd-Frank Act, 12 U.S.C. § 5511(a)–(b) (2019).

[24] *See* Tene & Polonetsky, *supra* note 3, at 241 (arguing the need for a new legal framework because the existing one has been outpaced by developments in Big Data).

[25] *See, e.g.*, Jay P. Kesan et al., *Information Privacy and Data Control in Cloud Computing: Consumers, Privacy Preferences, and Market Efficiency*, 70 WASH. & LEE L. REV. 341, 395 (2013).

protected health information.[26] None of these laws—or any of the even more particularized subsequent regulations protecting children's online privacy or adults' video viewing history—provide for data portability, or even a strong right of access, for consumers.[27]

However, consumers have more recently won some rights to portability outside the context of personal data, including the right to port their phone numbers when they switch to a new wireless carrier, and the right to "unlock" phones that they own in order to switch network providers.[28] These examples have more to do with a right to take something specific (a ten-digit number, a physical device) and use it with a new service than a right to transfer "information," but they do suggest circumstances when utility for consumers outweighs the business desire to "lock in" customers.[29]

Part of the problem with the U.S. patchwork approach to privacy and data protection is that the lack of a general framework makes it difficult to determine what rights consumers should have and, for the purposes of this Article, whether or not portability is one of those rights.[30] Furthermore, questions arise as to what a right to portability is really about as stakeholders are concerned with a variety of issues like access to data, ownership rights over information, and fostering competition.[31]

For Europeans, the situation is clearer. While the United States theoretically views privacy as an aspect of individual freedom from intrusion, Europeans see privacy as an aspect of human dignity, affording the right to exercise autonomy over information about themselves.[32] Thus, when the

---

[26] Health Insurance Portability and Accountability Act ("HIPAA") of 1996; Electronic Commc'n Privacy Act of 1986, Pub. L. No. 99–508, 100 Stat. 1848 (codified at 18 U.S.C. §§ 2510–2522, 2701–2712); Fair Credit Reporting Act of 1970, Pub. L. No. 91–507, 84. Stat. 1114 (codified at 12 U.S.C §§ 1830–1831, 15 U.S.C. § 1681 a–x).

[27] *See* Children's Online Privacy Protection Act of 1998, 15 U.S.C. §§ 6501–6506 (2011) (preventing websites from collecting children's data without notice and parental consent); Video Privacy Protection Act of 1988 (codified at 18 U.S.C. § 2710 (2010)) (preventing the disclosure of personally identifiable rental records).

[28] *See* AT&T Corp. v. Iowa Util. Bd., 525 U.S. 366 (1999) (Thomas, J., Rehnquist J., Breyer J., concurring in part) ("The FCC has authority to regulate on the subject of number portability" under 47 U.S.C. § 251.); Colleen Bryan, *Number Portability for Consumers: Taking Your Wireless Number With You*, 16 LOY. CONSUMER L. REV. 267, 269 (2004).

[29] Bryan, *supra* note 28, at 275.

[30] *See* DANIEL J. SOLOVE, THE DIGITAL PERSON: TECHNOLOGY AND PRIVACY IN THE INFORMATION AGE 71 (2004) ("[T]he federal privacy statutes form a complicated patchwork of regulation with significant gaps and omissions.").

[31] *See id.* ("[T]he approach to making privacy policy in the United States is reactive rather than anticipatory, incremental rather than comprehensive, and fragmented rather than coherent.").

[32] *See, e.g.*, Kesan et al., *supra* note 25, at 418.

GDPR calls for a fundamental right to data portability, it draws on a long legal tradition of European consumers having an inherent right to control their personal information.[33] In the United States, however, the Federal Trade Commission (FTC) released a final report on its privacy framework that does not include the word "portability."[34] The report is intended to help Congress when considering future legislation regarding consumer protections as electronic data becomes an ever more important feature of American life.[35] The FTC urges businesses to adopt best practices like privacy by design, simplified choice, and greater transparency.[36] While the report does not include data portability as a recommended practice, it does recognize the importance of global interoperability between privacy regimes, and includes a core principle that companies should provide "reasonable access" to consumer data.[37] An examination of the types of access American consumers are legally entitled to will shed light on whether portability is a right under any pieces of the patchwork.

B. Laws Including an Access or Portability Right

While the United States has an abundance of laws relating to privacy, very few are concerned with consumer access to or control over personal information. Those laws that do address access and control issues primarily focus on health and financial information.[38] In pertinent part, HIPAA allows individuals to access their protected health information to "inspect and obtain a copy" of it, subject to a list of exceptions including if the information is being used for research in progress or if it was obtained confidentially from a non-healthcare provider, among other grounds for denial.[39] The implementing regulation states that the covered entity must act on a request for access within thirty days and should deliver the information in electronic form and in the format requested by the individual when possible.[40]

Similar to the right of access to health information, consumers have certain access rights when the information concerns personal finances. For

---

[33] *See, e.g.*, SOLOVE, *supra* note 30, at 106–07.

[34] FED. TRADE COMM'N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE (2012) [hereinafter PROTECTING CONSUMER PRIVACY].

[35] *Id.*

[36] *Id.* at 22, 35, 60.

[37] *Id.* at 9–10, 71.

[38] *See* Kesan et al., *supra* note 25, at 395–99.

[39] Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-91, 110 Stat. 1936 (codified as amended in scattered sections of 42 U.S.C. and 29 U.S.C.); 45 C.F.R. § 164.524 (2014).

[40] 45 C.F.R. § 164.524.

example, the Fair and Accurate Credit Transactions Act of 2003 (FACTA), which amended the Fair Credit Reporting Act (FCRA), requires that consumer reporting agencies "clearly and conspicuously disclosed to the consumer" all the information in consumer's file, the sources of the information, and each person who received a report on the consumer.[41] Further, consumers are entitled to one free copy of their report each year from each of the major reporting agencies, who must provide the report within fifteen days of the request.[42]

Another finance-related access right comes from the Dodd-Frank Act, which in 2010 empowered the Bureau of Consumer Financial Protection to enforce consumer financial law to ensure "access to markets" that are "fair, transparent, and competitive."[43] Specifically, the consumer right of access includes the right to receive, in a usable electronic form, information relating to a financial product or service, transaction, or account "including costs, charges and usage data."[44] Exceptions include confidential information, predictive algorithms, information collected to prevent or report crime, and information that cannot be retrieved in "the ordinary course of its business."[45] However, the future of Dodd-Frank is unclear after an Executive Order spurred legislators to propose alterations and the elimination of key provisions of the Act, which may further limit consumers' already slim access rights.[46]

Although many have argued that the access rights provided by laws like HIPAA, FCRA, and Dodd-Frank exist in part to promote portability, the legislative language lacks express provisions that would tip the scale from mere access to a right to transmit information from one service provider to another.[47] State laws are also lacking when it comes to explicitly providing citizens a right to transfer their data. The sweeping California Consumer Privacy Act, with its new rights of access and opt-out, uses the term "portable" to describe mere access, stopping short of true portability.[48] Similarly,

---

[41] Fair and Accurate Credit Transactions Act of 2003, Pub. L. No. 108-159, 117 Stat. 1952 (codified to 15 U.S.C. § 1681(g)–(j); 15 U.S.C. § 1681g(a)(1)–(3)).

[42] 15 U.S.C. § 1681j(a)(1)–(2).

[43] 12 U.S.C. § 5511(a).

[44] 12 U.S.C. § 5533(a).

[45] 12 U.S.C. § 5533(b)(4).

[46] Exec. Order No. 13772, 82 Fed. Reg. 9965 (Feb. 8, 2017).

