



SCHOOL OF LAW
TEXAS A&M UNIVERSITY

Texas A&M University School of Law
Texas A&M Law Scholarship

Faculty Scholarship

3-2020

Data and the Social Obligation Norm of Property: An Essay in Honor of Professor Gregory S. Alexander

Christopher K. Odinet

Follow this and additional works at: <https://scholarship.law.tamu.edu/facscholar>



Part of the [Legal History Commons](#), [Privacy Law Commons](#), [Property Law and Real Estate Commons](#), and the [Science and Technology Law Commons](#)

AN ESSAY IN HONOR OF PROFESSOR
GREGORY S. ALEXANDER

DATA AND THE SOCIAL OBLIGATION
NORM OF PROPERTY

*Christopher K. Odinet**

In the age of the Cambridge Analytica/Facebook scandal and sundry other data breaches at Under Armour, Target, and Best Buy, the issue of security and privacy in consumer data has become increasingly important. For much of the modern era, the development of technology has gone relatively unchecked, with the United States having ceded much of the policymaking terrain to Silicon Valley. This has resulted in the unbridled creation of vast amounts of consumer data. Users who engage with tech platforms generate bits and bytes about themselves based on their activities, preferences, and habits. This information—this “data”—is then harnessed by tech companies for a variety of purposes ranging from advertising to market analytics, and more, leaving privacy as an afterthought.

In terms of defining the legal rights around personal data, scholars have argued that the United States abandoned a property law view long ago in preference to a tort-based approach. This has resulted in data protection regimes being focused on liability rules, yielding compensation remedies when electronic information has been used in an unauthorized or impermissible way. Although various efforts have been made to introduce property rules to data in the United States, they have produced varying results or have failed outright.

*But during the 2018 term, the U.S. Supreme Court decided two important cases that, albeit indirectly, edged toward a more robust conception of data as property—*South Dakota v. Wayfair* and *Carpenter v. United States*. In both cases, however, the Court struggled with how to articulate this concept. Sometimes the Court appeared to cling tightly to*

* Professor of Law, The University of Iowa College of Law. Thanks to Joseph William Singer, Donald J. Kochan, Timothy Mulvaney, Shelly Ross Saxer, Natalie Banta, the participants of the American Association of Law Schools (AALS) Property Law Section Works-in-Progress Program. This Essay is part of a series of works dedicated to the many accomplishments of Professor Gregory S. Alexander and commemorates his retirement from the Cornell Law School faculty. As always, I thank the University of Oklahoma College of Law’s library staff for their skillful research support. All errors and views are mine alone.

bedrock pillars of property law, such as physicality and alienability. At other times, however, the justices seemed to be treading new ground (or rediscovering old roads), such as with the disaggregation of digital rights and the idea of involuntary electronic bailments. Building upon the leanings of these recent cases, this Essay—in celebration of Professor Gregory Alexander—offers up progressive property theory as a lens through which courts and legislatures can build rules and standards for data as property. To do this, I draw upon Professor Alexander’s work in the property theory literature and its ideals of social obligations, dignity, and owner responsibility in property rights.

INTRODUCTION	644
I. DATA AND PROPERTY LAW DISRUPTION	650
A. <i>In Tort Law</i>	651
B. <i>In Cryptocurrencies</i>	653
C. <i>In Inheritance</i>	654
D. <i>In Secured Lending</i>	655
II. DATA PROPERTY AT THE SUPREME COURT	658
A. <i>A Case About Taxes (South Dakota v. Wayfair)</i>	658
B. <i>A Case About Cell Phones (Carpenter v. United States)</i>	660
III. A PROGRESSIVE PROPERTY APPROACH TO DATA	664
A. <i>Property and Social Obligation Norms</i>	666
B. <i>Data and a Community of Rights</i>	668
C. <i>Data as Governance Property</i>	670
CONCLUSION	672

INTRODUCTION

“What’s clear is this: Those who own the data win.”¹

We all want to protect our data privacy. We are angered when we see data breaches in the news or when we learn of companies we thought could be trusted use our data in a way that makes us feel betrayed.²

¹ KPMG, *YOUR CONNECTED CAR IS TALKING. WHO’S LISTENING?* 10 (2016), <https://assets.kpmg.com/content/dam/kpmg/br/pdf/2016/11/your-connected-car-is-talking.pdf>.

² AnnaMaria Andriotis, Michael Rapoport & Robert McMillan, *‘We’ve Been Breached’: Inside the Equifax Hack*, WALL ST. J. (Sept. 18, 2017, 8:04 AM), <https://www.wsj.com/articles/weve-been-breached-inside-the-equifax-hack-1505693318>; Louise Talbot, *‘This Is Huge’: Massive Data Breach at Marriott Hotel Chain Affects 500 Million Guests*, NEW DAILY (Dec. 1, 2018, 10:31 AM), <https://thenewdaily.com.au/news/world/2018/12/01/marriott-database-hacked/>; Ed Targett, *5 Things We Know About the German Hack, from Porn to Mirrors*, COMPUT. BUS. REV. (Jan 4, 2019), <https://www.cbronline.com/news/german-data-leak>; Natasha Singer, *What You Don’t Know About How Facebook Uses Your Data*, N.Y. TIMES (Apr. 11, 2018), <https://www.nytimes.com/2018/04/11/technology/facebook-privacy-hearings.html>.

But we also readily give our data away. We click through terms and conditions on the internet and breezily swipe along through smart phone apps as we consent to myriads of tiny print. As technology started to play a larger and larger role in our everyday lives, there was at least some acknowledgement that we were engaging in a trade.³ Data for you, benefit for me. Yet, new innovations in technology are making that trade more difficult to see—or at least to see clearly.⁴ Moreover, rights to data are raising large social, political, and economic issues across the United States and the world.⁵ Consider, for example, home security cameras like Amazon Cloud Cam, Netgear Arlo Pro, and Nest Hello—often used as part of making your residence a “smart home.”⁶ From a data privacy perspective, these seem rather innocuous. The homeowner just wants to know who is coming to the front door.⁷ If a “bad guy” comes knocking, the camera captures his or her image and can scan the internet using facial recognition technology to discover who the unwelcome guest might be.⁸

However, what happens if that facial data gets shared with others? What if it gets posted to social media accounts and spreads further through the internet?⁹ What also happens when law enforcement officials or immigration control officers become involved?¹⁰ If this sounds far-fetched, consider that Ring—a prominent digital home security device—already has a “neighborhood social network”¹¹ as part of its service package, and the owner of Ring (Amazon) has filed a patent application for a “database of suspicious persons.”¹² It’s easy to see how the wrong person being caught on camera (and then having his or her face photo

³ Farhad Manjoo, *It’s Time to Panic About Privacy*, N.Y. TIMES (Apr. 4, 2019), <https://www.nytimes.com/interactive/2019/04/10/opinion/internet-data-privacy.html>.

⁴ *Id.*

⁵ *Id.*

⁶ *Best Security Cameras for 2019*, CNET, <https://www.cnet.com/topics/security-cameras/best-security-cameras/> (last visited Feb. 25, 2019).

⁷ Manjoo, *supra* note 3.

⁸ *Id.*; David White, James D. Dunn, Alexandra C. Schmid & Richard I. Kemp, *Error Rates in Users of Automatic Face Recognition Software*, PLOS ONE (Oct. 14, 2015), <https://doi.org/10.1371/journal.pone.0139827>; Nancy Gupton, *Understanding Facial Recognition Software*, FRANKLIN INST., <https://www.fi.edu/understanding-facial-recognition-software> (last visited Apr. 16, 2019).

⁹ Manjoo, *supra* note 3.

¹⁰ *Id.*; Laura Entis, *The Crazy, Cool and Unsettling Ways Police Are Using Social Media*, ENTREPRENEUR, <https://www.entrepreneur.com/article/233604> (last visited Apr. 17, 2019).

¹¹ *Welcome to Ring Neighbors*, RING, <https://support.ring.com/hc/en-us/articles/115004841143-Welcome-to-Ring-Neighbors> (last visited Apr. 12, 2019).

¹² Peter Holley, *This Patent Shows Amazon May Seek to Create a ‘Database of Suspicious Persons’ Using Facial-Recognition Technology*, WASH. POST (Dec. 18, 2018, 6:01 AM), https://www.washingtonpost.com/technology/2018/12/13/this-patent-shows-amazon-may-seek-create-database-suspicious-persons-using-facial-recognition-technology/?utm_term=.ca1e46612997.

shared) can turn into a quick case of digital profiling.¹³ And what about all the additional data that can be collected from smart home cameras that are within the home? Although a homeowner might only intend to keep an eye on the dog or the kids while in the playroom, one wonders what other uses this data can be put to, such as by internet service providers, data brokers, or abusive spouses.¹⁴ Indeed, smart home cameras are already a favorite tool of domestic abusers.¹⁵ And most people would be surprised to learn that the 2017 Congressional repeal of certain Obama era rules¹⁶ now allows internet service providers to collect data about *any* internet-connected device in a person's home—everything from baby monitors to TVs and more.¹⁷ Moreover, these internet companies can sell this collected data to third parties without consumer approval and even without the consumer knowing.¹⁸

So, it's not quite as clear as it once was what exactly we give up when we make that trade of data for a benefit. Each time we engage with the digital world—each time we buy and power-up a new device—we give up a little more about ourselves: where we go, what we do, who we do it with (or even what we do when we're alone).¹⁹ In the US, we think of China as a surveillance state, but there's one being built here at home and most Americans only have the vaguest notion that it is happening and hardly any idea of how extensive it has (or will) become.²⁰ Further, the government is not behind the watching here—it's corporate America and, specifically, Silicon Valley.²¹ And despite much howling in the face of data breaches as with the Cambridge Analytica/Facebook scandal and at places like Under Armour, Target, and Best Buy, lawmakers have done little to truly regulate data privacy.²² Indeed, in 1974 Congress at-

¹³ See Manjoo, *supra* note 3.

¹⁴ *Id.*

¹⁵ Nellie Bowles, *Thermostats, Locks and Lights: Digital Tools of Domestic Abuse*, N.Y. TIMES (June 23, 2018), <https://www.nytimes.com/2018/06/23/technology/smart-home-devices-domestic-abuse.html>.

¹⁶ See H.R.J. Res. 86, 115th Cong. (2017) (“Providing for congressional disapproval under chapter 8 of title 5, United States Code, of the rule submitted by the Federal Communications Commission relating to ‘Protecting the Privacy of Customers of Broadband and Other Telecommunications Services’”).

¹⁷ Matt Reynolds, *Your Broadband Provider Can Use Your Smart Devices to Spy on You*, NEW SCIENTIST (Aug. 28, 2017), <https://www.newscientist.com/article/2145450-your-broadband-provider-can-use-your-smart-devices-to-spy-on-you/> (emphasis added).

