PRIVATE LAW IN UNREGULATED SPACES

ELIZABETH A. ROWE*

 I express my appreciation to Guido Noto La Diega, Margaret Hu, Andrea Matwyshyn, Xuan-Thao Nguyen, Sharon Sandeen and participants at the 2023 Intellectual Property Scholars Conference at Cardozo Law School, the Scholars in Technology, Equity, and Policy Workshop, and Wake Forest School of Law faculty workshop for insights, comments, or conversations about the ideas expressed in earlier versions of this work. Thank you to Alice Ko, Kelvin Hawkins, and Alejandra Muniz for excellent research assistance.

INTRODUCTION

This Essay expounds on the outsized role of private law in governing ownership of new technologies and data. As scholars lament gaps between law and technology, and the need for government regulation in these various spaces,[1] private law has quietly intervened to essentially regulate key features related to ownership, control, and access. Whether such intervention is welcome, efficient, or effective probably depends on the context and is subject to debate. Nevertheless, this Essay provides an excellent illustration of the organic development of private ordering to occupy spaces left open by public law, and posits that the significance of this phenomenon, whether for better or worse, cannot be lost in the weeds.

More specifically, the way in which contract law and intellectual property law have coalesced to define and control data ownership is striking. As a threshold matter, it is property ownership that allocates control of and access to data resources and ultimately enables monetization and value in the marketplace.[2] This control extends to both the public and private spheres, and the attendant implications are far reaching.[3]

Building on my recent work,[4] this Essay will provide three exemplar contexts in which 'private law creep' has occurred, especially with respect to trade secrecy—the area of intellectual property law most likely to govern data transactions.[5] By scrutinizing implantable medical devices, facial recognition technology, and algorithmic models in the criminal justice system, one observation remains salient and pervasive: contracts rule. Despite the strong public interests that are implicated in these domains, none

---

1 *See, e.g.*, Susanna Bagdasarova, *Brave New World: Challenges in International Cybersecurity Strategy and the Need for Centralized Governance*, 119 PENN STATE L. REV. 1005 (2015); Urs Gasser, *Recoding Privacy Law: Reflections on the Future Relationship Among Law, Technology, and Privacy*, 130 HARV. L. REV. F. 61 (2016); Chris Laughlin, *Cybersecurity in Critical Infrastructure Sectors: A Proactive Approach to Ensure Inevitable Laws and Regulations Are Effective*, 14 COLO. TECH. L.J. 345 (2016); Mark D. Fenwick, Wulf A. Kaal, Erik P.M. Vermeulen, *Regulation Tomorrow: What Happens When Technology Is Faster than the Law?*, 6 AM. U. BUS. L. REV. 561 (2017).

2 *See, e.g.*, Abraham Bell & Gideon Parchomovsky, *Reconfiguring Property in Three Dimensions*, 75 U. CHI. L. REV. 1015, 1022 (2008) ("The property right must specify the owner . . . . Indeed, it is impossible to conceive of allocating property without specifying . . . ownership."); James Y. Stern, *Property's Constitution*, 101 CALIF. L. REV. 277, 294–95 (2013) (describing ownership as the "basic building block" of property); Jeffrey Ritter & Anna Mayer, *Regulating Data as Property: A New Construct for Moving Forward*, 16 DUKE L. & TECH. REV. 220, 247 (2018) (noting that control of data is the basis of asserting and transferring property rights over data).

3 *See infra* Section III.B.

4 Elizabeth A. Rowe & Nyja Prior, *Procuring Algorithmic Transparency*, 74 ALA. L. REV. 303 (2022); Elizabeth A. Rowe, *Regulating Facial Recognition Technology in the Private Sector*, 24 STAN. TECH. L. REV. 1 (2020) [hereinafter Rowe, *Regulating Facial Recognition Technology*]; Elizabeth A. Rowe, *Sharing Data*, 104 IOWA L. REV. 287 (2018) [hereinafter Rowe, *Sharing Data*].

5 *See infra* Section II.B.

of them are regulated on a federal level. Instead, rights of access and ownership are governed by private law.

For instance, manufacturers own the intellectual property in the software that runs patients' implantable medical devices, and they control who has access to the data and the level of access.[6] Patients do not have access, nor do they control what could happen to the information collected from their devices.[7]

With respect to facial recognition technology,[8] one of the biggest areas of concern for consumers is the collection of photos and biometric data used to create the various databases and algorithms both in the private sector and by the government.[9] Here again, private contracts define the rights and responsibilities.

Finally, in the criminal justice system,[10] many algorithmic models used, for instance, by law enforcement to make arrests and as evidence in court, are considered "black boxes," whose internal workings are kept secret.[11] These models use data in an unknown manner to produce results or predictions that appear facially neutral but may actually yield discriminatory results.[12] Yet contracts shield these models from scrutiny, and criminal defendants are unable to challenge potential defects.[13]

Contracts have come to facilitate property rights in the management of data resources in almost unbounded fashion. In so doing, contracts effectively yield an even stronger property right than that associated with tangible property. Though contracts are no stranger to property law transactions, in the context of new technologies and intangible goods, I posit that we have a new formulation for creating property:

Intellectual property + Contracts = Property squared.

The potential significance of this equation is that, unlike with real property—where ownership comes with outer limits or guardrails such as

---

6 *See infra* Section I.B.1.

7 *See infra* Section I.B.1.

8 *See infra* Section I.B.2.