[47] *See, e.g.*, Chris Hydak, *Data Portability Issues in US Foreshadow Challenges in EU*, LAW360.COM (Apr. 14, 2017, 1:50 PM), https://www.law360.com/articles/911474/data-portability-issues-in-us-foreshadow-challenges-in-eu (explaining how financial institutions and data aggregators can work together to allow sharing through application programming interfaces ("APIs")).

[48] CAL. CIV. CODE § 1798.100(d) (West 2020).

Massachusetts has the most detailed and specific law when it comes to protecting personal information, but the law—which requires companies to have a written information security program—seems to suggest that the secure information should stay protected where it is.[49]

Taken together, it appears that laws dealing with access rights focus on providing consumers with information that they need for critical decision-making, as in the areas of health and finances. Outside of these vital categories, it is difficult to find access rights for consumers, much less rights to portability.

C. Why Conditions Are Right for Data Portability in the United States

Seeing that consumers lack meaningful control over their personal data via the current legislative framework, the question is whether there is enough interest and enough room in the legal landscape to justify a general right to portability. Many have argued that baseline regulations are needed for data privacy and security, but a comprehensive federal law has not yet emerged.[50] The closest thing to a standard baseline is found in the body of FTC settlements, which reveal that the agency has become the "de facto data protection authority" in the United States, and its decisions, taken together, "have come to function as a de facto body of common law."[51] With its codification of norms and best practices, and its development of certain baseline protections, a look at the FTC's privacy jurisprudence may help to illuminate the direction that data protection is going, and whether portability can fit into its future.[52]

The FTC is empowered under section 5 of the FTC Act to prevent the use of "[u]nfair methods of competition in or affecting commerce and unfair or deceptive acts or practices in or affecting commerce."[53] In addition to publishing significant guidance on data privacy and security issues, the FTC investigates and files complaints for both "deceptive" and "unfair" violations.[54]

---

[49] 201 MASS. CODE REGS. § 17.00 (2009).

[50] *See* Kesan et al., *supra* note 25, at 464–65 (advocating that a "floor" be set by having baseline privacy regulations, including provisions for "data mobility," that cannot be contracted around); Ari Melber, Woodrow Hartzog, & Evan Selinger, *Fighting Facebook, a Campaign for a People's Terms of Service*, THE NATION (May 22, 2013) (arguing for a "people's terms of service" for social networking).

[51] Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583, 584 (2014) ("[T]he foundations exist to develop this 'common law' into a robust privacy regulatory regime, one that focuses on consumer expectations of privacy.").

[52] *See generally id.*

[53] 15 U.S.C. § 45(a)(2) (2012).

[54] *See generally* PROTECTING CONSUMER PRIVACY, *supra* note 34.

Early cases focused on misrepresentations in privacy policies related to data collection and sharing, while later cases have also been concerned with tracking and inadequate data security.[55] The resulting settlements order measures like comprehensive privacy and security programs, auditing and compliance reports, fines, and consumer notification.[56] While no settlements have yet specifically required data portability, the FTC has stepped in when consumers' expectations are defeated by unfair design or default settings, such as when an app or program shares data unexpectedly by default or comes with software that cannot be removed without making the program unusable.[57] This type of design or default unfairness may also describe the portability problem: consumers invest time in a particular social network, for example, sharing gigabytes of posts, photos, comments, and other personal data, only to have their expectation that the information is "theirs" thwarted by a policy or practice that locks in the data and forces the user to either stay or give up their investment.[58]

One significant problem with seeking to justify data portability in the context of FTC jurisprudence is that the agency also enforces antitrust law, which has been used to suggest that companies cannot be required to provide data portability or even compatibility with other companies' websites.[59] In 2007, LiveUniverse, the operator of social networking site vidilife, sued MySpace for preventing users from incorporating content from vidilife in their MySpace profiles.[60] The court held that MySpace had not engaged in exclusionary conduct, noting the general antitrust principle that there is no duty to deal with competitors, and adding that MySpace had no obligation to make its products compatible with rival products.[61]

Similarly, in 2016, the Ninth Circuit affirmed part of a lower court decision that said Facebook had not engaged in exclusionary conduct when it prevented social media aggregator Power Ventures from accessing Facebook

---

[55] See PROTECTING CONSUMER PRIVACY, *supra* note 34, at 6, 24; Alexander E. Reicher & Yan Fang, *FTC Privacy and Data Security Enforcement and Guidance Under Section 5*, 25 J. ANTITRUST, UCL & PRIVACY SEC. ST. B. CAL. 89 (2016).

[56] *See* Solove & Hartzog, *supra* note 51, at 620–24.

[57] *See* Frostwire LLC and Angel Leon, F.T.C. Matter 112-3041 (2011); Sony BMG Music Entertainment., In the Matter of, F.T.C. Matter 062-3019 (2007); *id.* at 642.

[58] *See* James Grimmelmann, *Saving Facebook*, 94 IOWA L. REV. 1137, 1192–94 (2009) (discussing the need to close the gap between what social media users expect and what they get).

[59] *See, e.g.*, Christopher S. Yoo, *When Antitrust Met Facebook*, 19 GEO. MASON L. REV. 1147, 1156 (2012).

[60] LiveUniverse, Inc. v. MySpace, Inc., No. CV 06-6994 AHM (RZx), 2007 WL 6865852, at *1 (C.D. Cal. June 4, 2007), *aff'd*, 304 F. App'x 554 (9th Cir. 2008).

[61] *Id.* at *11–14.

user accounts, even though Power Ventures had users' permission, and even though Facebook itself accessed its users' third party accounts like Gmail and Yahoo by doing precisely what it prevented Power Ventures from doing.[62] The lower court said that lack of interoperability with competing products is not an antitrust violation, and that "[i]f Facebook has the right to manage access to and use of its website, then there can be nothing anticompetitive about taking legal action to enforce that right."[63]

It appears that a right to portability may be in tension with U.S. antitrust law, in that a mandate would impose upon companies a form of "duty to deal."[64] While there are not any cases that impose a duty to make programs interoperable to facilitate portability, there are some decisions that appear to encourage interoperability.[65] Furthermore, in 2010, the Obama Administration launched "My Data" initiatives which sought to provide Americans with access to their personal data, focusing on interoperability, security, and access in the health, energy, finance, and education sectors.[66] And in 2016, the White House Office of Science and Technology Policy (OSTP) sought comments on "whether and how" to increase access to and portability of personal data.[67] Based on the comments received, the OSTP concluded that data portability is increasingly important and deserves more focus, and that many commenters believed that it "should be incentivized but not mandated."[68] The question remains: how can the U.S. attitude against a mandate of data portability be reconciled with the compliance requirements of the EU's GDPR?

---

[62] Facebook, Inc. v. Power Ventures, Inc., 844 F.3d 1058 (9th Cir. 2016); Facebook, Inc. v. Power Ventures, Inc., No. C 08-05780 JW, 2010 WL 3291750, at *1, *13–14 (N.D. Cal. July 20, 2010).

[63] Facebook, Inc. v. Power Ventures, Inc., No. C 08-05780 JW, 2010 WL 3291750, at *14 (N.D. Cal. July 20, 2010). The D.C. Circuit has also weighed in on interoperability by saying that "In order to violate the antitrust laws, the incompatible product must have an anticompetitive effect that outweighs any procompetitive justification for the design . . . . simply . . . developing a product that is incompatible with those of its rivals [is not sufficient]." United States v. Microsoft Corp., 253 F.3d 34, 75 (D.C. Cir. 2001) (internal citation omitted).

[64] *See, e.g.*, Verizon Communications, Inc. v. Trinko, LLP, 540 U.S. 398, 415 (2004) (quoting a law review article). The court went on to hold that "traditional antitrust principles [include] the proposition that there is no duty to aid competitors." *Id.* at 411.