¹⁸ Kieren McCarthy, *Your Internet History on Sale to Highest Bidder: US Congress Votes to Shred ISP Privacy Rules*, REGISTER (Mar. 28, 2017, 7:42 PM), https://www.theregister.co.uk/2017/03/28/congress_approves_sale_of_internet_histories/.

¹⁹ Manjoo, *supra* note 3.

²⁰ *Id.*

²¹ See *id.*

²² See, e.g., Cameron F. Kerry, *Will This New Congress Be the One to Pass Data Privacy Legislation?*, BROOKINGS (Jan. 7, 2019), <https://www.brookings.edu/blog/techtank/2019/01/07/will-this-new-congress-be-the-one-to-pass-data-privacy-legislation/>; *Congress Is Trying*

tempted to create a privacy law and succeeded, but heavy lobbying resulted in the law only applying to the government—not to businesses.²³ Later privacy laws were enacted such as the Health Insurance Portability and Accountability Act of 1996 (HIPAA) dealing with health record privacy and the Gramm-Leach-Bliley Act of 1999 dealing with financial privacy, but none attempted to deal comprehensively with data privacy.²⁴ More recent efforts have stalled completely.²⁵

It is quite fitting that the collection of works of which this Essay is a part comes as a tribute the retirement of Professor Gregory Alexander—one of the giants of modern American property law²⁶—because when it comes to the law of data, the law of property might be the only tool that can make a difference in this fight for data privacy. Although lawmakers have been unwilling to make hard decisions about data privacy, data privacy issues—legal issues—continue to come into prominence. In the 2018 term, the Supreme Court of the United States issued two major decisions dealing with data and in both cases property law very much served as the foundation for how the Court reached its decision. The two cases, *Wayfair v. South Dakota*²⁷ and *Carpenter v. United States*,²⁸ dealt with quite different issues. The former was a taxing case involving online retailers and the limitations of state power under the dormant commerce clause.²⁹ The latter was a dispute about unlawful searches and seizures involving the use of cell phone location data obtained from third party

to Create a Federal Privacy Law, *ECONOMIST* (Feb. 28, 2019), <https://www.economist.com/usa/2019/02/28/congress-is-trying-to-create-a-federal-privacy-law> (“The fourth attempt in 45 years turns on how federal law will supersede state laws.”).

²³ Kerry, *supra* note 22; see Privacy Act of 1974, Pub. L. No. 93-579, 88 Stat. 1896. During this time, the well-intentioned but much flawed Fair Credit Reporting Act was also passed. See Pub. L. No. 91-508, 84 Stat. 1114-2 (1970) (codified as amended in scattered sections of 12 U.S.C. and 31 U.S.C.).

²⁴ See Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936 (HIPAA); see also Pub. L. No. 106-102, 113 Stat. 1338 (GLB).

²⁵ Issie Lapowsky, *Get Ready for a Privacy Law Showdown in 2019*, *WIRED* (Dec. 27, 2018, 7:00 AM), <https://www.wired.com/story/privacy-law-showdown-congress-2019/>; see also Kerry, *supra* note 22.

²⁶ Among his many accomplishments, Professor Alexander is the author of one of the country’s most widely-used first year property law casebooks. See generally JESSE DUKEMINIER, JAMES E. KRIER, GREGORY S. ALEXANDER, MICHAEL H. SCHILL & LIOR JACOB STRAHILEVITZ, *PROPERTY* (2017).

²⁷ 138 S. Ct. 2080 (2018).

²⁸ 138 S. Ct. 2206 (2018).

²⁹ Phillip Popkin, *The Effect of the Internet Era and South Dakota v. Wayfair on the Unitary Business Rule*, 60 B.C. L. REV. E-Supplement II.-82, II.-86 (2019); Matthew C. Boch, *Way(Un)fair? United States Supreme Court Decision Ends State Tax Physical Presence Nexus Test*, *ARK. LAW.*, Summer 2018, at 18.

mobile phone companies.³⁰ The connection of both to property law is not direct but is nevertheless quite consequential.

For much of the modern era, the development of technology has gone relatively unchecked. In the United States, we have adopted a policy of encouraging technological innovation and growth, with the government ceding much of the policymaking terrain to Silicon Valley. Whereas numerous types of manufacturing, banking, consumer financial services, airlines, and other sectors of the economy operate under fair heavy regulation, technology has enjoyed a relatively light touch. With such a benefit in hand, technology has grown significantly over the past few decades. This is perhaps best seen in the contest of online platforms like Facebook, Instagram, Twitter, Google, Amazon, and YouTube.³¹ Some of these firms are used nominally for social connectivity while others are engaged in large-scale retail commerce.³² Common to all of them, however, is the way in which they facilitate the creation and then utilization of vast amounts of consumer data.³³ Users who engage with these firms generate bits and bytes about themselves based on their activities, preferences, and habits.³⁴ This information—this “data”—is then harnessed by tech companies, either the ones generating its creation or ones that acquire it from others—for a variety of purposes ranging from advertising to market analytics, and more.³⁵ The amount of data which is generated is both vast and effortlessly created by virtue of algorithms, machine learning, and other advances.³⁶

Yet, we struggle with what to do with data. Instinctively, we desire to use the tools and frames of property law to deal with data.³⁷ Property

³⁰ Paul M. Schwartz, *Legal Access to the Global Cloud*, 118 COLUM. L. REV. 1681, 1711 (2018); see also Paige M. Boshell, *Survey of Developments in Federal Privacy Law*, 74 BUS. LAW. 191, 198 (2019).

³¹ See Jeff Desjardins, *Animation: The Biggest Tech Companies by Market Cap over 23 Years*, VISUAL CAPITALIST (Mar. 18, 2019), <https://www.visualcapitalist.com/biggest-tech-companies-market-cap-23-years/>; Julie E. Cohen, *Law for the Platform Economy*, 51 U.C. DAVIS L. REV. 133, 136 (2017); Orly Lobel, *The Law of the Platform*, 101 MINN. L. REV. 87, 94 (2016).

³² Lobel, *supra* note 31, at 96 (“[T]he platform economy’s offerings are so diverse that neatly describing its scope is impractical.”).

³³ D. Daniel Sokol & Roisin Comerford, *Antitrust and Regulating Big Data*, 23 GEO. MASON L. REV. 1129, 1131 (2016).

³⁴ See, e.g., Kenneth A. Bamberger & Orly Lobel, *Platform Market Power*, 32 BERKELEY TECH. L.J. 1051, 1077–78 (2017) (discussing the “God View” where data can be harnessed so comprehensively and precisely that the state of the market can be ascertained at any particular point in time).

³⁵ Lobel, *supra* note 31, at 94–95.

³⁶ *Id.*

³⁷ See *South Dakota v. Wayfair*, 138 S. Ct. 2080 (2018); *Carpenter v. United States*, 138 S. Ct. 2206 (2018); Barb Darrow, *The Question of Who Owns the Data Is About to Get a Lot Trickier*, FORTUNE (Apr. 6, 2016), <http://fortune.com/2016/04/06/who-owns-the-data/>; Josef Drexler et al., *Data Ownership and Access to Data - Position Statement of the Max Planck*

law is familiar. It is tried and true. Property law is laden with doctrines and rules and norms that have been honed over time and that provide a level of comfort and fluency. Perhaps because of this, it is no surprise that the Court in both *Wayfair* and *Carpenter* used aspects of property law to decide the case. What is most significant about the Court's use of property law here, however, is that it has an even greater potential to help the nascent contouring of the law governing data.

This Essay attempts to modestly add to the scholarly discussion about data as property—a topic that has already benefited from the insightful scholarship of others in the legal academy³⁸—by advocating for a progressive property approach. In reviewing the decision of the Court

Institute for Innovation and Competition of 16 August 2016 on the Current European Debate (Max Planck Inst. for Innovation & Competition, Res. Paper No. 16-10, Jan. 2016); Barbara J. Evans, *Much Ado About Data Ownership*, 25 HARV. J.L. & TECH. 69, 70 (2011); Nadezhda Purtova, *Do Property Rights in Personal Data Make Sense after the Big Data Turn?: Individual Control and Transparency* (Tilburg Law Sch. Research Paper No. 2017/21, 2017); Sjef van Erp, *Ownership of Digital Assets and the Numerus Clausus of Legal Objects* (Maastricht European Private Law Inst. Working Paper No. 2017/6, 2017).

³⁸ See, e.g., Natalie M. Banta, *Property Interests in Digital Assets: The Rise of Digital Feudalism*, 38 CARDOZO L. REV. 1099 (2017); Natalie M. Banta, *Death and Privacy in the Digital Age*, 94 N.C. L. REV. 927 (2016); Natalie M. Banta, *Inherit the Cloud: The Role of Private Contracts in Distributing or Deleting Digital Assets at Death*, 83 FORDHAM L. REV. 799 (2014); Natalie Banta & Naomi R. Cahn, *Digital Asset Planning for Minors*, PROB. & PROP., Jan./Feb. 2019, at 44; Victoria Blachly, *Uniform Fiduciary Access to Digital Assets Act: What UFADAA Know*, 29 PROB. & PROP., July/Aug. 2015, at 8, 10; Charles Blazer, *The Five Indicia of Virtual Property*, 5 PIERCE L. REV. 137 (2006); M. Scott Boone, *Virtual Property and Personhood*, 24 SANTA CLARA COMPUT. & HIGH TECH. L.J. 715, 716 (2008); Christopher J. Ciffrino, *Virtual Property, Virtual Rights: Why Contract Law, Not Property Law, Must Be the Governing Paradigm in the Law of Virtual Worlds*, 55 B.C. L. REV. 235, 235 (2014); Michael Druckman-Church, *Taxing a Galaxy Far, Far Away: How Virtual Property Challenges International Tax Systems*, 51 COLUM. J. TRANSNAT'L L. 479 (2013); JOSHUA A.T. FAIRFIELD, OWNED: PROPERTY, PRIVACY, AND THE NEW DIGITAL SERFDOM (2017); Joshua A.T. Fairfield, *Bitproperty*, 88 S. CAL. L. REV. 805 (2015); Joshua A.T. Fairfield, *Virtual Property*, 85 B.U. L. REV. 1047, 1047 (2005); Jennifer Gong, *Defining and Addressing Virtual Property in International Treaties*, 17 B.U. J. SCI. & TECH. L. 101, 102 (2011); Steven J. Horowitz, *Competing Lockean Claims to Virtual Property*, 20 HARV. J.L. & TECH. 443 (2007); Kurt Hunt, *This Land Is Not Your Land: Second Life, Copybot, and the Looming Question of Virtual Property Rights*, 9 TEX. REV. ENT. & SPORTS L. 141 (2007); Sarah Howard Jenkins, *Application of the U.C.C. to Nonpayment Virtual Assets or Digital Art*, 11 DUQ. BUS. L.J. 245 (2009); Dan E. Lawrence, *It Really Is Just a Game: The Impracticability of Common Law Property Rights in Virtual Property*, 47 WASHBURN L.J. 505 (2008); Michael Meehan, *Virtual Property: Protecting Bits in Context*, 13 RICH. J.L. & TECH. 7, 1 (2006); John William Nelson, *The Virtual Property Problem: What Property Rights in Virtual Resources Might Look Like, How They Might Work, and Why They Are a Bad Idea*, 41 MCGEORGE L. REV. 281 (2010); AARON PERZANOWSKI & JASON SCHULTZ, THE END OF OWNERSHIP: PERSONAL PROPERTY IN THE DIGITAL ECONOMY (2018); Michael C. Pollack, *Taking Data*, 86 U. CHI. L. REV. 77 (2019); Sally Brown Richardson, *Classifying Virtual Property in Community Property Regimes: Are My Facebook Friends Considered Earnings, Profits, Increases in Value, or Goodwill?*, 85 TUL. L. REV. 717 (2011); Pamela Samuelson, *Privacy as Intellectual Property?*, 52 STAN. L. REV. 1125, 1131 (2000); Ryan Vacca, *Viewing Virtual Property Ownership Through the Lens of Innovation*, 76 TENN. L. REV. 33 (2008).