9 *See* Kashmir Hill & Aaron Krolik, *How Photos of Your Kids Are Powering Surveillance Technology*, N.Y. TIMES (Oct. 11, 2019), https://www.nytimes.com/interactive/2019/10/11/technology/flickr-facial-recognition.html [https://perma.cc/Q29X-ZYU3].

10 *See infra* Section I.B.3.

11 The issue of the "black box" has been ongoing for over a decade. *See, e.g.*, Elizabeth A. Rowe, *Striking a Balance: When Should Trade-Secret Law Shield Disclosures to the Government?*, 96 IOWA L. REV. 791, 826–35 (2011) (addressing when the government can request disclosure of "black box" algorithms).

12 *See* Anupam Chandler, *The Racist Algorithm?*, 115 MICH. L. REV. 1023, 1024–25 (2017) (noting that because "[e]ven a transparent, facially neutral algorithm can still produce discriminatory results," we may assume that algorithms are "deeply suffused with invidious discrimination").

13 *See infra* Section I.B.3.

public registries, zoning regulations, and other public policy exceptions[14]—data resources in new technologies lack any such limits.

The Essay argues that owners, through contractual provisions, reserve for themselves very broad powers to control a wide range of activities and behaviors relating to data, particularly its accessibility.[15] As such, contracts create de facto property rights, even though contracts themselves are not property.[16] Thus, the declaration of ownership, coupled with courts' broad enforcement of such contract terms,[17] creates a property right or, at a minimum, a quasi-property right, that then coalesces with and augments the accompanying intellectual property rights.

Consequently, the power and discretion to limit access in whatever way an owner chooses, without checks and balances from public policy exceptions, has caused substantial tension with public values.[18] Moreover, as some scholars have noted, there is a public-private vulnerability dynamic at play, especially as it concerns consumers with a power disparity.[19] As the exemplar illustrations reveal, those concerns are especially challenging in public-private partnerships—an increasingly common business model for government acquisition of new technologies.[20]

Moreover, just as contracts bolster property rights by giving owners broad rights over data, they also tend to simultaneously disclaim liability.[21] If one considers the public interest and the public law values embedded in accountability, is this normatively a sound ideal? Is the issue of harm likely to be a touchstone that ultimately exposes private law's existence without boundaries? Should other areas of private law (like tort law) serve as a stopgap in the absence of public law setting exceptions and guardrails? The Essay probes these complex questions and lays a foundation for further grappling with these issues.

---

14 *See generally* Jonathan Remy Nash & Stephanie M. Stern, *Property Frames*, 87 WASH. U. L. REV. 449 (2010).

15 *See generally* Guido Noto La Diega & Cristiana Sappa, *The Internet of Things at the Intersection of Data Protection and Trade Secrets. Non-Conventional Paths to Counter Data Appropriation and Empower Consumers*, 3 EUR. J. CONSUMER L. 419 (2020).

16 *See, e.g.*, Lashbrook v. Oerkfitz, 65 F.3d 1339, 1345 (7th Cir. 1995) ("An explicit contract can create such property rights."); Lim v. Cent. DuPage Hosp., 871 F.2d 644, 648 (7th Cir. 1989) ("Contracts can create property rights, but a contract that creates merely a right to procedure does not create a property right within the meaning of the due process clause."); YORAM BARZEL, ECONOMIC ANALYSIS OF PROPERTY RIGHTS 91 (2d ed. 1997) (noting that vast majority of property rights are created by contract).

17 *See infra* note 141 and accompanying text.

18 *See infra* Section III.B.

19 *See* Andrea M. Matwyshyn, *CYBER!*, 2017 BYU L. REV. 1109, 1190 (2018) (noting that because the "current structures of vulnerability indexing are completely opaque to consumers," there needs to be a "consumer-usable version of vulnerability information").

20 *See infra* Section III.B.2.

21 *See infra* Section III.C.

The question of public regulation is a complex and highly nuanced issue, and I take no specific normative stance on where and whether limits should exist. Rather, this Essay unveils the legal landscape that has emerged through private law in the absence of such public limits. Thus, private law has become the de facto regulatory framework for new technologies, including artificial intelligence (AI), that continue to rely extensively on data resources. For better or worse, ownership of and access to the data in these technologies are largely determined by private contracts among businesses, notwithstanding, for instance, one's constitutional rights (as with defendants in the criminal justice system)[22] or one's privacy rights (as with biometric data and implantable medical devices).[23]

Finally, rather than offering any specific prescriptions, I outline high-level structural responses to some of the concerns arising from this development. Using the European Union as a point of contrast,[24] I offer another lens from which to think about the role of public law in regulating new technologies. This lens could support rethinking how or whether jurisdictions in the United States could choose to expand public law to reach or modify contractual agreements regarding ownership. Further, in the absence of public law expansion (or even in conjunction with it), other areas of private law, in particular tort law, could be modified to address and assign duties and liabilities for those areas where public law is silent or insufficient.

Part I begins by defining the data resources that are the subject of this Essay, and introduces the exemplars. Part II focuses on the significance of data's status as property, and the critical importance of that designation to the privileges of ownership.

Part III turns to the core of this Essay's objective by discussing how contracts epitomize the reign of private law in spaces where public law has been slow to enter. The section describes the use of contracts to define ownership and the tensions that result, especially when public values are at odds with transactions dominated by private law. Moreover, it explores the paradox by which contracts allow owners to bolster their property rights while simultaneously disclaiming liability for harm resulting from the processing or outputs of data resources within their control.