[65] *See, e.g.*, Lotus Dev. Corp. v. Borland Int'l, Inc., 49 F.3d 807, 818–19 (1st Cir. 1995) (holding that Lotus' menu command hierarchy is not copyrightable, so Borland cannot be prevented from using it to make its own spreadsheet program, thus writing its own code to promote interoperability); Swire & Lagos, *supra* note 18, at 377.

[66] Tene & Polonetsky, *supra* note 3, at 264–65; Alexander Macgillivray, *Summary of Comments Received Regarding Data Portability*, THE WHITE HOUSE PRESIDENT BARACK OBAMA (Jan. 10, 2017 at 9:19 AM), https://obamawhitehouse.archives.gov/blog/2017/01/10/summary-comments-received-regarding-data-portability.

[67] Macgillivray, *supra* note 66.

[68] *Id.*

II. THE GENERAL DATA PROTECTION REGULATION (GDPR)

After the early European data protection laws in the 1970s, the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data was adopted in 1981, followed by the EU Data Protection Directive 95/46 in 1995.[69] The Directive provided the basis for the proposal of a General Data Protection Regulation in 2012, which after much debate and modification by the European Parliament and the Council of the European Union, replaced the Directive and took full effect in May 2018.[70] The European Commission proposing the GDPR sought to update the EU's data protection rules to account for technological advancement and to strengthen citizens' digital rights.[71] The GDPR states that protection with regard to processing personal data is a "fundamental right" and that globalization and technology have transformed our economic and social lives such that a "strong and more coherent data protection framework" is needed to increase the free flow of information and to give people control over their personal data.[72] While reaction to the GDPR from individuals, business leaders, and academics has been mixed,[73] it is clear that the law—with its provisions for extraterritoriality and noncompliance fines of up to twenty million Euro or four percent of annual global turnover—will have a tremendous impact in the years to come.[74] The rights of data subjects include privacy by design, breach notification, and the right to access, to be forgotten, and to data portability—the last of which is the particular subject of this Article.[75]

A. The New Right of Data Portability Under GDPR

The purpose of data portability, as envisioned by GDPR drafters, is to empower data subjects by helping them "move, copy or transmit personal data easily from one IT environment to another" while seeking to "'re-balance' the

---

[69] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Jan. 28, 1981, E.T.S. No. 108; Council Directive 95/46, 1995 O.J. (L 281) 31 (EC); Kesan et al., *supra* note 25, at 418 [hereinafter *Directive*].

[70] Barbara Van der Auwermeulen, *How to Attribute the Right to Data Portability in Europe: A Comparative Analysis of Legislations*, 33 COMPUT. L. & SEC. REV. 57, 72 (2017).

[71] Aysem Diker Vanberg & Mehmet Bilal Unver, *The Right to Data Portability in the GDPR and EU Competition Law: Odd Couple or Dynamic Duo?*, 8 EUR. J. L. & TECH. 1, 2 (2017).

[72] GDPR, *supra* note 15, at ¶¶ 1, 3, 6, 7.

[73] *See* Vanberg & Unver, *supra* note 71, at 2.

[74] GDPR applies to all companies that process the personal data of EU data subjects, regardless of the location of the company. *See generally* GDPR, *supra* note 15.

[75] *See id.*

relationship between data subjects and data controllers."[76] Specifically, the law provides an individual "the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format" and to have the data transmitted "without hindrance."[77]

The type of data that falls within the scope of the law is that which is personal to the individual and which the individual has *provided* to the controller.[78] The Article 29 Working Party, which represents EU privacy regulators, issued guidelines specifying the reach of the terms "personal data" and "provided."[79] The guidelines state that, while anonymous data are not within the scope of the law, pseudonymous data that can be connected back to the data subject are.[80] Additionally, the guidelines explain that portability covers data the individual knowingly provides as well as data generated through observation, such as "search history . . . location data" and "raw data such as the heartbeat tracked by a wearable device."[81] "Inferred" or "derived" data, however, are excluded from the scope because this type of data uses personal information to create something new like an algorithm, profile, or risk assessment by analyzing the observed behavior of data subjects.[82]

Not to be confused with interoperability—which concerns the technical compatibility of systems—data portability merely requires controllers to transmit data in a "structured, commonly used and machine-readable" format, and Recital 68 clearly states that, while interoperability is "encouraged," the law does not impose an obligation on controllers "to adopt or maintain processing systems which are technically compatible."[83] Furthermore, the right to data portability only applies when the data was provided pursuant to consent or contract and when the processing was "carried out by automated means."[84] These limitations mean that the benefits of GDPR portability are narrow in practice.

---

[76] *Guidelines on the Right to Data Portability*, *supra* note 16, at 4.

[77] GDPR, *supra* note 15, art. 20.

[78] *Id.*; *Guidelines on the Right to Data Portability*, *supra* note 16, at 9.

[79] *Guidelines on the Right to Data Portability*, *supra* note 16, at 9.

[80] *Id.*

[81] *Id.* at 10.

[82] *See id.* at 10–11.

[83] GDPR, *supra* note 15, ¶ 68; Barbara Engels, *Data Portability Among Online Platforms*, INTERNET POL'Y REV., at 3–4 (June 11, 2016).

[84] As a result, paper records are not covered, nor are data processed by certain financial institutions, concerning employees, or in business to business relationships. *See* GDPR, *supra* note 15, ¶ 68; *Guidelines on the Right to Data Portability*, *supra* note 16, at 8–9.

B. Benefits of a GDPR-style Right to Data Portability

The Article 29 Working Party heralds data portability as a way to empower individuals, facilitate information flow, and foster competition and innovation.[85] The GDPR envisions a future where data portability will be as intuitive and seamless as number portability for mobile phones is now.[86] There was initial resistance to mobile number portability, but today it is clear that the move provided consumers with greater choice, decreased "lock-in" and network effects, and increased market participation.[87]

Data portability will provide a great convenience to consumers and increase their choices in the digital economy.[88] By saving users from having to manually re-enter all of their information in order to join a new service, people will be more free to switch to the providers that best meet their individual needs.[89] As a result, new websites, apps, and online services are likely to emerge as the barrier to entry is lowered, providing even more innovative and tailored solutions for consumers.[90]

In addition to increased convenience and choice, the most often cited benefit of a right to data portability is decreased consumer "lock-in" caused by high switching costs and network effects.[91] Network effects are produced in systems where the value of a network is dependent on the number of users it reaches.[92] For platforms like social networks, online marketplaces, and search engines, more users in a given network generally means greater value.[93] These

---

[85] *See Guidelines on the Right to Data Portability*, *supra* note 16, at 3.

[86] *See* Kesan et al., *supra* note 25, at 469–70.

[87] *See id.* at 470.

[88] *See* Van der Auwermeulen, *supra* note 70, at 3.

[89] *See id.* In response to the controversy over facial recognition technology, Yana Welinder argues that users will not be able to demand respect for their privacy expectations until they are "truly free to switch" social networks by porting their personal data. *See* Yana Welinder, *A Face Tells More than a Thousand Posts: Developing Face Recognition Privacy in Social Networks*, 26 HARV. J. L. & TECH. 165, 168 (2012).

[90] *See* Engels, *supra* note 83, at 8 ("[T]he incentive to innovate for new entrants increases under data portability because it is easier to attract customers when the customers know that their data invested in the incumbent platform is not lost.").

[91] *See id.* at 5.