in both *Wayfair* and *Carpenter*, I point out examples of where the Justices struggle with the optimal way to think about data. At times the Court seems to eschew property concepts when it comes to digital information in favor of other standards, such as contract law or constitutional standards of privacy. At other times, the justices cling tightly to the age-old bedrock pillars of property law, asking the allegedly simple question of who owns what. And still on other occasions, members of the Court seem to be treading new ground (or rediscovering old roads) in property law when it comes to the ever-present and increasingly vast world of data information.

It is here in this wayward struggle of defining “property as data” that the sea-change in property law thinking that Professor Alexander and others have heralded under the banner of the progressive property movement can have a significant and continued impact. In the face of legislative inaction, American courts are struggling to use property law concepts to deal with rights in data. The results of this hammering and chipping will have significant and long-term consequences for how we create, control, and dispose of the information we are constantly generating about ourselves. Rather than continuing to allow this sliced and hewn body of law to haphazardly develop, progressive property scholars in the tradition of Professor Alexander should help courts and lawmakers understand the collective values and human flourishing goals that are so inherent in property law and how these same concerns can and should animate the law of digital property.

I. DATA AND PROPERTY LAW DISRUPTION

Property law has a propensity to cling to a persistent concept of physicality.³⁹ Much of property law focuses on possession⁴⁰ in the physical sense—capturing⁴¹ or finding⁴² an object or conveying⁴³ a physical thing. Even commercial law—a sort of cousin to property law—has a significant commitment to the tangible.⁴⁴ The connection between physicality and property law is not at all surprising. Indeed, it is emotive.⁴⁵ It

³⁹ Juliet M. Moringiello, *What Virtual Worlds Can Do for Property Law*, 62 FLA. L. REV. 159, 181 (2010); Juliet M. Moringiello, *False Categories in Commercial Law: The (Ir)relevance of (in)tangibility*, 35 FLA. ST. U. L. REV. 119, 122 (2007).

⁴⁰ SHELDON E. KURTZ, HERBERT HOVENKAMP, CAROL NECOLE BROWN & CHRISTOPHER K. ODINET, *CASES AND MATERIALS ON AMERICAN PROPERTY LAW* § 3.1–6 (7th ed. 2019).

⁴¹ *Id.* § 1.3.

⁴² *Id.* § 1.4.

⁴³ *Id.* § 14.1–4.

⁴⁴ An example of this is the entirety of Article 3 of the Uniform Commercial Code which requires a physical piece of paper for negotiable instrument law to operate. *See* U.C.C. art. 3 (AM. LAW INST. & UNIF. LAW COMM’N 2014).

⁴⁵ Ben McEniery, *Physicality and the Information Age: A Normative Perspective on the Patent Eligibility of Non-Physical Methods*, 10 CHL.-KENT J. INTELL. PROP. 106, 129 (2010).

reflects our understanding of the things around us—property—in a way that matches many of our sensibilities. What we can touch, feel, and see is salient to us and therefore is more meaningful when it is handed over or taken away.

These considerations raise the issue of how exactly we should treat data and digital assets in the context of property since they lack physicality.⁴⁶ First, some definitional concerns should be addressed. I refer to “data” to mean information recorded in any electronic form or medium.⁴⁷ In turn, a “digital asset” is data in which a person has a right or interest but which does not have a physical form.⁴⁸ For instance, the narratives, videos, images, and profile information loaded to a social media account constitute data. The social media account itself is a digital asset. In turn, one could also argue that the narratives, videos, images, and profile information are each on their own a type of digital asset under the theory that the account holder—separate and apart from the account itself—has rights in these items. To explore the idea of property as data further, the following shows how property law and data or data-like rights often try to work hand-in-hand but with varying degrees of success.

A. *In Tort Law*

As an obvious point, data lack physicality. It is in fact this lack of physical form that I believe causes most problems with how the law deals with data broadly and digital assets more specifically. Consider the many ways in which the law tries to shoe-horn digital assets into property paradigms. In *Kremen v. Cohen*, the Ninth Circuit stated that a domain name is “an intangible property right” but was quick to impose physicality on the item in order to resolve the dispute by declaring that such a right was similar to “staking a claim to a plot of land” and then recording title to it in a registry system to put others on notice.⁴⁹ Similarly, U.S. bankruptcy courts have held that rights in a domain name are deemed assets of the bankrupt estate under the theory that the registrant of the domain name has rights akin to “direct, immediate and exclusive authority over a thing”—thereby harkening to a test that relies on an

⁴⁶ See Pollack, *supra* note 38 (giving justifications for treating data as property for Takings Clause purposes).

⁴⁷ This definition of data is derived from HIPAA and is also being used in the deliberations of the American Law Institute and the European Law Institute for their principles for a digital economy project (documentation is on file with author). See also 45 C.F.R. § 160.103 (2019). It is used in combination with the American Bar Association’s 2019 report on digital assets. See ABA, DIGITAL AND DIGITIZED ASSETS: FEDERAL AND STATE JURISDICTIONAL ISSUES (Mar. 2019), <https://www.steptoe.com/images/content/1/9/v2/190803/ABA-Digital-Assets-White-Paper.pdf>.

⁴⁸ See generally ABA, *supra* note 47, at 25.

⁴⁹ *Kremen v. Cohen*, 337 F.3d 1024, 1030 (9th Cir. 2003).

analogy to physical dominion.⁵⁰ In the context of property torts, some courts have embraced the non-physicality of certain types of property to allow for recovery under conversion. The Arkansas court in *Integrated Direct Marketing, LLC v. May* stated that “[t]here is simply no reasonable basis for allowing a claim for conversion of paper documents but not for their electronically stored counterparts.”⁵¹ Courts in Indiana have similarly held that digital assets, such as information generated from the use of a computer, constitute property for theft purposes.⁵²

Yet courts are not uniform in this approach and are not even consistent within the same jurisdiction. One Indiana court in 2005 held that alleged misuse of software-generated data is not actionable under “conversion, trespass, or replevin” because these claims “relate only to chattels themselves”⁵³ while another Indiana court in 2009 held that a “website design is personal property and is subject to a conversion claim. . . .”⁵⁴ The Tennessee court in *Wells v. Chattanooga Bakery, Inc.* refused to allow the tort claim of conversion to operate in the context of a digital image when it stated that “[c]onversion is the wrongful appropriation of another’s tangible property; an action for the conversion of intangible personal property is not recognized in Tennessee.”⁵⁵ The Georgia court in *Internal Medicine Alliance, LLC v. Budell* similarly wed itself to a physicality requirement in holding that “[c]onversion is not available as a cause of action with regard to intangible property interests that have not been merged into a document.”⁵⁶ Other states as diverse as Rhode Island,⁵⁷ Texas,⁵⁸ Illinois,⁵⁹ and Mary-

⁵⁰ *In re Larry Koenig & Assoc.*, No. 01-12829, 2004 WL 3244582, at *6 (Bankr. M.D. La. Mar. 31, 2004).

⁵¹ *Integrated Direct Mktg., LLC v. May*, 495 S.W.3d 73, 76 (Ark. 2016).

⁵² *See State v. McGraw*, 480 N.E.2d 552, 554 (Ind. 1985).

⁵³ *Coleman v. Vukovich*, 825 N.E.2d 397, 408 (Ind. Ct. App. 2005).

⁵⁴ *Conwell v. Gray Loon Outdoor Mktg. Grp., Inc.*, 906 N.E.2d 805, 818 (Ind. 2009).

⁵⁵ *Wells v. Chattanooga Bakery, Inc.*, 448 S.W.3d 381, 392 (Tenn. Ct. App. 2014).

⁵⁶ *Internal Med. Alliance v. Budell*, 659 S.E.2d 668, 675 (Ga. Ct. App. 2008).

⁵⁷ *Narragansett Elec. Co. v. Carbone*, 898 A.2d 87, 97 (R.I. 2006) (“[A] conversion action will not lie for a partnership interest or other intangible property right that is not manifested by a tangible instrument, such as a written agreement, a bankbook, or a promissory note, that may, in turn, be converted.”) (quoting *Montecalvo v. Mandarelli*, 682 A.2d 918, 929 (R.I. 1996)).

⁵⁸ *Rehak Creative Servs., Inc. v. Witt*, 404 S.W.3d 716, 734 (Tex. App. 2013), *disapproved of by In re Lipsky*, 460 S.W.3d 579 (Tex. 2015) (“[I]ntangible property cannot be converted unless the underlying intangible right has been merged into a document that has been converted.”).

⁵⁹ *In re Thebus*, 483 N.E.2d 1258, 1260 (Ill. 1985) (“[T]he subject of conversion is required to be an identifiable object of property of which the plaintiff was wrongfully deprived. Money may be the subject of conversion, but it must be capable of being described as a specific chattel”) (reaffirmed in *The Film & Tape Works, Inc. v. Junetwenty Films, Inc.*, 856 N.E.2d 612, 624 (Ill. App. Ct. 2006)).

land⁶⁰ also eschew the possibility that an intangible right can be converted (and thereby give relief to the right holder) unless it is represented in a physical, paper form.