Finally, while maintaining its perspective on the structural interaction between public and private law, Part IV considers possible structural responses to some of the concerns that have been identified. It begins with a contrasting public law approach to that which the United States has adopted, by looking at relevant pending and recently passed legislation for new

---

22 *See* Rowe & Prior, *supra* note 4, at 333 (noting that "many defendants have been unsuccessful in challenging forensic algorithm use without disclosure as a due process violation.").

23 *See infra* Section I.B.

24 *See infra* Section IV.A.

technologies in the European Union, especially for AI. It proceeds to suggest that jurisdictions in the United States could choose to expand public law to reach or modify contractual agreements regarding ownership. It further probes the potential role of tort law to address and assign duties and liabilities where public law has been silent.

I
DATA RESOURCES

In keeping with its propertization theme, this Essay envisions and operationalizes data resources (data) broadly. The term is inclusive of Big Data, but not limited to it, recognizing that with continuing advancements in technology, algorithmic models that process raw data into outputs of value exist ubiquitously and in innumerable contexts. Thus, the broad-stroke approach is intentional. Moreover, it is consistent with the Essay's paradigm of treating data as symbolic of the kinds of intangible goods (created by ever-evolving new technologies) which public law has yet to regulate or to regulate effectively.

A. More than Big Data

Several years ago, the phrase Big Data entered our national lexicon.[25] Traditional electronic databases and datasets gave way to complex "high-volume, high-velocity, and/or high-variety information assets that demand[ed] cost effective, innovative forms of information processing."[26] Since then, Big Data, including associated processing tools like artificial intelligence, machine learning, and the various algorithmic models that turn raw data into consumable products, have become ubiquitous in our economy and across every sector.[27] Indeed, data has been described as "the new oil"[28] and "the lifeblood of today's economy."[29] In part, and perhaps most significantly, this is because as we have embraced a sharing economy, and data facilitates business transactions.[30]

---

25 *See* Neil M. Richards & Jonathan H. King, *Big Data Ethics*, 49 WAKE FOREST L. REV. 393, 403 (2014) ("A new era of big data began when companies began to gather and analyze large amounts of information from internal and external sources.").

26 *Big Data*, GARTNER INFO. TECH. GLOSSARY, https://www.gartner.com/en/information-technology/glossary/big-data [https://perma.cc/76TE-FKR9].

27 *See* Ruth L. Okediji, *Government as Owner of Intellectual Property? Considerations for Public Welfare in the Era of Big Data*, 18 VAND. J. ENT. & TECH. L. 331, 334 (2016) (noting that data and algorithmic tools are a "critical new frontier and resource for innovation").

28 Perry Rotella, *Is Data the New Oil?*, FORBES (Apr. 2, 2012, 11:09 AM), https://www.forbes.com/sites/perryrotella/2012/04/02/is-data-the-new-oil [https://perma.cc/7PW6-ED9Y].

29 Heather Payne, *Sharing Negawatts: Property Law, Electricity Data, and Facilitating the Energy Sharing Economy*, 123 PENN STATE L. REV. 355, 361 (2019).

30 *Id.* at 360.

While raw data by itself may have little value or significance, in context, and with the appropriate algorithmic models, it can be transformed into something of tremendous value.[31] As one commentator noted, "Data is just like crude [oil]. It's valuable, but if unrefined it cannot really be used. It has to be changed into gas, plastic, chemicals, etc to create a valuable entity that drives profitable activity; so [too] must data be broken down [and] analyzed for it to have value."[32] The following Section explores the ways in which data can be transformed into useful and valuable tools for consumers.

B. Data in Context—Three Examples

To orient the reader, this section will provide three specific examples to illustrate the kinds of unregulated uses of data that have contributed to my grappling with the larger question addressed in this Essay. Namely, to what extent has private law played an outsized role in regulating spaces where public law has left a void? These illustrations arise from prior work on the use of data in various contexts, thus the brevity with which they are described below is by design.[33] They are intended to provide concrete exemplars of the use of data in discrete and diverse contexts, none of which are regulated, and all of which rely heavily on private law regulation.

1. Implantable Medical Devices[34]

Modern implantable medical devices are now relatively commonplace.[35] Among the more common implantable devices are pacemakers that treat heart conditions and control abnormal heart rhythms.[36] They do so by delivering electrical pacing pulses to the heart.[37] Implantable defibrillators also deliver electrical energy to the heart to control excessively rapid heart rates.[38]

These devices rely on and produce data. Implantable defibrillators and pacemakers contain a significant amount of data about the patient's heart,

---

31 *See* Noto La Diega & Sappa, *supra* note 15, at 440 ("Valuable knowledge may derive from data mining and aggregation of data that is accumulated over time from multiple sources.").

32 Michael Palmer, *Data Is the New Oil*, ANA BLOGS (Nov. 3, 2006), https://ana.blogs.com/maestros/2006/11/data_is_the_new.html [https://perma.cc/KTL3-VAVK].

33 Interested readers are encouraged to review the papers associated with each example for further edification, and citations are provided.

34 *See generally* Rowe, *Sharing Data*, *supra* note 4 (noting that while a patient does not have direct access to the data generated by an implantable medical device, that very information may be accessible to others).

35 James Williams & Jens Weber-Jahnke, *Regulation of Patient Management Software*, 18 HEALTH L.J. 73, 83 (2010).

36 *Id.*

37 Data Logging Sys. for Implantable Med. Device, U.S. Patent No. 6,628,985 (filed Dec. 18, 2000) (issued Sept. 30, 2003).