[92] *See id.*

[93] *See id.* at 11–13;

network effects result in higher switching costs, which causes many people to simply stay with a service—even when a better alternative exists—because moving is too costly.[94] Data portability would allow users to move more naturally in the market and avoid getting "locked-in" to a particular provider.[95]

Finally, it is likely that with increased freedom to switch, the relationship between online service providers and users will be improved, and the enhanced trust will encourage users to share more personal data, which in turn benefits service providers.[96] Furthermore, as portability and transparency are adopted, companies can distinguish themselves by offering greater transparency or more streamlined portability.[97]

C. Drawbacks of GDPR's Data Portability

While a general right to data portability offers many benefits, the provision of the GDPR that grants this right has an abundance of drawbacks. A major problem is that the right to portability interferes with a variety of other established rights in the United States and elsewhere.[98] Acknowledging the web of competing interests related to data acquisition and control, the GDPR states that the right to receive personal data from a controller "shall not adversely affect the rights and freedoms of others."[99] It may be that a data portability mandate cannot help but affect the rights of others. For example, porting certain information may infringe the intellectual property rights of companies or the privacy rights of other people in a contact list. The attempt to preserve these other rights may dilute the right to data portability such that it cannot effectively fix the problems for which it was created.[100]

> The quality of search results and the targeting of advertising using Google Search relies to a large extent on personal data—i.e. the user's previous searches and . . . data shared through other services . . . such as Google Photos . . . Gmail . . . Google Maps . . . and YouTube . . . .

Vanberg & Unver, *supra* note 71, at 10.

[94] *See* Engels, *supra* note 83, at 5 ("Without data portability . . . information . . . that the user has . . . "invested," such as messages, photos, reputation and search histories, remain with the original platform.").

[95] *See id.* at 7.

[96] *See* Van der Auwermeulen, *supra* note 70, at 59–60.

[97] *See id.* at 60.

[98] *See infra* Part III.

[99] GDPR, *supra* note 15, art. 15(4).

[100] *See infra* Part III.

First, data portability under the GDPR applies to limited categories of information and is subject to numerous conditions and exceptions.[101] One such limitation is that the right applies only to information provided by the data subject, thus excluding inferences—these inferences are the very types of information that people who are concerned with data rights want.[102] While it is convenient to be able to port pictures, contacts, posts, and messages, a serious concern underlying calls for portability is the fact that much of the personal information being gathered by companies is used to draw inferences to make consumer profiles that people fear may subject them to denial of service or prejudicial treatment.[103] It is this aversion to secret profiling and the use of algorithms and statistical analyses to categorize and theorize that fuels the desire for portability as an enhanced form of transparency, but if the GDPR does not allow consumers to exercise control over these inferences, the goal of "empowerment" will not be fully realized by merely allowing consumers to move their raw data around.[104]

Another limitation is that data controllers are subject to the portability requirement only when data was obtained by consent or contract, which is only one of six grounds for lawful processing of data.[105] Because consent is required only for processing special categories of personal information such as health, race, and religion, the vast majority of personal data collection and processing will be based on "legitimate interests" and therefore not subject to portability.[106] Furthermore, a "legitimate interest" is defined as a real, lawful,

---

[101] *See supra* text accompanying notes 81–84.

[102] *See* Lachlan Urquhart, Neelima Sailaja & Derek McAuley, *Realising the Right to Data Portability for the Domestic Internet of Things*, 22 PERS. & UBIQUITOUS COMPUTING 317 (2017).

[103] *See id.*

[104] *See id.* Online marketplaces like eBay are a less nefarious example of the limitations of raw data transfer. The reputation a seller builds through positive feedback has tremendous value, but if a seller is not permitted to take his reputation profile to another auction site, he will likely be deterred from switching. *See* Vanberg & Unver, *supra* note 71, at 3.

[105] *See* GDPR, *supra* note 15, at art. 6(1)(a)–(f), 20(1)(a).

[106] *See id.* art. 6(1)(a)–(b), (f) (processing pursuant to consent, contract, or legitimate interests), art. 9(1)–(2)(a) (special categories); *Guidelines on the Right to Data Portability*, *supra* note 16, at 8 (explaining, for example, that employee data is not subject to portability because power imbalances between employer and employee make freely given consent generally unobtainable). The irony of the Article 29 Working party's explanation is unavoidable: the right to portability is supposed to "re-balance" power between individuals and data controllers, but, recognizing that employees lack power relative to their employers such that they cannot freely consent to turning over their information in this context, the law allows employers to process the information without consent, claiming "legitimate interests" and preventing the employee from exercising the right to data portability.

and "clearly articulated" interest.[107] In other words, anything not illegal can be a legitimate interest. The Article 29 Working Party explains that legitimate interests are still subject to a balancing test against consumer rights, but it also says that marketers have a legitimate interest in selling products and that even "less compelling interests" can "override" consumer rights.[108]

Another limitation regarding the scope of the GDPR's right to data portability is that it does not solve the much-maligned "lock-in" problem because network effects persist, even with portability, in the absence of interoperability.[109] Portability would allow Facebook users, for example, to make a one-time transfer of their pictures, messages, and contacts to their Snapchat account; interoperability, on the other hand, would allow Facebook users to post directly to a friend's Snapchat or share a status update with them in real time.[110] Facebook already has an export feature that allows a user to download all of her information to take with her someplace else—the problem is that there really isn't anywhere else to go. The network effect persists because all of the user's friends are still on Facebook, so the utility of a competing network is drastically reduced such that switching—though made simple through the handy export feature—is pointless because the user will essentially be "locked out" of the Facebook garden while all of her friends are locked in.[111]

Relatedly, some scholars argue that a data portability mandate may actually decrease rather than encourage innovation as the risks associated with creating something new are exacerbated.[112] If first-movers are faced with the prospect of lower returns because of a portability mandate that forces them to give away valuable data, they may be discouraged from taking on development risk in the first place.[113] Furthermore, the GDPR not only applies to dominant players like Facebook and Apple, but also to small and medium sized businesses that process personal information.[114] If the GDPR is interested in preventing lock-in, it seems unnecessary to require an innovative start-up to meet the same compliance obligations as Google. Not only is a start-up unlikely to have any market power that would create a lock-in problem, but

---

[107] *Opinion 06/2014 on the Notion of Legitimate Interests of the Data Controller*, Article 29 Data Protection Working Party 25 (Apr. 9, 2014), https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf.

[108] *Id.* at 25–26.

[109] *See* Engels, *supra* note 83, at 4.

[110] *Id.*

[111] Welinder, *supra* note 89, at 220; Jerome, *supra* note 9, at 3.

[112] Swire & Lagos, *supra* note 18, at 358–60.

[113] *Id.*

[114] *Id.* at 352.

also a small company may find the cost of discerning its compliance obligations and writing necessary software a prohibitive barrier to entry.[115]

Finally, among the drawbacks of GDPR portability is its potentially adverse effects on privacy, security, and intellectual property rights. Professor James Grimmelmann argues that, because social networks have varying "legal, technical, [and] social constraints" that apply to information on each site, empowering people to port their information from one site to another will "create a privacy race to the bottom."[116] Grimmelmann asserts that regulations like mandatory data portability fail to recognize that privacy expectations are contextual and thus cautions that increasing portability may increase the risk of data breaches, which puts privacy at risk as well.[117] Additionally, a right to portability raises both privacy and intellectual property questions related to who has the right to control which data. For example, should one Facebook user have the right to port all of his pictures and contacts to another site even though that information also concerns other data subjects?[118] Or, in the context of online gaming, users often invest hundreds of hours creating individualized avatars which collect experiences and generate even more data.[119] Who should control this data, and should a user be permitted to port their avatar to another platform?[120] Finally, giving individuals the ability to obtain a lifetime's worth of data, and potentially store it less securely than before it was portable, vastly increases the quantity of data at risk of being accessed by a bad actor.[121] Further, requiring portability to be granted "without hindrance" means that "one moment of identity fraud can turn into a lifetime breach of personal data."[122] Despite these drawbacks, U.S. companies that collect or process Europeans' data are required to comply with the GDPR.[123] The next Part explores what this compliance will probably look like as far as data portability is concerned.