B. *In Cryptocurrencies*

Newer forms of digital assets have proven even more difficult for courts and lawmakers to define. The most prominent example are cryptocurrencies (also called virtual currencies) such as the likes of Bitcoin.⁶¹ The issue of whether these complex strings of 1s and 0s that some people use to pay for goods and services, and others use for investment purposes, actually constitute “property” has vexed policymakers and courts.⁶² The determination has wide-ranging effects for purposes of sundry legal regimes ranging from criminal and tort law to securities, commercial, and tax law.⁶³

As recently as January 2018, the Idaho Senate introduced a bill that would have explicitly included virtual currency as property for purposes of the state’s unclaimed property act.⁶⁴ The bill defined “virtual currency” to mean “a digital representation of value used as a medium of exchange, unit of account or store of value that does not have legal tender status recognized by the United States.”⁶⁵ Iowa’s legislature is also currently considering a bill to implicitly recognize cryptocurrencies as a form of property by specifically exempting them from the state’s sales and use tax.⁶⁶ Kentucky has made similar efforts.⁶⁷ Yet there is uncertainty around cryptocurrencies as a true form of property. Some commentators have critiqued treating them as property because of the

⁶⁰ *Thompson v. UBS Fin. Servs., Inc.*, 115 A.3d 125, 136 (Md. 2015) (“Maryland will remain among the many jurisdictions that maintain conversion of a document as an element of conversion of intangible property[.]”).

⁶¹ See generally REGULATING BLOCKCHAIN: TECHNO-SOCIAL AND LEGAL CHALLENGES (Philipp Hacker, Georgios Dimitropoulos, Stefan Eich & Ioannis Lianos eds., 2019) (explaining cryptocurrencies) (“Blockchain is a technology that facilitates value exchanges in a secure and decentralized manner, without the need for an intermediary.”).

⁶² PERKINS COIE, TREATMENT OF BITCOIN UNDER U.S. PROPERTY LAW (Mar. 2017), <https://www.perkinscoie.com/images/content/1/9/v5/199638/2018-Treatment-of-Bitcoin-Under-U.S.-Property-Law-White-Paper.pdf>; Thomas Merrill & Henry Smith, *Optimal Standardization in the Law of Property: The Numerus Clausus Principle*, 110 YALE L. J. 1, 4 (2000).

⁶³ PERKINS COIE, *supra* note 62, at 11–14.

⁶⁴ Matthew E. Kohen & Justin S. Wales, *State Regulations on Virtual Currency and Blockchain Technologies*, CARLTON FIELDS (Jan. 9, 2019), <https://www.carltonfields.com/insights/publications/2018/state-regulations-on-virtual-currency-and-blockchain-technologies>. See also S.F. 125, 65th Leg., Gen. Sess. (Wy. 2019) (classifying digital assets as property, which allows for direct ownership of cryptoassets and entails that commercial law protections available under the Uniform Commercial Code apply to such ownership).

⁶⁵ S.F. 125.

⁶⁶ *Id.*; see also H.F. 255, 2019 Gen. Assemb., Reg. Sess. (Ia. 2019).

⁶⁷ Kohen & Wales, *supra* note 64; H.B. 354, 2019 Gen. Assemb., Reg. Sess. (Ky. 2019).

semi-anonymous nature of the public access keys, meaning that there cannot be a clear claim of exclusion.⁶⁸ Other commentators wonder whether situations where no single person or entity has control over access to a cryptoasset—such as in situations where multiple keys are held by multiple parties and all need to agree in order to transact business—create rights that should be appropriately called property rights.⁶⁹

C. *In Inheritance*

Perhaps nowhere has the law of data and digital property seen more difficulty and also more progress than in the inheritance context. For years a struggle existed between online companies and heirs of account holders for access to a decedent's online accounts. This struggle is perhaps best explained in the context of the 2017 case of *Ajemian v. Yahoo!, Inc.* In that case, Robert created a Yahoo! email account for his brother John in 2002.⁷⁰ John used the account until his death in 2006.⁷¹ Robert and another sibling, Marianne, were later appointed co-representatives of John's estate.⁷² As part of administering the estate, a written request was sent to Yahoo for access to John's email account.⁷³ Yahoo, however, declined by stating first that it was prohibited from doing so by certain requirements of the Stored Communications Act⁷⁴ and second by declaring that Yahoo's email account terms of service gave the company complete discretion to reject an access request by a personal representative.⁷⁵ Similar arguments have been made by other online companies in the context of obtaining access to the online accounts—i.e., the data and digital assets—of decedents.⁷⁶ Here again the issue came down to whether the accounts constituted the “property” of the decedent such that it was unequivocally part of the estate.

What resulted from these disputes was a law reform effort led by the Uniform Law Commission. The end-product was the Uniform Fiduciary Access to Digital Assets Act,⁷⁷ which attempts to address the many

⁶⁸ PERKINS COIE, *supra* note 62, at 14; *see also* RYAN J. STRAUS & MATTHEW J. CLEARY, *THE LAW OF BITCOIN: THE UNITED STATES* 187 (Jeiry Brito ed., 2015).

⁶⁹ PERKINS COIE, *supra* note 62, at 15. Objections based on traceability are raised as well. *See id.*

⁷⁰ *Ajemian v. Yahoo!, Inc.*, 84 N.E.3d 766, 768 (Mass. 2017).

⁷¹ *Id.*

⁷² *Id.*

⁷³ *Id.*

⁷⁴ 18 U.S.C. §§ 2701–2712 (2018); *Ajemian*, 84 N.E.3d at 768.

⁷⁵ *Ajemian*, 84 N.E.3d at 768.

⁷⁶ *See, e.g., In re Estate of Serrano*, 54 N.Y.S.3d 564, 566 (Sur. Ct. 2017) (seeking access to a Google account); *In re Scandalios*, No. 2017-2976/A, 2019 WL 266570 (N.Y. Sur. Ct. Jan. 14, 2019) (seeking access to an Apple account); *In re Facebook, Inc.*, 923 F. Supp. 2d 1204 (N.D. Cal. 2012) (seeking access to a Facebook account).

⁷⁷ NAT'L CONFERENCE OF COMM'RS ON UNIF. STATE LAWS, Revised Fiduciary Access to Digital Assets Act (2015), <https://www.uniformlaws.org/committees/community-home/library>

situations in which someone dies and leaves behind a host of digital assets ranging from “photographs, electronic investment account statements, e-mails, social media accounts, bank account statements, and so on” but where the person did not make arrangements for those they leave behind to have access to these important items.⁷⁸ It also attempts to address situations where the account holder is still alive but where a power of attorney has been executed or a guardian has been appointed. But even here, the issue of who “owns” the information was controversial and the legislation mostly gestures toward who has “access.”⁷⁹

D. *In Secured Lending*

And to be sure, it is not just courts that have difficulty in dealing with data and digital assets. Legislators and law reform groups find the task difficult as well. As an example, consider the use of digital assets in secured lending.⁸⁰ The law in this area (Article 9 of the Uniform Commercial Code or just “UCC 9”) suffers from major structural weaknesses in dealing with collateralizing data/digital assets.

In terms of what kind of property *can* be the subject of a UCC 9 security interest, the law sets forth a number of collateral-specific categories, ranging from equipment and inventory, to instruments and investment property.⁸¹ In most cases parties use these broad categories to describe the collateral rather than overly detailing the particulars of the property in question.⁸² The category most relevant for a discussion of data or digital assets is that of “general intangibles.”⁸³

documents?communitykey=f7237fc4-74c2-4728-81c6-b39a91ecdf22&tab=librarydocuments (last visited Oct. 10, 2019).

⁷⁸ Elizabeth D. Barwick, Note, *All Blogs Go to Heaven: Preserving Valuable Digital Assets Without the Uniform Fiduciary Access to Digital Assets Act's Removal of Third Party Privacy Protections*, 50 GA. L. REV. 593, 607–08 (2016) (discussing transferability problems with online accounts); Jamie P. Hopkins, *Afterlife in the Cloud: Managing a Digital Estate*, 5 HASTINGS SCI. & TECH. L.J. 209, 212 (2013); Samantha D. Haworth, Note, *Laying Your Online Self to Rest: Evaluating the Uniform Fiduciary Access to Digital Assets Act*, 68 U. MIAMI L. REV. 535, 537 (2014); Elizabeth Holland Capel, *Conflict and Solution in Delaware's Fiduciary Access to Digital Assets and Digital Accounts Act*, 30 BERKELEY TECH. L.J. 1211, 1242 (2015).

⁷⁹ See *The Revised Uniform Fiduciary Access to Digital Assets Act (RUFADAA)*, NOLO, <https://www.nolo.com/legal-encyclopedia/ufadaa.html> (last visited Apr. 17, 2019).

⁸⁰ Christopher K. Odinet, *Bitproperty and Commercial Credit*, 94 WASH. U. L. REV. 649, 676 (2017).

⁸¹ See Christopher K. Odinet, *Testing the Reach of UCC Article 9: The Question of Tax Credit Collateral in Secured Transactions*, 64 S.C. L. REV. 143, 154–55 (2012); see also LES-TER E. DENONN, SECURED TRANSACTIONS UNDER THE UCC 36 (1965).

⁸² Terry M. Anderson et al., *Attachment and Perfection of Security Interests Under Revised Article 9: A “Nuts and Bolts” Primer*, 9 AM. BANKR. INST. L. REV. 179, 187–89 (2001).

⁸³ See U.C.C. § 9-102(a)(42) (2015); see also Odinet, *supra* note 80, at 681.

First, as a broad matter the way in which all general intangibles are collateralized is fairly uniform.⁸⁴ The debtor, through a security agreement, grants an interest to the creditor in his or her “general intangibles,” and then the creditor files a financing statement describing the same in the UCC records of the jurisdiction.⁸⁵ From the perspective of UCC Article 9, nothing else need be done.⁸⁶ However, the process is not quite as simple as the law of secured transactions suggests.⁸⁷ Despite seemingly treating intangible assets as property on the front end, the UCC does not actually treat them as having the attributes of true property on the back-end.⁸⁸

The reason for this mismatch is because many online accounts where data are stored (i.e., digital assets) are comprised chiefly of license entitlements.⁸⁹ The interplay of this contract law concept creates significant difficulty in making data collateralization viable. While UCC section 9-408 attempts to blunt the effects of anti-assignment clauses in license agreements, the actual rights that a creditor can take in such forms of property are quite weak and, in the end, undercut the very value that the secured party seeks to capture.⁹⁰

To see this assertion play-out, consider the standard terms and conditions agreements for Facebook,⁹¹ Twitter,⁹² YouTube,⁹³ and PayPal.⁹⁴ They all describe the relationship between the platform and the user as being that of licensor and licensee and further explicitly prohibit the licensee from assigning his or her rights to anyone else. Likewise, most domain name agreements also contain similar provisions.⁹⁵ Collectively, these agreements signify that most all digital assets (despite how property-like we might consider them) are in fact not *really* property in the

⁸⁴ See WILLIAM D. WARREN & STEVEN D. WALT, *SECURED TRANSACTIONS IN PERSONAL PROPERTY* 363–64 (2007).