38 *Id.*

and this data can only be obtained by the patient during an office visit.[39] None of the data is available to a patient in real time.[40]

These medical devices represent a complex web of data inputs and outputs in the most personal and private context—from within a patient's body. In general, the network that allows data to flow in and out might include a device in the patient (hardware), software that runs the device, data from the patient's body going into the device, data outputs from the device, other hardware that communicates with the device, and software that facilitates that communication. There are also device programmers that transfer information from the implanted device to the manufacturers' systems, and information can then be transferred to the medical provider.[41]

The security of this data is of utmost importance, and intellectual property protection along with contractual terms are integral to facilitating these transactions. For instance, passwords and encryption protect patient data, as well as the data transfers to the manufacturer.[42] Trade secrecy also protects data that is stored and collected, as well as the codes to access or unlock data.[43]

Because manufacturers own the intellectual property rights in both the software and in the data generated from the patient, they can control who has access to the data and the level of access.[44] Patients do not have access to the data, and reports generated from the data are provided only to the patient's physician or medical facility.[45] Nor do patients control what could happen to the information collected from their devices.[46] Furthermore, there are no regulations in the United States that mandate access.[47]

---

39 *See* David Lee Scher, *Data from Implantable Defibrillators and Pacemakers: The World's Best Kept Secret*, DIGIT. HEALTH CORNER (Jan. 30, 2012), https://davidleescher.wordpress.com/2012/01/30/data-from-implantable-defibrillators-and-pacemakers-the-worlds-best-kept-secret [https://perma.cc/6HB2-8GPW].

40 *See id*. (noting that the process required to obtain data from the devices occurs during an office visit or remotely).

41 ADVANCED MED. TECH. ASS'N, LONG COMMENT REGARDING A PROPOSED EXEMPTION UNDER 17 U.S.C. § 1201, at 4 (2015), https://copyright.gov/1201/2015/comments-032715/class%2027/AdvaMed_Class27_1201_2014.pdf [https://perma.cc/L5J5-VMCB].

42 *Id*. at 5.

43 *See infra* Section II.B.

44 Rowe, *Sharing Data*, *supra* note 4, at 297.

45 *Id*. at 295.

46 *See infra* Section III.B.1.

47 Compare with the European Union, where the Medical Device Regulation (MDR) clarifies that the General Data Protection Regulation (GDPR) applies to data generated by medical devices. Sarita Lindstad & Kaspar Rosager Ludvigsen, *When Is the Processing of Data from Medical Implants Lawful? The Legal Grounds for Processing Health-Related Personal Data from ICT Implantable Medical Devices for Treatment Purposes Under EU Data Protection Law*, 31 MED. L. REV. 317, 319 (2022).

2. Facial Regulation Technology[48]

The use of facial recognition technology (and other biometric technologies) has become widespread. Virtually all consumers encounter these technologies in daily life.[49] Even government agencies are "consumers" of the technology.[50] Indeed, government agencies (federal and state) are probably the most extensive users of facial recognition technology in the United States today.[51] Consequently, the use of facial recognition technology, especially in the criminal justice context, has received extensive treatment in the literature.[52]

Similarly, facial recognition technology is being used by businesses for a wide range of purposes, from employee time-keeping to manufacture and sales of consumer products and services.[53] Businesses credit the technology for improving efficient and effective practices in many aspects of business, from marketing to security.[54] Additionally, developers use facial recognition technology to create consumer conveniences in smart phones, smart homes, and even for child monitoring.[55] Admittedly, facial recognition technology offers beneficial uses to businesses and consumers alike, and for the most part have been welcomed as convenient tools for everything from unlocking our iPhones to moving through lines more quickly.

---

48 *See generally* Rowe, *Regulating Facial Recognition Technology*, *supra* note 4 (addressing the regulation of facial recognition technology in the civil and commercial sector).

49 *Id*. at 8.

50 *Id*. at 9.

51 *Id*. at 15.

52 *See, e.g.*, Katelyn Ringrose & Divya Ramjee, *Watch Where You Walk: Law Enforcement Surveillance and Protester Privacy*, 11 CALIF. L. REV. ONLINE 349 (2020); Katelyn Ringrose, Essay, *Law Enforcement's Pairing of Facial Recognition Technology with Body-Worn Cameras Escalates Privacy Concerns*, 105 VA. L. REV. ONLINE 57 (2019); Mariko Hirose, *Privacy in Public Spaces: The Reasonable Expectation of Privacy Against the Dragnet Use of Facial Recognition Technology*, 49 CONN. L. REV. 1591 (2017).

53 Fambrough v. Uber Techs., Inc., No. 4:19-cv-0398-DGK, 2019 WL 2411442 (W.D. Mo. June 7, 2019) (considering a suit brought by an employee of Uber whose driving account was deactivated as a result of the facial recognition technology wrongly reporting that the employee was using someone else's photo for verification).

54 *See* Rowe, *Regulating Facial Recognition Technology*, *supra* note 4, at 9–11 (discussing beneficial uses of facial recognition technology to businesses by allowing identification of consumer trends and shoplifters).

55 *See, e.g.*, Amy Gamerman, *Home Is Where They Know Your Name (and Face, Hands and Fingerprints)*, WALL ST. J. (June 20, 2019, 12:22 PM), https://www.wsj.com/articles/home-is-where-they-know-your-name-and-face-hands-and-fingerprints-11561047729 [https://perma.cc/A3AW-W8FL] (discussing how companies are increasingly building off of biometric technology in order to not only personalize experiences for private homeowners but also increase the marketability and resale value of homes); Julie Jargon, *Facial Recognition Tech Comes to Schools and Summer Camps*, WALL ST. J. (July 30, 2019, 12:19 PM), https://www.wsj.com/articles/facial-recognition-goes-to-camp-11564479008 [https://perma.cc/J7U4-AZ5C] (describing facial recognition technology that allows parents to quickly review group photos that include their child instead of sorting through all photos).