---

[115] *See id.*

[116] Grimmelmann, *supra* note 58, at 1194.

[117] *Id.* ("Personal information is only as secure as the least secure link in the chain through which such information passes.").

[118] *See* Van der Auwermeulen, *supra* note 70, at 4.

[119] *See id.* at 14.

[120] Swire & Lagos, *supra* note 18, at 348.

[121] *See id.* at 374.

[122] *See id.* at 380.

[123] *See infra* Part III.

III. THE PROBLEM OF COMPLIANCE WITH GDPR DATA PORTABILITY

While the United States may continue with the patchwork approach to data privacy and security regulation, the European Union has gone in the opposite direction with its comprehensive GDPR, which has extraterritorial reach.[124] U.S. businesses must be in compliance with the GDPR or risk administrative fines that could total four percent of worldwide turnover.[125] Specifically, data processors or controllers outside the EU must comply if they process EU data subjects' personal information to offer goods and services or to analyze or predict consumer preferences.[126] In other words, businesses with any kind of internet presence ought to be concerned about compliance. The problem for U.S. businesses is, because of a differing historical and theoretical basis for data privacy, existing U.S. laws are in tension with the EU data portability mandate.[127] Additionally, because there is no such requirement for the portability of U.S. citizens' data, companies may be further incentivized to circumvent compliance with mandatory portability.

A. Tension Between GDPR Portability and Established United States Law

The tension arising from differing conceptions of privacy in Europe and the United States implicate intellectual property, antitrust, and even laws seeking to prohibit hacking. First, mandatory data portability raises a variety of concerns regarding intellectual property law. While the GDPR restricts the right of *access* when it affects trade secrets and other IP rights, there is no such restriction as it relates to data *portability*.[128] The broad issue of "ownership" of data is thorny, and U.S. companies have valuable IP portfolios to protect.[129] Additionally, mandatory data portability appears to conflict with traditional antitrust principles and more recent precedent.[130] Scholars in this field have observed that EU competition law may be able to step in and serve as a complement to GDPR data portability, but U.S. antitrust is not such a

---

[124] *See* GDPR, *supra* note 15, rec. 23–24.

[125] *See id.* art. 83(5).

[126] *See id.* rec. 23, 24.

[127] *See supra* notes 32–33 and accompanying text.

[128] *See, e.g.*, Vanberg & Unver, *supra* note 71, at 5 (using the example of True Fit, an online service that uses personal data to align shoppers and clothing retailers, to illustrate the type of business model that would be made "obsolete" if required to share data).

[129] *See, e.g.*, Tene & Polonetsky, *supra* note 3, at 269 ("Personal information should be regarded as neither an exclusive asset of individuals … nor exclusively the property of businesses[;] [r]ather, personal information should be treated as a valuable joint resource and a basis for value creation and innovation.").

[130] *See supra* notes 60–63 and accompanying text.

complement.[131] "No duty to deal" is an established principle that was applied in *LiveUniverse v. MySpace* and *Facebook v. Power Ventures* seemingly to foreclose the possibility that a portability mandate could be required on the basis of exclusionary conduct.[132] If neither refusal to deal with competitors, nor incompatible website design, nor refusal to allow data portability are considered exclusionary conduct, then it is difficult to see how a data portability mandate could be justified for companies that have had their right to design and manage their sites as they see fit so adamantly affirmed.[133]

In addition to antitrust tension, mandatory data portability may also conflict with principles derived from the application of the Computer Fraud and Abuse Act (CFAA) in recent cases.[134] The CFAA was originally passed in 1984 as part of the Comprehensive Crime Control Act in order to target criminal hackers.[135] It has since been amended many times and includes both civil and criminal liability as well as a private right of action designed to deter both access "without authorization" and access that "exceeds" authorization to obtain information from a "protected computer."[136] Circuits are split on the interpretation of authorized access, and there has been much debate over the reach of the statute, as it can subject a person to liability simply for accessing a website in a way that violates the terms of service.[137] In an attempt to limit the ability of competing websites to use profiles and other user information, social media companies are bringing CFAA suits against others employing "screen scraping," a process by which information is copied from websites. In cases like these, plaintiffs are generally victorious as courts have held that private companies are allowed to restrict access to their websites, and after access has been revoked, further attempts at gaining information are violative

---

[131] *See generally* Van der Auwermeulen, *supra* note 70; Vanberg & Unver, *supra* note 71, at 9 ("[I]n the US, the courts have refused to give mandatory access to specific databases, particularly after the *Trinko* decision which limited the use of essential facilities doctrine to a great extent.").

[132] *See* Facebook, Inc. v. Power Ventures, Inc., 844 F.3d 1058 (9th Cir. 2016); LiveUniverse, Inc. v. MySpace, Inc., No. CV 06-6994 AHM (RZx), 2007 WL 6865852, at *1 (C.D. Cal. June 4, 2007), aff'd, 304 F. App'x 554 (9th Cir. 2008); *supra* notes 60–63 and accompanying text.

[133] *See, e.g.*, Facebook, Inc. v. Power Ventures, Inc., No. C 08-5780 JW, 2010 WL 3291750, at *14 (N.D. Cal. July 20, 2010) ("If Facebook has the right to manage access to and use of its website, then there can be nothing anticompetitive about taking legal action to enforce that right.").

[134] *See* 18 U.S.C. § 1030 (2016).

[135] Comprehensive Crime Control Act of 1984, Pub. L. No. 98–473, 98 Stat. 1976 (1984) (codified as amended at 18 U.S.C. §§ 1–6006 (1984).

[136] 18 U.S.C. § 1030(a)(2)(C), (g) (2016).

[137] Tiffany Curtiss, *Computer Fraud and Abuse Act Enforcement: Cruel, Unusual, and Due for Reform*, 91 WASH. L. REV. 1813, 1818–24 (2016).

of the CFAA.[138] With strong precedent in favor of companies' ability to restrict data portability, a GDPR-style mandate which forces companies to transfer data to competitors "without hindrance" seems unlikely in the United States. Consequently, because GDPR compliance is mandatory for companies that process EU citizens' data, U.S. businesses are likely to attempt to circumvent the portability provision, or at the very least, segregate EU citizens' data from that of U.S. citizens.

B. Circumventing Portability while Maintaining GDPR Compliance

One way that businesses can achieve compliance with GDPR while avoiding an obligation to make portability available to users is to justify their data collection as serving a "legitimate interest," which, unlike collection via consent or contract, does not trigger portability.[139] The Article 29 Working Party makes clear that this sixth option for legal processing of data should be seen as neither a "last resort" nor a "preferred option."[140] Controllers, however, are likely to make this the preferred option to justify their data processing activities because the controller itself conducts the "balancing test" to assure that its interests outweigh those of the data subject and because any trivial interest can be deemed "legitimate."[141]

One obstacle to controllers relying on legitimate interests is that there are special categories of data for which express consent of the data subject is required, which triggers the portability obligation.[142] However, because the vast majority of information collected is not in these special categories, businesses are incentivized to employ a two-stage approach to data collection, in which data is collected on the basis of legitimate interests, with additional sensitive data requested via consent.[143] Accordingly, only the data that was collected via consent would be subject to portability, and these special, limited categories of data are not going to be useful for consumers to port.[144]

---

[138] *See* Facebook, Inc. v. Power Ventures, Inc., 844 F.3d (cert. denied 2017); Craigslist Inc. v. 3Taps Inc., 964 F. Supp. 2d 1178, 1187 (N.D. Cal. 2013) ("[T]he statute protects all information on any protected computer accessed 'without authorization,' and nothing in that language prohibits a computer owner from selectively revoking authorization to access its website.").

[139] *See supra* notes 105–08 and accompanying text.