⁸⁵ See *id.*

⁸⁶ *Id.*

⁸⁷ See Odinet, *supra* note 80, at 681–82.

⁸⁸ *Id.*

⁸⁹ A license is “[a] permission, [usually] revocable, to commit some act that would otherwise be unlawful.” *License*, BLACK’S LAW DICTIONARY (11th ed. 2019).

⁹⁰ Odinet, *supra* note 80, at 695.

⁹¹ *Terms of Service*, FACEBOOK, § 4.5.4, <https://www.facebook.com/terms.php> (last revised Apr. 19, 2019) (“You will not transfer any of your rights or obligations under these Terms to anyone else without our consent.”); *id.* § 3.3.1 (“The license will end when your content is deleted from our systems.”).

⁹² *Twitter Terms of Service*, TWITTER, § 4, <https://twitter.com/en/tos> (last revised May 25, 2018).

⁹³ *Terms of Service*, YOUTUBE, §§ 5.A, 13, <https://www.youtube.com/static?template=terms> (last revised May 25, 2018).

⁹⁴ *PayPal User Agreement*, PAYPAL, <https://www.paypal.com/us/webapps/mpp/ua/user-agreement-full> (sections titled “Intellectual Property” and “Miscellaneous”) (last revised Sept. 3, 2019).

⁹⁵ See Odinet, *supra* note 80, at 696 n.321.

traditional sense and cannot be used as collateral without the consent of the actual platform company. In fairness, UCC section 9-408 attempts to deal with these anti-assignment clauses in license agreements by rendering them null. Any provision that attempts to prohibit the granting of a security interest in a general intangible (even if a license right) is considered ineffective, per the law.⁹⁶

However, section 9-408 makes a rather hollow promise. Although the anti-assignment clause may be ineffective, UCC Article 9 provides no way for the secured creditor to actually make *use* of the collateral once a default has occurred. The creditor will naturally want to take control of the digital asset upon the debtor's default and, as soon as possible, move to dispose of it to generate funds for satisfaction of the debt. However, that is impossible under the current scheme, as UCC section 9-408 makes clear that the licensor need not pay the slightest attention to the creditor or its supposed rights.⁹⁷ What value does the creditor have in the asset if it cannot compel the licensor to recognize the creditor's security interest in the so-called property?⁹⁸

Further, the creditor, aside from being unable to make a disposition of the collateral, cannot itself make use of the data.⁹⁹ If, for example, a company debtor that provided its inventory and general intangibles as collateral defaults, the creditor can certainly seize the physical inventory. However, it would *not* be able to take control of the company's website or social media accounts under the theory that they are merely license rights.¹⁰⁰ Indeed, it might very well be possible for the debtor to continue using the digital asset even after the creditor has seized the debtor's computers and other electronic equipment.¹⁰¹

In sum, the rise of data as valuable assets, and their bundling into discrete packages to which we ascribe some layman's sense of ownership (digital assets), has challenged property law in significant ways. Legal conundrums involving data and digital assets arise in the context of taxation, international law, intellectual property, searches and seizures, the takings clause, legal theory, and much more.¹⁰² Yet, despite the lack of physicality that so historically has defined traditional property law, courts and lawmakers still show a propensity to nevertheless use property

⁹⁶ See U.C.C. § 9-408(a) (2015).

⁹⁷ U.C.C. § 9-408 cmt. 2 ("However, under subsection (d), the secured party (absent the licensor's agreement) is not entitled to enforce the license or to use, assign, or otherwise enjoy the benefits of the licensed software, and *the licensor need not recognize (or pay any attention to) the secured party.*") (emphasis added).

⁹⁸ Steven D. Walt, *Uncertainty About Free Assignment: Payment and General Intangibles Under Article 9*, 2 J. PAYMENT SYS. L. 4, 16 (2006).

⁹⁹ U.C.C. § 9-408(d)(5) (2015).

¹⁰⁰ See *id.*

¹⁰¹ See *id.* § 9-408 cmt. 2.

¹⁰² See *supra* note 38 and accompanying citations.

constructs to define the rules that govern data and digital assets—even when these constructs are an awkward or even ineffective fit.

II. DATA PROPERTY AT THE SUPREME COURT

During the 2018 term, the US Supreme Court handed down two major decisions that reveal much about where the law of data is headed. Neither case had anything to do, at least facially, with property law. Yet, even a modest bit of unpacking reveals that property law was lurking right under the surface and at least partially influenced the justices' way of thinking.

A. *A Case About Taxes* (South Dakota v. Wayfair)

The first case is that of *South Dakota v. Wayfair*.¹⁰³ This case dealt with the ability of states to force online companies that conduct business in their borders (but do not have a physical presence there) to collect and remit use/sales tax to the jurisdiction.¹⁰⁴ In other words, when a consumer makes a purchase on his or her smart phone or laptop from an online company with no storefront or employees in that consumer's state, must the company nevertheless collect use tax on that transaction and remit it to the state taxing authorities?¹⁰⁵

At its core, the case involved the Dormant Commerce Clause of the U.S. Constitution, which bars states from creating undue burdens on interstate commerce. In the 1967 decision of *National Bellas Hess, Inc. v. Department of Revenue*, the Court held that a state *cannot* require a seller with no physical presence within that state to collect and remit taxes for property sold or shipped into the state.¹⁰⁶ This physical presence rule was clarified and again affirmed in the 1992 case of *Quill Corp. v. North Dakota*.¹⁰⁷ And again in the 2015 case of *Direct Marketing Ass'n v. Brohl*,¹⁰⁸ the Court declined to overturn the rule. However, in *Direct Marketing* Justice Kennedy questioned in a concurrence whether the physical presence rule should persist in light of the fast-changing digital economy and its impact on interstate commerce.¹⁰⁹

In response to Justice Kennedy's subtle invitation, the South Dakota Legislature passed a law requiring individuals who sell goods in that state, but who do not have a physical presence in South Dakota, to still

¹⁰³ 138 S. Ct. 2080 (2018).

¹⁰⁴ *Id.* at 2084; *see also* Annette Nellen, *New State and Local Tax Obligations in Cyberspace*, 74 BUS. LAW. 279, 279 (2019).

¹⁰⁵ *See Wayfair*, 138 S. Ct. at 2084.

¹⁰⁶ 386 U.S. 753 (1967) (emphasis added).

¹⁰⁷ 504 U.S. 298, 311–12 (1992).

¹⁰⁸ 135 S. Ct. 1124, 1127 (2015).

¹⁰⁹ *Id.* at 1134–35.

remit sales/use tax just as would sellers with a physical presence.¹¹⁰ Almost immediately after its passage, South Dakota commenced a declaratory judgment action against Wayfair and a number of other online retailers doing business in South Dakota and sought a judicial clarification that the new law was indeed constitutional—banking on the Supreme Court taking the case and overturning *Bellas Hess* and *Quill*.¹¹¹

In a 5–4 majority written by Justice Kennedy, the Court held that the physical presence rule was “unsound and incorrect” and therefore the cases upholding it were overruled.¹¹² The Court declared that sellers who engage in “a considerable amount of business in the State” can be forced to collect and remit taxes, without the need to have a physical presence in that state.¹¹³

Thus far, it may not seem clear as to how this decision deals with data and property law. Admittedly the connection is slight but is nevertheless present and important. In a bit of dicta, the majority opinion stated:

Modern e-commerce does not align analytically with a test that relies on the sort of physical presence defined in *Quill*. . . . [I]t is not clear why a single employee or a single warehouse should create a substantial nexus while “physical” aspects of pervasive modern technology should not. For example, a company with a website accessible in South Dakota *may be said to have a physical presence in the State via the customers’ computers. A website may leave cookies saved to the customers’ hard drives, or customers may download the company’s app onto their phones. Or a company may lease data storage that is permanently, or even occasionally, located in South Dakota. . . .* Between targeted advertising and instant access to most consumers via any internet-enabled device, “a business may be present in a State in a meaningful way without” that presence “being physical in the traditional sense of the term.”¹¹⁴

Now to be sure, this case was not decided on physicality. Indeed, the Court eschewed physicality as part of its test. But what is noteworthy is what this passage above says about the Court’s view on physicality

¹¹⁰ *Wayfair*, 138 S. Ct. at 2088–89.

¹¹¹ Tim Anderson, *Two Midwest States Join South Dakota with ‘Kill Quill’ Laws; Goal is to Collect Remote Sales Taxes*, CSG MIDWEST (May 2017), <https://www.csgmidwest.org/policyresearch/0517-commerce-sales-tax.aspx>.

¹¹² *Wayfair*, 138 S. Ct. at 2099.

¹¹³ *Id.*

¹¹⁴ *Id.* at 2095 (emphasis added).

and data—specifically, how despite admitting its inapplicability to this issue, the tangibility of property law still lurks as a fundamental background principle. In other words, the Court felt the need to express a view that data’s intangible nature can still be conceptualized as tangible under the law. This was done by expressing the idea that cookies generated by a website and stored automatically on the user’s computer constitute “property” of the website company and that said property is physically located in the place where the computer is located.¹¹⁵ This judicial desire to tie the concept of data to traditional property concepts is interesting because it tells us something about where the Court might go in the future as it deals with data issues. It shows a judicial proclivity to squeeze data concepts into traditional property law boxes—even when the fit is uncomfortable and perhaps (as in the cookie example) not even technically correct. For instance, who actually “owns” a cookie file is not self-evident. Visiting a website may indeed generate a cookie.txt file on the user’s computer, but the user has the ability to delete his or her cookies at will, thereby depriving the website of the user’s information.¹¹⁶ Indeed, a user can even disable the cookie function on his or her computer altogether.¹¹⁷ Does that make a cookie file seem less like property? Or does it make cookies seem more like the property of the user, rather than the website? Against this background, it is not so easy to classify the cookie—the data—as being exclusively owned by either of them.

B. *A Case About Cell Phones (Carpenter v. United States)*

The second (and even more pertinent) case is *Carpenter v. United States*,¹¹⁸ which was a search and seizure case involving cell phone location data.¹¹⁹ In this case, police arrested four individuals in connection with a series of armed robberies.¹²⁰ One of the individuals confessed and

¹¹⁵ Cookies are files that are transmitted from web sites (like Amazon.com) to a user’s web browser (like Safari) when that user visits the site. The web browser then stores these messages in a small file (called a cookie) on the user’s computer. The cookie collects information about the user’s activities on the website. The next time the user visits that site, the cookie is automatically sent to the website so that the website knows the user has been there before and will tailor the user’s experience accordingly (i.e., through directed advertising or automatically filling in the user name or password for the individual). WebWise Team, *What Are Cookies?*, BBC (Oct. 10, 2012), <http://www.bbc.co.uk/webwise/guides/about-cookies>.