How companies are collecting data from employees or consumers to create or implement these products and services has raised concerns and often implicates privacy issues.[56] For example, the collection of photos and biometric data used to create the various databases and algorithmic models that support facial recognition technology, has raised questions.[57] Some worry that companies are free to collect photos and create large databases that can be shared with other companies. As an example, MegaFace collected millions of faces from Flickr to develop and train its algorithm.[58] Flickr users were not aware that their photos, including those of minors, were being used.[59]

There is currently no federal regulation of biometric data in the United States.[60] While a few states have stepped in with their own regulations,[61] government use remains unregulated.[62] Some believe permissive privacy laws in the United States have fostered companies' liberal use of people's faces without their knowledge to build and grow facial recognition technology.[63] At present, most Americans have limited recourse for uses of their photos and biometric data, unless they are from Illinois and are protected by the Biometric Information Privacy Act (BIPA).[64] Indeed, it is questionable whether photos themselves, as opposed to scans of the photos,

56 *See* Rowe, *Regulating Facial Recognition Technology*, *supra* note 4, at 25–27 (highlighting the concern that without privacy regulations, companies are free to collect a large amount of data that can be shared with other companies).

57 *See* Hill & Krolik, *supra* note 9 (noting that privacy law in most states is permissive and has not prohibited companies from collecting and using photos of individuals without their permission).

58 *Id*.

59 Mary Meisenzahl, *If You Uploaded Photos of Your Kids to Flickr They Might Have Been Used to Train AI*, BUS. INSIDER (Oct. 17, 2019, 12:37 PM), https://www.businessinsider.com/flickr-photos-kids-train-ai-facial-recognition-database-megaface-report-2019-10 [https://perma.cc/5TAP-JBTS].

60 Rowe, *Regulating Facial Recognition Technology*, *supra* note 4, at 34.

61 *See id*. at 39–40 ("For example, Connecticut, Iowa, Nebraska, North Carolina, Oregon, Wisconsin, and Wyoming have regulated the collection of biometric information by defining 'personal information' in data security breach notification laws to include some types of biometric data.").

62 *Id.* at 34.

63 *See infra* Section III.B.2.

64 740 ILL. COMP. STAT. 14/15, 14/20 (2023) (establishing requirements for retention, collection, disclosure, and destruction of biometric information, and granting a private right of action for individuals to bring a claim against a private entity for violations thereof).

are covered by BIPA.[65]

3. Algorithmic Models in Criminal Justice[66]

Forensic technologies that incorporate data and algorithms are utilized in various ways throughout the criminal justice system. These include such applications as facial recognition, DNA analysis, fingerprint analysis, and ballistic analysis.[67] They are also used at all stages of the criminal justice process, including at the law enforcement level, during trial as evidence, and for sentencing determinations.[68] However, despite the well-intentioned motivations to adopt such technologies, one criticism is that algorithmic implementation in decision-making can occur before rigorous testing has been conducted, and without independent evaluation.[69]

It is axiomatic that algorithms cannot operate effectively without sufficient data.[70] Thus, a prerequisite to all these systems is the input of specific variables and the selection of precise mathematical relationships between the variables.[71] When machine learning is involved, artificial intelligence allows algorithms to discover correlations "on their own" only after they have been programmed to do so.[72] In the criminal justice context, risk assessment software, for example, considers factors such as

---

65 *See id.* at 14/10 (excluding photographs from the definition of "biometric identifier" protected under the Act).

66 *See generally* Rowe & Prior, *supra* note 4 (noting that an increasing number of jurisdictions continue to adopt algorithmic models in various criminal justice contexts in order to optimize resources, reduce bias, and promote justice).

67 *See, e.g.*, U.S. GOV'T ACCOUNTABILITY OFF., FORENSIC TECHNOLOGY: ALGORITHMS USED IN FEDERAL LAW ENFORCEMENT 5–11, https://www.gao.gov/assets/gao-20-479sp.pdf [https://perma.cc/UXQ9-K7LH]; Rebecca Wexler, *Life, Liberty, and Trade Secrets: Intellectual Property in the Criminal Justice System*, 70 STAN. L. REV. 1343, 1363–64 (2018).

68 *See, e.g.*, Alex Chohlas-Wood, *Understanding Risk Assessment Instruments in Criminal Justice*, BROOKINGS (June 19, 2020), https://www.brookings.edu/research/understanding-risk-assessment-instruments-in-criminal-justice [https://perma.cc/4HHM-E5PA]; Wexler, *supra* note 67, at 1356–71.

69 *See, e.g.*, Robert Brauneis & Ellen P. Goodman, *Algorithmic Transparency for the Smart City*, 20 YALE J.L. & TECH. 103, 152 (2018) (describing researchers' inability to obtain records about the creation and implementation of algorithms already in use in twenty-three states); Kashmir Hill, *Wrongfully Accused by an Algorithm*, N.Y. TIMES (Aug. 3, 2020), https://www.nytimes.com/2020/06/24/technology/facial-recognition-arrest.html [https://perma.cc/RNA3-TD5H] (describing facial recognition firm DataWorks's lack of accuracy or bias testing for its algorithm, which has been on the market since 2005).