[140] *See Opinion 06/2014 on the Notion of Legitimate Interests of the Data Controller*, *supra* note 107, at 9.

[141] *Id.* at 43.

[142] *See supra* note 106 and accompanying text.

[143] *See* Robert Madge, *GDPR: Data Portability is a False Promise*, MEDIUM (2017), https://medium.com/mydata/gdpr-data-portability-is-a-false-promise-af460d35a629.

[144] *See id.*

Finally, even though the GDPR mandates portability in certain instances, the mandate only applies to EU citizens' data, and U.S. businesses are free to treat the data of U.S. citizens differently. It may prove to be more cost-effective to apply the heightened protections of the GDPR only where required, resulting in segregation of U.S. citizens' data, which will not be afforded any additional protections as a result of the GDPR.[145] However, because many in the United States recognize the potential benefits of greater portability,[146] the ideal solution would incentivize companies to implement portability without a blanket mandate as in the GDPR.

C. Incentivize Rather than Mandate Portability

While a portability mandate runs counter to U.S. precedent in areas like antitrust and CFAA decisions,[147] it is clear that data portability has many potential benefits for consumers and businesses alike, and the United States is not altogether opposed to the idea.[148] In the fall of 2016, the White House Office of Science and Technology Policy (OSTP) requested comments "on whether and how to increase your ability to get and use your data."[149] The overall consensus from industry, advocacy groups, and individuals was "portability should be incentivized but not mandated."[150] Further support for this position can be found in the response from the Center for Democracy and Technology (CDT), which advocates for empowering individuals with the increased control over their data that portability provides.[151] The CDT makes recommendations about how to increase portability but cautions that business environments are extremely varied, and "a universe of interoperable standards" which form "a marketplace [of] competing technical approaches" is preferable to a less practical, one-size fits approach.[152]

The CDT's view is reinforced by the FTC in its response to a request for information from the National Telecommunications and Information

---

[145] *See* Swire & Lagos, *supra* note 18, at 354–56 (discussing the cost and difficulty of implementing data portability, especially for small and medium sized businesses).

[146] *See infra* Part IV.

[147] *See supra* Part III.A.

[148] *See* Macgillivray, *supra* note 66, at 1.

[149] *Id.*

[150] *Id.* at 2.

[151] *See* Jerome, *supra* note 9, at 1–4.

[152] *Id.* at 9.

Administration (NTIA) about the Internet of Things (IoT).[153] The FTC emphasizes that interoperability standards benefit competition, innovation, and product quality while enhancing consumer data portability and choice.[154] It explains the benefits of a "collaborative standard-setting process" for interoperability but warns that "widespread adoption" of one standard may reduce competition.[155]

Incentivizing rather than mandating data portability makes sense from a competition standpoint as well as a technological one, and it also addresses the limitations of GDPR portability, which almost guarantee that ordinary consumers will not receive the benefits intended by the mandate.[156] As noted above, an important gap in the GDPR mandate is that it requires portability without requiring interoperability, so it may be that encouraging industry to take meaningful steps toward interoperability will have greater long-term pay-offs than forcing companies to make portability work now.[157] Further, while one-time transfers offer consumers meaningful benefits, opening up systems through interoperability will unlock innovation for decades to come.

Finally, rather than creating a race to the bottom as companies generally seek to do just enough to meet their compliance obligations, incentivizing portability leading to interoperability recognizes the complex technical landscape and makes competition the impetus for change as companies respond to users' demands for greater transparency and control.[158] For example, the GDPR clearly does not require companies to disclose their decision criteria, or how they draw inferences from the information in their enormous databases.[159] But this is information that people want in order to avoid "[i]naccurate, manipulative, or discriminatory conclusions [that] may be

---

[153] FTC Comments to NTIA's RFI In re The Benefits, Challenges, and Potential Roles for the Government in Fostering the Advancement of the Internet of Things, No. 160331306-6306-01 (June 2, 2016), https://www.ftc.gov/system/files/documents/advocacy_documents/comment-staff-bureau-consumer-protection-office-policy-planning-national-telecommunications/160603ntiacomment.pdf.

[154] *Id.* at 15.

[155] *Id.* at 15–16 ("[A] marketplace with competing technical approaches would induce firms to innovate to develop interoperability solutions with privacy and data security attributes desired by consumers.").

[156] *Supra* notes 81–84; *see supra* notes 102–11 and accompanying text.

[157] *See supra* note 83 and accompanying text; *see also* Welinder, *supra* note 89, at 235–36 ("[T]he legislature could mandate data portability and interoperability standards to make it easier for users to switch between social networks. This type of 'indirect' legal regulation can sometime be more effective than 'direct' legislation.").

[158] *See, e.g.*, Welinder, *supra* note 89, at 220–21 ("Given that interoperability of social networks is a highly technical matter, it should not be micromanaged by the state.").

[159] *See supra* notes 102–04 and accompanying text.

drawn from perfectly innocuous, accurate data." [160] Under the GDPR, individuals are unlikely to gain access to decision criteria through the portability mandate. However, if companies are required not to automatically implement portability but merely to disclose the extent to which they make it available, consumers can make informed choices about with whom they invest their data. Consequently, companies will likely be pushed to offer the transparency and control features consumers want most.[161] This disclosure could take the form of a data portability policy.

IV. DATA PORTABILITY POLICIES AS A WAY FORWARD FOR U.S. COMPANIES AND CONSUMERS

Due to its limited scope, compliance with the data portability provision of the GDPR will not require U.S. companies to drastically change. However, it is clear that the United States has an interest in encouraging data portability. While a mandate is not a workable solution, requiring companies to write and maintain data portability policies would put the focus on user expectations while encouraging innovation and striking the right balance between data control in the hands of individuals and in the databases of companies.

A. The Requirement of Data Portability Policies

A data portability policy is a plain-language document that tells users what they can bring in and take out when they are using a particular site or service. In contrast to the traditional privacy policy, which informs users what a company can do with their information, the data portability policy tells *users* what *they* can do with it.[162] A portability policy should be short, clear, and simply written so that users can easily gauge how much of their pictures, posts, messages, settings, lists, and other objects they will be able to freely move and how they will be able to do it.[163] The policy should explain whether users will be given the ability to download their information, port it to another service provider, delete it, allow an aggregator to access it, or use it collaboratively

---

[160] *See* Tene & Polonetsky, *supra* note 3, at 270–71.

[161] For a discussion of transparency concerning criteria, *see id.* at 270–72.

[162] Bizannes, *supra* note 19.

[163] Privacy policies themselves need a lot of work in the areas of clarity and brevity. *See* Melber et al., *supra* note 50 ("Facebook … offers a contract almost as long as the US Constitution.").

with information hosted elsewhere.[164] A "bare-bones" example created by a group called the DataPortability Project illustrates how such a policy might be structured.[165]

A basic framework with certain required categories would be sufficient to ensure that users are informed of the consequences of investing their data with a given provider. It would be up to the individual service provider to decide how much extra information to disclose or whether to explain the rationale for some of their data control choices. As users become accustomed to seeing portability policies, their choices will start to affect what kinds of options companies provide—ultimately leading to the most efficient amount of portability that reflects the desires and expectations of consumers.[166] Critics have long recognized that current practices governing individuals' online relationships to companies—consisting of one-sided, non-negotiable terms-of-service contracts—offer little if any protection for consumer interests and reflect an increasingly imbalanced power dynamic as more and more of our business and personal lives are conducted online.[167] Data portability policies simply require companies to communicate what they are doing; it is up to consumers to use their collective will to push the industry toward a fairer and more useful balance of data control rights.[168]

To avoid some of the pitfalls of traditional privacy policies on the Web,[169] a focus on clarity and succinctness is essential. Of course, the ideal context for portability policies would be within a federal baseline privacy framework like the FTC has perennially proposed.[170] Short of such a framework, companies can still look to the FTC's guidance on dotcom disclosure for the criteria and requirements of "clear and conspicuous" disclosures.[171] FTC actions and guidance also provide insight into how data portability policies could be required and enforced.