¹¹⁶ Michael King, *How to Clear Cookies from Your Browser*, PCWORLD (June 6, 2019), https://www.peworld.com/article/242939/how_to_delete_cookies.html.

¹¹⁷ See, e.g., *Turn Cookies On or Off*, GOOGLE ACCOUNT HELP, <https://support.google.com/accounts/answer/61416?co=GENIE.Platform%3DDesktop&hl=en> (last visited Oct. 11, 2019).

¹¹⁸ 138 S. Ct. 2206 (2018).

¹¹⁹ See Boshell, *supra* note 30, at 198; see also Zachary R. Hoover, *The Pervasion of Cell Phones and the Fourth Amendment: A Right to Privacy in Locational Data*, 46 CAP. U. L. REV. 739, 761 (2018); Schwartz, *supra* note 30, at 1711.

¹²⁰ *Carpenter*, 138 S. Ct. at 2212.

gave investigators his cell phone number and the numbers of some of the other participants.¹²¹ The government then used this information to obtain court orders (but not warrants) to obtain transactional records for each of the phone numbers from the respective cell phone companies.¹²² The cell phone data provided included the date and time of calls from each of the numbers and, importantly, the approximate location where calls began and ended.¹²³

Based on the cell location data, the other individuals were charged with crimes, but the defense was raised that the data was obtained in violation of the accused's Fourth Amendment right to be free of unlawful searches and seizures.¹²⁴ Specifically, Carpenter argued that a warrant was needed for the government to obtain and then use this information against him because the cell phone data was *his property*, and the Fourth Amendment protects one's security in his or her "persons, houses, papers, and effects, against unreasonable searches and seizures."¹²⁵

Chief Justice Roberts wrote in yet another 5–4 majority that the government's warrantless acquisition of the cell phone indeed data violated the Fourth Amendment.¹²⁶ Admittedly, the majority did not decide the case based on property law concepts—which have long guided Fourth Amendment caselaw.¹²⁷ The Court held instead that the Fourth Amendment protects not only property interests, but *also reasonable expectations of privacy*.¹²⁸ In essence, the majority side-stepped the question of property rights by not answering the question of who actually owned the location data. The majority instead said that expectations of privacy in this age of digital data do not fit neatly into existing property precedents but that tracking a person's location at any given time through cell phone data is far more intrusive than the prior court decisions might have foreseen.¹²⁹ It is worth noting that the government argued that a person does not have a privacy interest *in the property of others*, and they based this assertion on the contents of the defendant's cell phone user agreement.¹³⁰ This contract specifically stated that any location data generated by the use of the phone belonged to the cell phone company, not the user of the phone.¹³¹

¹²¹ *Id.* at 2212–13.

¹²² *Id.*

¹²³ The location information was obtained based on each cell phone number's proximity to a relevant cell towers. *Id.* at 2211.

¹²⁴ *Id.* at 2209.

¹²⁵ *Id.* (emphasis added); *see also* U.S. CONST. amend. IV.

¹²⁶ *Carpenter*, 138 S. Ct. at 2221.

¹²⁷ *Id.* at 2213.

¹²⁸ *Id.* at 2215–17.

¹²⁹ *Id.* at 2209–10.

¹³⁰ *Id.* at 2219, 2225.

¹³¹ *Id.* at 2225, 2235.

The property analysis—which was significant—came in the form of the multiple dissents to *Carpenter*, written separately by each of Justices Alito, Thomas, Kennedy, and Gorsuch.¹³² Each of the dissenting justices used a property-based analysis and three of them said that, based on the user agreement, the data belonged to the cell phone company. Justice Kennedy noted that “[t]he right of the people [is] to be secure in their . . . persons, houses, papers, and effects”—not the persons, houses, papers, and effects of others.”¹³³ He explained that “[t]his case should be resolved by interpreting accepted property principles as the baseline for reasonable expectations of privacy.”¹³⁴ Similarly, Justice Thomas proclaimed that:

By obtaining the cell-site records of MetroPCS and Sprint, the Government did not search Carpenter’s property. He did not create the records, he does not maintain them, he cannot control them, and he cannot destroy them. Neither the terms of his contracts nor any provision of law makes the records his. The records belong to MetroPCS and Sprint. . . .¹³⁵

Importantly, Justice Thomas chided the defendant in stating that “[h]e cites no property law in his briefs to this Court, and he does not explain how he has a property right in the companies’ records under the law of any jurisdiction at any point in American history.”¹³⁶ Justice Alito was similarly convinced of the property justifications for rejecting the application of the Fourth Amendment to the acquisition of the data when he wrote that Carpenter lacked “the most essential and beneficial of the constituent elements’ of property—i.e., the right to use the property to the exclusion of others. . . .”¹³⁷

But perhaps no other dissent in *Carpenter* explored the idea of data as property so fully as that provided by Justice Gorsuch.¹³⁸ He explained that despite what cell phone user agreements might say about who owns data, “[p]eople often *do* reasonably expect that information they entrust to third parties, especially information subject to confidentiality agreements, will be kept private.”¹³⁹ He explained that “e-mail should be treated much like the traditional mail it has largely supplanted—as a bailment in which the owner retains a vital and protected legal interest.”¹⁴⁰ A

¹³² *Id.* at 2223, 2235, 2246, 2261.

¹³³ *Id.* at 2247.

¹³⁴ *Id.* at 2235.

¹³⁵ *Id.*

¹³⁶ *Id.* at 2242.

¹³⁷ *Id.* at 2259 (internal quotations omitted).

¹³⁸ *Id.* at 2261–72.

¹³⁹ *Id.* at 2263.

¹⁴⁰ *Id.* at 2269.

bailment, of course, is a property law concept defined as “the delivery of personal property by one person (the bailor) to another (the bailee) who holds the property for a certain purpose.”¹⁴¹ Most importantly, a bailment only creates a change in possession, but it does not effectuate a change in title (i.e., ownership).¹⁴² In my view, he is suggesting that the law, at least in part, should set aside the contents of cell phone user agreements (and by extension most online-based user agreement), as he ruminated: “I doubt that complete ownership or exclusive control of property is always a necessary condition to the assertion of a Fourth Amendment right.”¹⁴³ Rather, he explained that “[w]here houses are concerned, for example, individuals can enjoy Fourth Amendment protection without fee simple title.”¹⁴⁴

Particularly instructive is Justice Gorsuch’s statements about societal expectations and norms. He notes that “[p]eople call a house ‘their’ home when legal title is in the bank, when they rent it, and even when they merely occupy it rent free.”¹⁴⁵ What immediately comes to mind, then, is the way people in current times speak of “my social media account” or “my online profile” even though technically the license agreements that authorize the service or content state that said rights are freely terminable by the licensor.¹⁴⁶ In other words, he could very well be understood as suggesting that there should be a role for societal expectations and social norms—particularly when they are expressed through rhetoric that is largely property rights-inspired—in influencing how the law treats data. Indeed, Justice Gorsuch explained that “just because you *have* to entrust a third party with your data doesn’t necessarily mean you should lose all Fourth Amendment protections in it.”¹⁴⁷ Indeed, he notes that since “the use of technology is functionally compelled by the demands of modern life” then the way we generate data and cause it to be stored with “third parties may amount to a sort of involuntary bailment. . . .”¹⁴⁸ Again, a bailment leaves title with the bailor, and the bailee only has custody (possession) of the property. Does this mean that cell phone companies—despite the contents of their user agreements—

¹⁴¹ *Bailment*, BLACK’S LAW DICTIONARY (10th ed. 2014).

¹⁴² *Vulic v. Dep’t of Treasury*, 909 N.W.2d 487, 491 (Mich. Ct. App. 2017), *appeal denied*, 911 N.W.2d 727 (Mich. 2018); *see also* 8A AM. JUR. 2D *Bailments* § 1 (2019).

¹⁴³ *Carpenter*, 138 S. Ct. at 2269.

¹⁴⁴ *Id.*

¹⁴⁵ *Id.*

¹⁴⁶ *See supra* Part I.D.

¹⁴⁷ *Carpenter*, 138 S. Ct. at 2270.

¹⁴⁸ *Id.* An “involuntary bailment” is when a person accidentally, but without negligence, leaves personal property in the possession of another. BLACK’S LAW DICTIONARY, *supra* note 141. The traditional rule is that an involuntary bailee who refuses to return bailment property to the owner when demanded of him may be liable for the tort of conversion. *See id.*; 8 C.J.S. *Bailments* § 14 (2019).

are actually unknowing bailees of their customers' data? Might we say the same about social media platforms and tech giants like Google, Amazon, and Apple?

Ultimately, Justice Gorsuch makes clear that he would have preferred the majority to make its decision on property grounds, but he does not necessarily view it as a foregone conclusion—as do his dissenting colleagues—that mere resort to the cell phone user agreement should produce the ultimate answer. Instead, he invites further developments in state property law to do the work of guiding the Court as to how data should be treated: “If state legislators or state courts say that a digital record has the attributes that normally make something property, that may supply a sounder basis for judicial decisionmaking than judicial guesswork about societal expectations.”¹⁴⁹ While one may argue that this case's musings on property law and data should be cabined to only Fourth Amendment disputes, it is not quite so clear that such a walling-off is merited. Many of the pronouncements are more general in nature—only expressed in the Fourth Amendment context because of its relevancy to the facts at hand. At least in combination with *Wayfair*, it seems more likely that the property principles articulated have a broader applicability in questions of data.

III. A PROGRESSIVE PROPERTY APPROACH TO DATA

I offer here that state law should take up Justice Gorsuch's challenge of further developing data as property. Despite the difficulty seen through the experiences of legislatures and courts in dealing with data through a property lens, property is still the most normatively appropriate instrument for the task. In fact, property law is precisely the tool best able to deal with data and the competing concepts at play in data policy decisions and disputes. Specifically, Professor Alexander's distinctive view of property law—as outlined below—has all of the components necessary to help courts and lawmakers not only think about data as property but also how to operationalize this thinking into concrete policy decisions.