70 *See generally* Willem Sundblad, *Data Is the Foundation for Artificial Intelligence and Machine Learning*, FORBES (Oct. 18, 2018, 10:30 AM), https://www.forbes.com/sites/willemsundbladeurope/2018/10/18/data-is-the-foundation-for-artificial-intelligence-and-machine-learning/#4bd8c64051b4 [https://perma.cc/94CW-BAXW] ("[D]ata is both the most underutilized asset of manufacturers and the foundational element that makes AI so powerful.").

71 Cary Coglianese & Lavi M. Ben Dor, *AI in Adjudication and Administration*, 86 BROOK. L. REV. 791, 796 (2021).

72 *Id.*

"socioeconomic status, family background, neighborhood crime, employment status," education, employment history, and demographic information to generate a high or low score with specific percentages based on an individual's criminal risk.[73]

Statisticians use these factors, along with sentencing data and historical recidivism rates, to identify which variables occur in the most relevant cases, and those data points are then used to create predictive models.[74] They then reverse the process to find the selected variables in new cases, which, if successful, can then be applied to active cases to generate recidivism risk scores.[75] Like all statistical models, these can be complex, and the quality of the algorithmic model will depend on many factors, including sample size, record completeness, and modeling strategy.[76]

In the criminal justice system, government agencies usually acquire these technologies, through a procurement process, from private entities. Through these contracts, the entities generally assert full ownership and control over the technology, including their data and algorithms. This includes the right to exclude. As such, the algorithmic models become "black boxes," whose internal workings are protected as trade secrets.[77] Ultimately, in such cases, criminal defendants are unable to challenge possible algorithmic model defects without some form of access to the underlying system or its data.[78]

II
PROPERTY & ITS SIGNIFICANCE

While the advancements and usefulness of data in all of its applications are impressive, as the above examples demonstrate, it is data's legal status as property that makes it an even more formidable asset to its owners and

---

73 *AI in the Criminal Justice System*, ELEC. PRIV. INFO. CTR., https://epic.org/algorithmic-transparency/crim-justice [https://perma.cc/QF5N-N6M7].

74 ANGÈLE CHRISTIN, ALEX ROSENBLAT & DANAH BOYD, COURTS AND PREDICTIVE ALGORITHMS 4 (2015), https://www.law.nyu.edu/sites/default/files/upload_documents/Angele%20Christin.pdf [https://perma.cc/XY96-EU9J].

75 *Id.*

76 *See, e.g.*, DAVID STEINHART, ANNIE E. CASEY FOUND., JUVENILE DETENTION RISK ASSESSMENT: A PRACTICE GUIDE TO JUVENILE DETENTION REFORM 52–53 (2006), https://www.aecf.org/m/resourcedoc/aecf-juvenileddetentionriskassessment1-2006.pdf [https://perma.cc/GM9M-JE4V] (noting that protocol for detention risk assessment must include a minimum sample size of 300 total cases, a test duration long enough to collect the minimum number of cases, and potentially supplemental documentation, such as police reports).

77 The issue of the "black box" has been ongoing for over a decade. *See, e.g.*, Rowe, *supra* note 11, at 826–35 (addressing when the government can request disclosure of "black box" algorithms).

78 *See* Rowe & Prior, *supra* note 4, at 324 ("[C]ourts have generally been unwilling to provide defendants with access to the algorithms.").

creators.[79] Indeed, ownership can only be established if there is a property right.[80] Even considering our underlying public policy of information diffusion, if data is not owned, then it belongs to the public, especially once it is disclosed. [81] Further, if it is not property, there can be no claim if it is misappropriated.Ownership of data looks a lot like it does for tangible goods and physical property, but there are major differences.[82] Key among those is that data is governed by *intellectual* property and that ownership of data is largely unregulated—leaving a void that has been captured by private law. What are the implications of that for owners, consumers, and public interest?

The significance of data as property cannot be overstated. It is this status that, coupled with contract law, makes it what I coin "property squared." It is also its treatment as intellectual property rather than traditional property that raises the biggest questions for regulation and accountability.

A. Tangible Property

Before elaborating on these distinctions and their implications, it is worth beginning with a brief primer of what property means and how we have come to conceive of real and personal property as distinct from intellectual property. Property in all its forms is a valuable resource. We typically categorize these property resources as tangible, including real (e.g., land and things growing on and attached to land)[83] and personal (e.g., not real property, is movable, and can be owned),[84] and intellectual property.[85] Intellectual property covers intangible property (like data) that comprise "commercially valuable product of the human intellect."[86]

In all its forms, crucial to the conception of property is the right to possess, use, control, or exclude others from one's property.[87] Whether supported by such property theories as the "tragedy of commons,"[88]

---

79 *See* James Grimmelmann & Christina Mulligan, *Data Property*, 72 AM. U. L. REV. 829, 844 (2023) ("Modern scholars who have considered the question widely agree that intangible things can be property.").

80 *See supra* note 2 and accompanying text.

81 *See generally* SHARON K. SANDEEN & ELIZABETH A. ROWE, TRADE SECRET LAW INCLUDING THE DEFEND TRADE SECRETS ACT OF 2016 IN A NUTSHELL § 2.9.1 (2d ed. 2018) (discussing the protection of information in the public domain).

82 *See* Grimmelmann & Mulligan, *supra* note 79, at 842–43 (discussing property in intangible things in the U.S. and civil law systems based on Roman law and comparing German law as an outlier).

83 *Real Property*, BLACK'S LAW DICTIONARY (10th ed. 2014).

84 *Personal Property*, BLACK'S LAW DICTIONARY (10th ed. 2014).