---

[164] Bizannes, *supra* note 19.

[165] *Id.*

[166] *See* Melber et al., *supra* note 50 ("Given enough collective will, start-ups seeking a competitive advantage will offer consumer-friendly terms and established companies will compete over allegiance to user rights. To move the market in this direction, we need a common language that communicates clear priorities.").

[167] *See id.* ("People's Terms of Service Agreement—a common reference point and stamp of approval, like a Fair Trade label for the web, to govern the next photo-sharing app or responsible social network.").

[168] *Id.* ("Sooner or later . . . enough people will wake up to the fact that our online lives are governed by form contracts . . . [a]nd . . . that group . . . could grow into something that Silicon Valley knows how to serve—a market.").

[169] *See infra* notes 186–92.

[170] *See, e.g.*, *Protecting Consumer Privacy in an Era of Rapid Change*, *supra* note 34, at iv.

[171]

B. The Authority to Require and Enforce Data Portability Policies

The most straightforward way to require data portability policies would be through congressional action; however, the U.S. Congress does not have a great track record when it comes to comprehensive data privacy and security legislation.[172] While bills like the BROWSER Act—one of several such comprehensive proposals contemplated recently—could mandate a baseline that includes requirements for privacy and data portability policies, history would suggest that the patchwork approach to legislation will persist.[173] But even without congressional action, the FTC likely has the authority to publish and enforce regulations in this area.[174]

Section 18 of the FTC Act authorizes the Commission to prescribe "rules which define with specificity acts or practices which are unfair or deceptive."[175] The FTC has written rules requiring disclosures in many instances already, and data portability policies would not be a divergence from these types of disclosures. [176] Furthermore, the Commission has a detailed history of enforcing against insufficient disclosures, and its interpretations of deception and unfairness are evolving to suit the changing technological climate.[177]

> In evaluating whether a disclosure is likely to be clear and conspicuous, advertisers should consider its placement . . . and its proximity to the relevant claim . . . . the prominence of the disclosure; whether it is unavoidable; whether other parts of the ad distract attention from the disclosure; whether the disclosure needs to be repeated . . . whether visual disclosures appear for a sufficient duration; and whether the language of the disclosure is understandable to the intended audience.

.com Disclosures: How to Make Effective Disclosures in Digital Advertising, F.T.C. at i–ii, (Mar. 2013).

[172] *See* Kesan, Hayes & Bashir, *supra* note 25, at 395–98.

[173] *See, e.g.*, BROWSER Act of 2017, H.R. 2520, 115th Cong. (2017) (empowering the FTC to enforce requirement of conspicuous privacy policies and user right of approval for disclosure and access).

[174] 15 U.S.C. § 57a (2006).

[175] 15 U.S.C. § 57a(a)(1)(B) (2006).

[176] *See, e.g.*, Influencers Rule, 16 C.F.R. 255.5 § (2016) (requiring advertisers to disclose connections with endorsers affecting credibility and whether they are receiving compensation); Franchise Rule, 16 C.F.R. § 436.2 (2009) (declaring failure of franchisors to furnish particular disclosures to franchisees an unfair or deceptive act or practice); Funeral Rule, 16 C.F.R. § 453.2 (2008) (declaring failure to furnish disclosures of costs of enumerated funeral goods and services an unfair or deceptive act or practice).

[177] F.T.C., 1980 POLICY STATEMENT ON UNFAIRNESS (1984) (describing unfair practices as those which cause or are likely to cause substantial injuries that consumers could not reasonably avoid). F.T.C., FTC POLICY STATEMENT ON DECEPTION (1983) (describing deceptive practices as those

In fact, although Congress has not yet passed any comprehensive legislation requiring privacy policies, the FTC has required comprehensive privacy programs as part of consent orders in a variety of settlements.[178] Professors Solove and Hartzog argue that FTC jurisprudence functions as the de facto common law of privacy and that after nearly twenty years of enforcement, the Commission has laid the foundation for a regulatory regime that goes beyond just privacy policies.[179] In actions brought for unfair or deceptive practices, the FTC has issued penalties up to $5 billion,[180] and has exercised wide-ranging discretion to order not only financial penalties, but also prohibitions on activities, requirements for reporting and auditing, deletion of data, modification of privacy policies, and the establishment of comprehensive privacy programs.[181]

With this authority already in place, it would not be an unreasonable stretch for the FTC to promulgate a rule requiring portability policies (either as part of, or in addition to, privacy policies) and declare that the failure to maintain such a policy is an unfair or deceptive act or practice.[182] In fact, even without such a rule, the FTC has already brought actions against companies when the design or function of a product so undermines consumer expectations as to render it unfair.[183] For example, in a settlement with peer-to-peer file sharing software developer FrostWire, the FTC required the company to change its default settings and provide clear and prominent disclosures about sharing after determining that FrostWire's program default was likely to cause consumers to unwittingly disclose their files.[184] This case, and others like it, extends unfairness and deception to include product design that defies user expectations.[185] Such reasoning could certainly apply to websites or programs

---

which are likely to mislead consumers and are material to their decision to use the product or service).

[178] *See, e.g.*, Google, Inc., FTC File No. 102-3136 (2011) (settling deceptive practices action against Google's Buzz Social Network and constituting the first time that the FTC required a comprehensive privacy program as part of a consent order).

[179] Solove & Hartzog, *supra* note 51, at 589.

[180] *See* U.S. v. Facebook, Inc., Case No. 19-CV-2184 (D. D.C. July 24, 2019).

[181] *Id.* at 614–19.

[182] *See* 15 U.S.C. § 57a(a)(1)(B) (2016); FTC Disclosure of Material Connections, 16 C.F.R. § 255.5 (2012) (requiring advertisers to disclose connections with endorsers affecting credibility and whether they are receiving compensation); FTC Obligation to Furnish Documents Rule, 16 C.F.R. § 436.2 (2009) (declaring failure of franchisors to furnish particular disclosures to franchisees an unfair or deceptive act or practice); FTC Price Disclosures Rule, 16 C.F.R. § 453.2 (2008) (declaring failure to furnish disclosures of costs of enumerated funeral goods and services an unfair or deceptive act or practice).

[183] *See* Solove & Hartzog, *supra* note 51, at 667.

[184] Fed. Trade Comm'n v. Frostwire LLC, No. 11-23643-CV-GRAHAM (S.D. Fla. Oct. 12, 2011).

[185] *See* Grimmelmann, *supra* note 58, at 1142 (arguing that "[c]hanges that pull the rug out from under users' expectations" should automatically be considered unfair practices); *see also* Solove &

that "lock in" user information in a way that consumers would not expect and would not have agreed to had they known that their data investment would be trapped and unusable in other contexts and applications.[186]

C. The Benefits and Utility of Requiring Data Portability Policies

Despite the fact that the FTC likely has the authority to require data portability policies, some would argue that there is no need for them in the first place because most people do not read privacy policies, so portability policies are unlikely to make a difference.[187] This type of thinking is too narrow. While it is true that very few people take the time to read privacy policies (and that reading all of the policies for the sites a person uses would take 76 full work days out of the year),[188] it does not follow that people simply do not care about privacy. Instead, this consumer inattention illustrates the ineffectiveness of the current scheme and the lack of tools and incentives for individuals to align their expectations and values with their daily practices online.[189] What the privacy policy problem really reveals is that consumers "cannot afford to indulge in transparency and access for their own sake without any tangible benefit."[190]

Data portability policies present an opportunity for individuals to engage with their data rights in ways that privacy policies have not been able to, because portability allows consumers to *use* their data for their own benefit,

---

Hartzog, *supra* note 51, at 666 (calling the FTC's shift from enforcing privacy promises to consumer expectations "profound," and speculating that in the future it may extend its prohibition on exploiting consumer ignorance to affirmatively require companies to combat consumers' false assumptions).