Before understanding the potential of Professor Alexander's work to make a lasting imprint in the data space, it is necessary for me to give an overview of his significant contributions. Although somewhat over-

¹⁴⁹ *Carpenter*, 138 S. Ct. at 2270 (Gorsuch, J., dissenting). In this part of his dissent, he cites TEX. PROP. CODE ANN. § 111.004(12) (West 2017), “defining ‘[p]roperty’ to include ‘property held in any digital or electronic medium.’” *Carpenter*, 138 S. Ct. at 2270 (alteration in original). State courts are busy expounding common law property principles in this area as well. *E.g.*, *Ajemian v. Yahoo!, Inc.*, 84 N.E.3d 766, 768 (Mass. 2017) (e-mail account is a “form of property often referred to as a ‘digital asset’”); *Eysoldt v. ProScan Imaging*, 194 Ohio App. 3d 630, 638, 2011-Ohio-2359, 957 N. E. 2d 780, 786 (permitting action for conversion of web account as intangible property). *See Carpenter*, 138 S. Ct. at 2270.

simplified, the traditional view of property law has been dominated by the concept of exclusion—the right to prevent others from using or otherwise enjoying property.¹⁵⁰ This idea is largely animated by a law and economics view of property rights that seeks to maximize individual welfare and lower transactions costs and frictions in property transactions.¹⁵¹ This long-standing view of property law has been most recently explored by the so-called exclusion or information theorists, who seek to understand property as concerned with the relationships between owners and non-owners.¹⁵²

However, a group of pioneering property scholars—which Professor Alexander led along with others—began developing alternative visions of ownership and property rights to contest the hegemony of the traditionalist view.¹⁵³ These pioneering legal thinkers are often referred to as the “progressive property” scholars,¹⁵⁴ and they endeavored to explain that “[p]roperty operates as both an idea and an institution.”¹⁵⁵ Because of this, internal tensions naturally arise as one person’s property rights have an impact—either positive or negative—on those of another. Thus, the progressive property scholars urged that when meeting the task of resolving property disputes, property law should “look to the underlying human values that property serves and the social relationships it shapes and reflects.”¹⁵⁶ In Professor Alexander’s words, the efforts of this new school of thought was to “correct the common but mistaken notion that ownership is solely about rights” and also to “emphasize the social obligations that are inherent in ownership.”¹⁵⁷

¹⁵⁰ See, e.g., J. E. PENNER, *THE IDEA OF PROPERTY IN LAW* 68 (1997); see also Larissa Katz, *Exclusion and Exclusivity in Property Law*, 58 U. TORONTO L.J. 275, 279–80 (2008); *Steltzer v. Spesaion*, 614 N.Y.S.2d 488, 490 (Civ. Ct. 1994) (“The right to exclude is a fundamental tenet of real property law.”).

¹⁵¹ See generally ROBIN PAUL MALLOY, *LAW AND ECONOMICS* (2019) (providing a concise explanation of law and economics concepts, including their applicable to property rules); Thomas W. Merrill & Henry E. Smith, *Making Coasean Property More Coasean*, 54 J.L. & ECON. S77 (2011); Thomas W. Merrill & Henry E. Smith, *What Happened to Property in Law and Economics?*, 111 YALE L.J. 357 (2001); A. MITCHELL POLINSKY, *AN INTRODUCTION TO LAW AND ECONOMICS* 9–10 (2d ed. 1983).

¹⁵² RICHARD A. EPSTEIN, *TAKINGS: PRIVATE PROPERTY AND THE POWER OF EMINENT DOMAIN* (1985); Thomas W. Merrill & Henry E. Smith, *The Morality of Property*, 48 WM. & MARY L. REV. 1849, 1853 (2007); Thomas W. Merrill, *Property as Modularity*, 125 HARV. L. REV. F. 151 (2012); Henry E. Smith, *Property as the Law of Things*, 125 HARV. L. REV. 1691 (2012); Thomas W. Merrill, *Property Rules, Liability Rules, and Adverse Possession*, 79 NW. U. L. REV. 1122 (1984); Thomas W. Merrill, *Property and the Right to Exclude*, 77 NEB. L. REV. 730 (1998).

¹⁵³ Gregory S. Alexander, *Pluralism and Property*, 80 FORDHAM L. REV. 1017 (2011).

¹⁵⁴ *Id.*

¹⁵⁵ Gregory S. Alexander et al., *A Statement of Progressive Property*, 94 CORNELL L. REV. 743 (2009).

¹⁵⁶ *Id.*

¹⁵⁷ Alexander, *supra* note 153.

This progressive concept of property has great potential to help shape the future law of data property. It provides the language and the analytical framework to help courts and lawmakers understand the competing views at play in data disputes, as well as the adaptable nature of property law in resolving these clashes. The following draws upon Professor Alexander's important work—much of which has formed the bedrocks of the progressive property movement—to help animate the notion of data as progressive property.

A. *Property and Social Obligation Norms*

Professor Alexander's specific contribution to the progressive property discussion involves a focus on the concept of social obligations being baked into and inherent in all property rights.¹⁵⁸ He explains in his 2009 article, *The Social-Obligation Norm in American Property Law*, that “[a] fully developed social-obligation norm requires some social vision.”¹⁵⁹ In other words, it needs “some substantive conception of the common good that serves as the fundamental context for the exercise of the rights and duties of private ownership.”¹⁶⁰ He fully admits that the tension “between individual and community interest[s]” makes a social norm of property rights “highly and inevitably contestable.”¹⁶¹ Yet, at the same time, he argues persuasively that “although human beings value and strive for autonomy, dependency and interdependency are inherent aspects of the human condition [as well].”¹⁶²

Buttressed by this notion of interconnectedness is the idea that humans are “social and political animals” which, in turn, helps us see what it means “to live a distinctively human life and to flourish in a characteristically human way.”¹⁶³ This idea of human flourishing is closely tied to a progressive account of property law. This is because, as Professor Alexander explains, “human beings develop the capacities necessary for a well-lived, and distinctly human life only in society with, indeed, dependent upon, other human beings.”¹⁶⁴ Secondly, flourishing includes “the capacity to make meaningful choices among alternative life

¹⁵⁸ This is sometimes also called an ontological or Aristotelian view of property law. See Gregory S. Alexander, *The Social-Obligation Norm in American Property Law*, 94 CORNELL L. REV. 745, 760–61 (2009).

¹⁵⁹ See *id.* at 757.

¹⁶⁰ *Id.*

¹⁶¹ *Id.*

¹⁶² *Id.* at 760; see also Gregory S. Alexander & Eduardo M. Peñalver, *Properties of Community*, 10 THEORETICAL INQ. L. 127 (2009).

¹⁶³ See Alexander, *supra* note 158, at 761.

¹⁶⁴ Alexander & Peñalver, *supra* note 162, at 135; see also Alexander, *supra* note 158, at 762.

horizons, to discern the salient differences among them, and to deliberate deeply about what is valuable within those available alternatives.”¹⁶⁵

Because of this close connection to community—to interconnectedness—human flourishing cannot occur if property law is only concerned with the individual and if it values exclusion to the marginalization of all else. In his important work titled *The Complex Core of Property*, Professor Alexander unpacks this idea in stating that “[t]he core of ownership is more complex than the right to exclude standing alone.”¹⁶⁶ But, by the same token, the social obligation theory of property does not jettison exclusion. It does not seek to “redistribute entitlements” but instead shines light on their context and complexity.¹⁶⁷

Thinking about data through this lens illuminates the digital rights debate. As in *Wayfair* and *Carpenter*, much of the focus was on who owned what. In *Wayfair*, the Court raised the notion that the ownership of the cookies by the online company created a willful manifestation of the company’s assent to the state’s taxing jurisdiction by virtue of being—in the most ephemeral sense—within the physical boundaries of the state.¹⁶⁸ In *Carpenter*, the court struggled with who exactly “owns” cell phone data: the user who created it and has an innate sense that his private movements are indeed private or the cell phone company, armed with a contract of adhesion, who created the service that generates the information.¹⁶⁹ Who owns what and who gets to exclude others from it? Professor Alexander and his progressive property colleagues would likely say that data “is more complex than the right to exclude standing alone.” This is because the creation of the data by the user and facilitation of that creation by the platform company is not so easily bifurcated. There is a certain level of “dependency and interdependency” in its creation that competes against the desire of each to exercise complete autonomy.

Rather than struggling against a traditionalist framework that ill-fits these complex, modern modes of property, the law should embrace a view of property that recognizes the context and complexity of data disputes, as this is needed to fully achieve the vision of human flourishing that Professor Alexander so elegantly sets forth. As the Supreme Court noted in *Carpenter*, “cell phones and the services they provide are ‘such a pervasive and insistent part of daily life’ that carrying one is indispensable to participation in modern society.”¹⁷⁰ Without a doubt, all can

¹⁶⁵ Alexander, *supra* note 158, at 761–62.

¹⁶⁶ Gregory S. Alexander, *The Complex Core of Property*, 94 CORNELL L. REV. 1063, 1070 (2009).

¹⁶⁷ *Id.*

¹⁶⁸ See *supra* Part II.A.

¹⁶⁹ See *supra* Part II.B.

¹⁷⁰ *Carpenter v. United States*, 138 S. Ct. 2206, 2210 (2018).

agree with the observations of Justice Gorsuch in his dissent when he stated: “Today we use the Internet to do most everything. Smartphones make it easy to keep a calendar, correspond with friends, make calls, conduct banking, and even watch the game.”¹⁷¹ And whether we like it or not, “[e]ven our most private documents—those that, in other eras, we would have locked safely in a desk drawer or destroyed—now reside on third party servers.”¹⁷² Can one really be said to exercise agency—to be a part of a community and have the ability to make reasoned choices about one’s life: to flourish—when each and every time we click a button, swipe about, or even put our cell phones in our pocket that we give away all things, big and small, about ourselves, where we go, our preferences, and even our most private moments? To flourish means to have some control, to believe there is some level of self-determination, that allows us to make meaningful choices—or, at least to know when certain choices are being made for us. As further expounded upon below, viewing data through a progressive property lens which recognizes the social obligations inherent in the collection and management of property can help achieve this balance when it comes to data.

B. Data and a Community of Rights

The idea of a community of rights when it comes to data is particularly helpful in advancing the notion of data as property. Professor Alexander draws upon Alan Gewirth’s work—and, in turn, that of Immanuel Kant—to explain that the rights of one person necessarily involve the recognition that others have rights as well. There is a sort of “mutuality of human rights” that serves as a symmetrical construction—“each person has rights to freedom and well-being against all other humans [and] every other human also has these rights against him, so that he has correlative duties toward them.”¹⁷³ This creates a community of rights which, in turn, creates community obligations as well. Alexander takes this idea one step further by arguing that valuing one’s own flourishing means to value the flourishing of others, as one is connected to the other.¹⁷⁴ And again, flourishing requires the recognition of community and the possession of the capabilities to make reasoned choices—in essence, to have agency in this world—about the direction of one’s life.¹⁷⁵

As part of this assertion that we must be normative committed to not only our own flourishing but also the flourishing of others is the idea of

¹⁷¹ *Id.* at 2262.

¹⁷² *Id.*

¹⁷³ Alexander, *supra* note 158, at 768–69 (citing ALAN GEWIRTH, THE COMMUNITY OF RIGHTS 305–06 (1996)).