85 *See Intellectual Property*, BLACK'S LAW DICTIONARY (10th ed. 2014) (noting intellectual property can be "in a concrete or abstract form").

86 *Id*.

87 *See* Payne, *supra* note 29, at 379.

88 For more information about the "tragedy of the commons," see Garrett Hardin, *The Tragedy of the Commons*, 162 SCI. 1243, 1244 (1968).

Lockean, or economic theories of property rights, exclusivity and control underlie an object's status as property.[89] Moreover, per the Blackstonian conception of property, the owner has sole and despotic dominion over their property (subject to specifically delineated exceptions—the very kinds of exceptions that I suggest are missing for intangible goods like data).[90]

It is also worth noting that in terms of market transactions, with real property there are requirements that such transactions are recorded and available to the public.[91] This is not the case with intangible property; not only is there generally no such requirement[92] but as discussed below, owners could require secrecy regarding the very existence of the transaction.[93] Overall, contract law, in the absence of such guardrails, permits the owner to exert relatively unbounded control.

In the United States, property is deeply ingrained in our economy. In a capitalist system, the favored mode of production is naturally "based on private control of the means of production and the extraction of surplus to maximize profits."[94] Thus, it should come as no surprise that property rights in intangible intellectual goods have tremendous importance. So it was highly predictable that contract law has come to facilitate and expand those property rights, and that private law is becoming our de facto legal scheme organizing legal relationships for data and these new technologies.

B. Intellectual Property

By my formulation, intellectual property plus contracts equals property squared. Thus, the use of intellectual property law bolstered by contract law (all private law) to govern data results in even stronger property rights than what property law alone would provide.[95] In other contexts, we have seen a

---

89 *See e.g.*, Julia E. Cohen, *What Kind of Property Is Intellectual Property?*, 52 HOUS. L. REV. 691, 699 (2014) (detailing "tragedy of commons" and other economic theories about why exclusivity is an essential feature of property rights); John F. Henry, *John Locke, Property Rights, and Economic Theory*, 33 J. ECON. ISSUES 609 (1999) (comparing Locke's theory of property with other neoclassical theories that are ostensibly derived from Locke, focusing particularly on scarcity, efficiency, exchange, and optimizing behavior).

90 *See* 2 WILLIAM BLACKSTONE, COMMENTARIES *2 (detailing exceptions including those things that can only be owned temporarily, such as light coming through a window, or those things which should be maintained by the state, such as forests).

91 *See* Charles Szypszak, *Real Estate Records, the Captive Public, and Opportunities for the Public Good*, 43 GONZ. L. REV. 5, 23–24 (2007/08) (describing state recording statutes as "the core of real estate conveyance law").

92 *See* Grimmelmann & Mulligan, *supra* note 79, at 850–51 (differentiating nonrival data from rival intangibles that are sometimes subject to registration, because exclusive ownership over non-rival data can only be achieved by keeping it secret).

93 *See infra* Section III.A.

94 Cohen, *supra* note 89, at 698.

95 *See, e.g.*, Raymond T. Nimmer, *Breaking Barriers: The Relation Between Contract and Intellectual Property Law*, 13 BERKELEY TECH. L.J. 827, 827 (1998) ("In the digital world, the

similar trend with patent law and licensing,[96] as well as in other areas of intellectual property such as copyright law[97] and trademark law.[98] This Essay focuses on intellectual property rights through trade secrecy, as it is the area most likely to govern private ownership and property rights in data.[99] This is especially so in the context of the contracts and private law transactions with which this Essay is concerned.

It is well settled that trade secrets are property. A case that is frequently cited for the proposition that trade secrets are a form of private property is

---

contract rather than the underlying property law defines the product."); Deepa Varadarajan, *The Trade Secret-Contract Interface*, 103 IOWA L. REV. 1543, 1590 (2018) ("Trade secret law is dependent on, but also potentially undermined by, contract law.").

96 *See, e.g.*, ProCD, Inc. v. Zeidenberg, 86 F.3d 1447, 1454 (7th Cir. 1996) ("Although Congress possesses power to preempt even the enforcement of contracts about intellectual property . . . [,] courts usually read preemption clauses to leave private contracts unaffected."); Kimble v. Marvel Ent., LLC, 576 U.S. 446, 453–54 (2015) (discussing various ways that a patent licensor and licensee can structure private agreements to get around certain patent law rules restricting royalties); Aronson v. Quick Point Pencil Co., 440 U.S. 257, 264–65 (1979) (refusing to relieve patent licensee of its contractual obligations); Hartell v. Tilghman, 99 U.S. 547, 548 (1878) (finding no jurisdiction in federal court "where the defendant admits the validity and his use of the plaintiff's letters-patent, and a subsisting contract is shown governing the rights of the parties in the use of the invention"); Elizabeth A. Rowe, *Patents, Genetically Modified Foods, and IP Overreaching*, 64 SMU L. REV. 859, 864 (2011) (noting the expansion of intellectual property protection afforded by the Plant Variety Protection Act, which extended patent-like protections to hybrid-seed companies, a more powerful protectant than the trade-secret protection they enjoyed prior to its passage).