[186] *See* Reicher & Fang, *supra* note 55, for a comprehensive overview of FTC action in both the privacy and security arenas.

[187] *See, e.g.*, Grimmelmann, *supra* note 58, at 1181–84.

[188] Alexis C. Madrigal, *Reading the Privacy Policies You Encounter in a Year Would Take 76 Work Days*, THE ATLANTIC (Mar. 1, 2012), https://www.theatlantic.com/technology/archive/2012/03/reading-the-privacy-policies-you-encounter-in-a-year-would-take-76-work-days/253851/. In 2008, even before the ubiquity of social media, researchers at Carnegie Mellon determined that the nationwide opportunity cost of reading the privacy policies for all the websites Americans visit is $781 billion. Aleecia M. McDonald & Lorrie Faith Cranor, *The Cost of Reading Privacy Policies*, 4 I/S: J. L. & POL'Y FOR INFO. SOC'Y 543, 564 (2008).

[189] *See* Solove & Hartzog, *supra* note 51, at 667 (explaining that if the FTC took social science research into account—which shows that people are influenced by their false assumptions about companies' privacy practices and by the framing of choices—"[e]xisting forms of notice might not be deemed sufficient because the empirical evidence shows that consumers are not really being notified.").

[190] *See* Tene & Polonetsky, *supra* note 3, at 268.

thereby transitioning from mere passive data subjects to active users and re-users of data.[191] It is clear from the success of the "app economy" that individuals desire to use their own data in new ways and that companies creating apps allowing these novel uses are responding to this very growing consumer demand.[192] Not just access for its own sake, but *useful* access will engage individuals seeking to use their data to draw better conclusions about health decisions, choosing the right car or vacation destination, or optimizing their smart home devices.[193]

The financial industry has already taken steps to facilitate data portability with good results for consumers, who use aggregators to analyze their finances, compare services, and streamline the process of checking accounts at different institutions.[194] Less regulated industries need the portability policy requirement as a baseline so that users have a tool to assess how much utility competing service providers will give them. Absent such a baseline, innovative alternatives to the closed-world model have sprung up in the social media context, but these decentralized sites alone will not solve the lock-in and network effects problem if the big players continue to remain locked and closed.[195] Additionally, these major players have recently signed on to the Data Transfer Project, an open source initiative working to create a connection framework that any provider can use to enable portability between platforms.[196] The fact that Apple, Google, Facebook, Microsoft, and Twitter are supporting portability is evidence of its desirability and potential. However, such initiatives can work to fend off regulation while a portability policy

---

[191] *See id.*, at 269–70 ("Where individuals can access data in a manner that is engaging, useful, or valuable, they will give rise to natural checks on inappropriate behavior, thus serving as a useful compliance mechanism for privacy law.").

[192] *See id.*, at 267 ("[Apps] enable individuals to make innovative use of their list of friends . . . . address books, Wi-Fi router locations, and many other sources of data. A recent study found that the app economy has created 466,000 jobs in the United States since 2007.").

[193]

> [O]ne can envision a future where . . . . an individual's health records could be easily shared with different doctors and health providers [and] [t]emperature and lighting preferences and other environmental controls could be moved from the smart home to the connected car. Insights from one grocery store's reward program could be transferred and used at an entirely different supermarket.

See Jerome, *supra* note 9, at 2.

[194] *See* Hydak, *supra* note 47, at 3–4 (describing the move from screen-scraping to Application Programming Interfaces ("API") and agreements between financial institutions and aggregators which outline what data can be ported and how privacy and security will be addressed).

[195] *See* Berners-Lee, *supra* note 1, at 82; Welinder, *supra* note 89, at 218–19. For descriptions of several decentralized social media networks such as GnuSocial, Diaspora, and Musubi, *see* Engels, *supra* note 83, at 4; Jerome, *supra* note 9, at 3; Welinder, *supra* note 89, at 220 (and accompanying text on network effects).

[196] DATA TRANSFER PROJECT, https://datatransferproject.dev (last visited Aug. 29, 2019).

requirement will ensure that companies large and small are using the same standards to fairly and accurately represent to consumers what they are offering. This standardization can potentially lead to a future where tech companies compete on the basis of the innovative services they offer rather than perpetually reaping the benefits of being the first to capture our data. Some consumer advocates envision a future where individuals exercise complete control over their digital information by keeping it in data "vaults" or other personal information management systems ("PIMS") and granting third parties access to it on their own terms.[197] While this future provides an interesting counterpoint to the current state of affsairs, the ownership conception of data presents a whole new set of challenges.[198] Rather than advocating for consumer data ownership, this Article suggests that the ultimate social good here is interoperability, and one way to increase interoperability is to require companies that collect data clearly communicate their portability options so that consumers can make choices that reflect their values and expectations.[199]

V. CONCLUSION

Tim Berners-Lee famously said that the Web exists to "serve humanity,"[200] and the GDPR states that data processing should likewise "serve mankind."[201] But at least when it comes to the data portability provision of the GDPR, ordinary people are unlikely to gain much beneficial use from the data they invest in social networks, online marketplaces, search engines, and

---

[197] *See* Tene & Polonetsky, *supra* note 3, at 266; Urquhart, Sailaja, & McAuley, *supra* note 102, at 9–10.

[198] *See, e.g.*, Tene & Polonetsky, *supra* note 3, at 269 ("The property metaphor fails to capture the psychological and sociological nuance of the right to privacy.").

[199] For a comprehensive treatment of the concept of interoperability *see* JOHN PALFREY & URS GASSER, INTEROP: THE PROMISE AND PERILS OF HIGHLY INTERCONNECTED SYSTEMS (2012) (arguing that there is no standard definition of interoperability, but at the core, "the ability to transfer and render useful data . . . . across systems, applications, or components" is good for humanity, and, although greater interconnectedness comes with trade-offs and people disagree about the optimal level of interoperability, over their years of research, Palfrey and Gasser "never found a single person who thinks that interop is anything other than a good thing in general. That is the starting point."). *Id.* at 4–5.

[200] Berners-Lee, *supra* note 1, at 85.

[201] GDPR, *supra* note 15, ¶ 4.

the like because of the limited scope of the portability requirement.[202] While there is no general portability right in the United States, the benefits of freer information flows are numerous, including increasing transparency and choice, decreasing lock-in, and encouraging innovation and competition.[203] Consequently, companies that collect data should be required to write and maintain portability policies to allow users to make informed decisions about where to invest their time and data.[204]

Encouraging data portability allows users to find gates in the walled gardens of dominant service providers seeking to maintain control over the information in their proprietary domains.

If there are no such gates, users will be informed that they are entering at their own peril rather than having their expectations thwarted after they're already trapped inside. We do not have to settle for a fragmented Web of closed worlds that limit interconnectedness. We control the growth of the Web by making legislative decisions that affect design, software, and architecture which determine how we will connect in the future. "'[W]alled gardens,' no matter how pleasing, can never compete in diversity, richness and innovation with the mad, throbbing Web market outside their gates. If a walled garden has too tight a hold on a market, however, it can delay that outside growth."[205] Required data portability policies are a modest and realistic step toward encouraging growth that serves humankind.

---

[202] *See supra* Part II.C.

[203] *See supra* Part III.C.

[204] *See supra* Part IV.

[205] Berners-Lee, *supra* note 1, at 83.