¹⁷⁴ *Id.*

¹⁷⁵ *Id.*

unreciprocated sacrifices when it comes to property rights. In other words, “even if the persons to whom we give are the same as the persons from whom we previously received some benefit, what we give is often not the same as what we received.”¹⁷⁶ Indeed, the amount we give and the amount we receive in return can sometimes be quite different.¹⁷⁷ Alexander argues that, in fact, we do not give in order to necessarily receive the exact same in return: instead, “[t]he real basis of our obligation here is not reciprocity but dependency.”¹⁷⁸ As humans, “[w]e need to belong to such social networks for the development of certain essential human capacities,” and, moreover, “that dependence places on us an obligation to maintain those nurturing social networks.”¹⁷⁹

To bring the discussion back to data, consider membership in the digital community. As between users and platform companies, there is a mutuality of benefit. However, it should not be that one necessarily expects the same in return for what is given. A user of a particular service on a smart phone app may purchase that app for real money and may even expect that a certain level of directed advertising will be shown to him or her. But the user certainly does not anticipate that intimate information about his or her personal preferences, location, or associations will be bundled and sold to faceless parties across a wide-web of commercial relationships. While it may be true that the platform created the mechanism for the data to be created and processed into usable form, its entitlement to this data may indeed need to be sacrificed in some way in order to balance the community of rights between platforms and users. The platform benefits from being a part of the digital community and, by virtue of this, some form of sacrifice of its labors must be recognized in order to maintain the dignity, the autonomy, the trust—the flourishing—of the many users in this community. A pure quid-pro-quo is not always the sole basis of what we are due. Rather, “[w]hat we owe is as often as not determined by the needs of others rather than what we have received.”¹⁸⁰

One may argue that within this community of rights ecosystem a platform company should not be forced to abandon the fruits of its labor through a sacrifice of data use entitlements. This would be antithetical to property rights and fairness, some might say, as much work and resources went into the creation of the program or software at play. Yet, Professor Alexander so duly notes that “[t]here are many occasions in which property law protects owners incompletely” such as in the use of

¹⁷⁶ *Id.* at 770.

¹⁷⁷ *Id.*

¹⁷⁸ *Id.* at 771.

¹⁷⁹ *Id.*

¹⁸⁰ *Id.*

eminent domain when property law “requires the owner to sell an entitlement unwillingly and at an objectively set price.”¹⁸¹ While it is true that platform companies, like the cell phone companies in *Carpenter*, must have their rights protected in the interest of “fairness, individual respect[,]” and even in the dignity of the company’s labor itself, we must simultaneously “recognize that community membership involves the possibility of unreciprocated sacrifices.”¹⁸²

The practical implementation of such a theory into hard policy might very well be that tech companies, despite creating the processed data through their labor, cannot make unfettered use of it. Limitations on such use, including the ability of the user (from whose actions or preferences the data is derived) to deny such use altogether, may very well be the end result. On the other hand, there is a down-side balancing on the user’s side as well. If the data’s use serves a human flourishing goal for society as a whole—such as when aggregate consumer data can be used to guide better public health policies or provide consumers with a more competitive (and therefore open) market for the goods and services they desire—then the user’s entitlements should bend and bow. This is the balancing within the community of rights ecosystem that Professor Alexander elucidates—one where there is a mutuality of benefit but also occasion for unreciprocated sacrifices when community obligations require.

C. *Data as Governance Property*

A third way in which Professor Alexander’s work contributes to an optimal method of thinking about data as property is through the concept of governance rules. He explains in his 2012 work *Governance Property* that this idea arises in cases where there is multiple-ownership of property.¹⁸³ He explains that with property where there is a “fragmentation of various sorts of coincident rights” there subsequently arises “the need for norms that govern the exercise of those rights.”¹⁸⁴ Alexander is careful, however, to note that this is not a commons-type situation where the resource is open-access—in other words, governance property is a not a “kind of nonownership regime.”¹⁸⁵

¹⁸¹ *Id.* at 775. Professor Pollack suggests just such an application to data in his article *Taking Data*. See Pollack, *supra* note 38.

¹⁸² Alexander, *supra* note 158, at 771–72.

¹⁸³ Gregory S. Alexander, *Governance Property*, 160 U. PA. L. REV. 1853 (2012). Noting that “[g]overnance property institutions have proliferated in virtually every area of social life,” Professor Alexander gives examples in marriage/domestic partnership law, co-tenancies of homes and households, common interest communities, leaseholds, and corporate entities. See *id.* at 1860–63.

¹⁸⁴ *Id.* at 1856.

¹⁸⁵ *Id.* at 1857.

Data like the kind described in *Wayfair* and *Carpenter* is generated by a duality of efforts. Both the user's activities and the labor of the service provider combine to produce the data in some way or another. In the case of social media accounts, Facebook or Instagram provides the service that allows users to create an account, build a profile, and upload (or download) files. In turn, the user's activities, browsing habits, likes, and shares are captured by the platform and turned into useable data for advertising and other purposes. This is a joint effort that, in a governance context, creates the need for rules to recognize the mutuality of interests—a sort of co-tenancy. In other words, data is a form of what Professor Alexander calls governance property.

Several aspects of governance property can assist courts and lawmakers in thinking about structuring data property law. First, in governance property there are often vertical relationships, “meaning that some interest holders hold exclusive or greater control than others over the asset.”¹⁸⁶ In the data context, therefore, it is possible to think of both the user and the platform having an interest but not ones that are equal or durationally consistent. There may indeed be a “temporal division of interest” where the rights of the co-owners shift, change, or adjust over time.¹⁸⁷ Data property law might operate similarly. At the moment the data is created it may be that the user has the most control—being able to decide how it is used or how much of it can be processed for use by others. However, after consent is given or a certain period of time has passed, it might be that the platform is given more latitude. This idea of differing (and even changing) rights along a hierarchy and time horizon can help lead policy discussions on how best to balance the interests of the parties.¹⁸⁸

Within the context of governance property is the need to resolve disputes. One aspect of dispute that Professor Alexander raises is the need to resolve issues of “contributions for improvements and repairs to the asset.”¹⁸⁹ With data, should the platform's rights be given special accord since it is through its efforts that raw data relative to a user's activities are turned into functional information that can help the user access better information and be steered toward more optimal choices? Mediating these disputes is part of building the rules for particular governance property types. Resolving these disputes is, in turn, important because the rules of governance property are the foundation for human flourishing: bound up in the idea that “property serves multiple values

¹⁸⁶ *Id.* at 1885.

¹⁸⁷ *Id.* at 1886.

¹⁸⁸ *Id.*

¹⁸⁹ *Id.* at 1868.

and that these values are incommensurable.”¹⁹⁰ These values include personal autonomy, individual security, self-realization, fairness, and community.¹⁹¹ The collection and use of data must be driven by a property regime that mediates between the interests of users and providers because, without such a facilitation, these values would be undermined.

CONCLUSION

Treating data as a form of property is not just a wishful theory or a hypothetical for conjecture. In fact, it is starting to happen even now. The Supreme Court’s decisions in *Wayfair* and in *Carpenter* represent a robust move in this direction, although one that requires some unpacking and one that is in a relatively early stage of development. Not only can this movement be seen in the language that the Court employs, but it is also evident in the contours of the Court’s analysis of the issues.

Yet, at the same time that the law is embracing data as property, the foundations of such treatment remain relatively ethereal. What does it mean to say that data is property? How should we think about data as a type of asset like a car, a book, or other type of personalty? Can we use existing personal property constructs to understand data or do we have to branch off and develop something new? And, even if we do treat data as property, what significance does it have for how we create, alienate, and otherwise transact with our data and the data of others?

Many of these questions remain unanswered or at least not fully explained. As I have argued here, the work of Professor Alexander and others in the progressive/Aristotelian school of thought can provide the language that courts and policymakers need to build the property architecture of data. Guided by this way of thinking, we should not make choices about entitlements to data property through purely deductive or algorithmic reflection.¹⁹² Rather, these decisions should be “both principled and contextual, and should draw upon critical judgment, tradition, experience, and discernment.”¹⁹³ After all, data, like other types of property, “can render relationships within communities either exploitative and humiliating or liberating and ennobling.”¹⁹⁴ Data can be used to help or to harm, and because of this there must be rules that take into account these possible outcomes. The implication, then, is that data implicates values.¹⁹⁵ In some cases “these values promote individual interests,

¹⁹⁰ *Id.* at 1875.

¹⁹¹ *Id.*

¹⁹² Alexander et al., *supra* note 155, at 744.

¹⁹³ *Id.*

¹⁹⁴ *Id.*

¹⁹⁵ *Id.*

wants, needs, desires, and preferences.”¹⁹⁶ But in other cases, these values “promote social interests, such as environmental stewardship, civic responsibility, and aggregate wealth.”¹⁹⁷

Drawing upon Professor Alexander’s ideas, the notion of protecting privacy in data creates “moral demands and obligations that underlie judgments about the interests that the law should recognize as property entitlements.”¹⁹⁸ To quote the Justice Gorsuch in *Carpenter*, “Today we use the Internet to do most everything.”¹⁹⁹ Yet, the majority opinion noted, “[the] sort of digital data at issue—personal location information maintained by a third party—does not fit neatly under existing precedents.”²⁰⁰ Indeed, the law must adapt to deal with the rise of data and its ever-present shadow in American life. Failing to do so can lead us farther down an already dangerous path. Consider past instances, like that involving Henrietta Lacks, where courts were unwilling to use sound property law concepts to remedy past wrongs.²⁰¹

Property law can help do the work of theorizing data in a way that is useful when it comes to more concrete policy decisions about how data transactions should be fairly regulated. That is not to say that ownership as a notion should be tossed aside. But, as Professor Singer (another leader in the progressive property movement) notes, “[o]wners have obligations; they have always had obligations. We can argue about what those obligations should be, but no one can seriously argue that they should not exist.”²⁰² These obligations become all the more contextualized with data because of the mutuality of efforts, the multiplicity of parties, and larger way in which data can be wielded to shape society. These ideas, however, are not foreign to property law. American property law has always implicitly included “a robust social-obligation norm.”²⁰³ And it is through the work of Professor Alexander—whose influential career we celebrate in these pages—that the notion of a social obligation of data property can be systemically developed.

¹⁹⁶ *Id.* at 743.

¹⁹⁷ *Id.*

¹⁹⁸ *Id.*

¹⁹⁹ *Carpenter v. United States*, 138 S. Ct. 2206, 2262 (2018).

²⁰⁰ *Id.* at 2214.

²⁰¹ See *Moore v. Regents of the Univ. of Cal.*, 793 P.2d 479 (Cal. 1990); see also REBECCA SKLOOT, *THE IMMORTAL LIFE OF HENRIETTA LACKS* (2010).

²⁰² JOSEPH WILLIAM SINGER, *ENTITLEMENT: THE PARADOXES OF PROPERTY* 18 (2000).

²⁰³ Alexander, *supra* note 158, at 818–19.