97 *See, e.g.*, Guy A. Rub, *Contracting Around Copyright: The Uneasy Case for Unbundling of Rights in Creative Works*, 78 U. CHI. L. REV. 257, 279 (2011) (noting that the power of contract law may disturb the balance that the Copyright Act tried to achieve); David Nimmer, Elliot Brown & Gary N. Frischling, *The Metamorphosis of Contract into Expand*, 87 CALIF. L. REV. 17, 24 (1999) ("[O]wnership and exploitation of copyright are structured at every turn by contract."); Guy A. Rub, *Copyright Survives: Rethinking the Copyright-Contract Conflict*, 103 VA. L. REV. 1141, 1156 (2017) ("[C]ontracts allow creators to regulate the use of ideas, which are not protected by copyright."); *ProCD*, 86 F.3d at 1450 (confirming that courts treat licenses as contracts, leaving aside any potential legal differences); 4DD Holdings, LLC v. United States, 169 Fed. Cl. 164, 179 (2023) (holding that a contractual release may not bar a copyright claim). Note, however, that copyright law itself does not create a property interest as broad as that created by trade secrecy, because while it prevents others from engaging in certain acts relative to the copyrighted material, it does not create affirmative rights that would, for instance, control access. *See* Grimmelmann & Mulligan, *supra* note 79, at 833.

98 *See, e.g.*, Marco's Franchising, LLC v. Soham, Inc., 365 F. Supp. 3d 891, 899 (N.D. Ohio 2019) (holding that under the terms of the contract the defendant's continued use of the plaintiff's trademark after the termination of the franchise agreement was unauthorized); Young Again Prods., Inc. v. Acord, 307 F. Supp. 2d 713, 715, 718 (D. Md. 2004) (finding federal jurisdiction for suit alleging use of various trademarked products without authorization, arguing that the existing contract between the parties was breached and did not constitute authorization).

99 *See generally* ROGER M. MILGRIM & ERIC E. BENSEN, 1 MILGRIM ON TRADE SECRETS § 2.01 (1967) (addresses intellectual property rights as a means to protect and utilize trade secrets and other intangible property); Michael P. Simpson, *The Future of Innovation: Trade Secrets, Property Rights, and Protectionism—An Age-Old Tale*, 70 BROOK. L. REV. 1121, 1122 (2005) (noting the expanding protection in trade secrets and intellectual property and their outsized benefit to "industry" at the detriment of "society").

Ruckelshaus v. Monsanto Co.[100] In *Ruckelshaus*, the Supreme Court considered whether certain provisions of the Federal Insecticide, Fungicide, and Rodenticide Act were unconstitutional.[101] Monsanto argued that the provisions of the law that required it to disclose certain information and data were unconstitutional because they amounted to a property taking without just compensation in violation of the Fifth Amendment to the U.S. Constitution.[102] To succeed on its claim, Monsanto had to first establish it had a property interest in the information. In finding a property interest in Monsanto's data, the Court in *Ruckelshaus* explained:

> Because of the intangible nature of a trade secret, the extent of the property right therein is defined by the extent to which the owner of the secret protects his interest from disclosure to others. . . . Information that is public knowledge or that is generally known in an industry cannot be a trade secret. . . . If an individual discloses his trade secret to others who are under no obligation to protect the confidentiality of the information, or otherwise publicly discloses the secret, his property right is extinguished.[103]

As noted above, whether information is characterized as property can have real-world consequences, and when deciding whether information will be treated as property, context matters. Information that meets the definition of a trade secret is property to the extent it can be precisely defined and is maintained within the exclusive control of the putative trade secret owner.[104]

Trade secret rights potentially apply to the data resources discussed in this Essay, as well as the accompanying software, and algorithmic models.[105] In general, trade secret rights cover operability and functionality of devices, and the algorithmic models that are often at the heart of processing data.[106] As such, secrecy produces and protects the robust ownership rights described in this Essay. In fact, these rights are sufficiently strong that putative trade secret owners may refuse to reveal the protected information, even to the government.[107]

---

100 467 U.S. 986 (1984).

101 *Id.* at 990.

102 *Id.* at 998–99.

103 *Id.* at 1002 (citations omitted).

104 *See generally* Ramon A. Klitzke, *Trade Secrets: Important Quasi-Property Rights*, 41 BUS. LAW. 555, 557 (1986) (noting that trade secret owners have exclusive rights that may continue indefinitely).

105 *See* Noto La Diega & Sappa, *supra* note 15, at 421 (describing "technical" secrecy, which results from "the opacity of the algorithms that underpin the [Internet of Things]" and "legal" secrecy, which results from "a combination of trade secrets, proprietary software and contracts").

106 Rowe & Prior, *supra* note 4, at 337.

107 *See, e.g.*, Rowe, *supra* note 11, at 793–94 (describing Toyota's refusal to disclose

Trade secret owners are also cautious because with trade secrecy (compared to patents), others may lawfully attempt to reverse engineer their products (intangible or otherwise) unless prohibited by contract.[108] Furthermore, trade secret rights are destroyed if improperly disclosed, and trade secret owners are required to take reasonable efforts to protect information that they deem a trade secret; courts typically expect such efforts, at a minimum, will include nondisclosure agreements.[109] Thus, a combination of trade secrecy and contract law through licensing agreements can be a powerful combination for controlling proprietary information.[110] This is why owners often insist on contracts generally and particularly provisions that protect confidentiality and nondisclosure.

C. Property Ownership

Data's status as property is a prerequisite to ownership, and ownership is a prerequisite to legal distribution and sharing of data.[111] This explains why ownership is so highly prized by companies in our economy. How is ownership of intangible property determined? It is determined by property law or by contract law.[112]

Indeed, failure to clearly assert ownership could result in uncertainty and ambiguity. For instance, in recent work I have noted that trade secrecy enforcement is a question mark in academia due to the lack of an ownership culture.[113] I argued that this is because academia is grounded not in a culture of ownership and secrecy, but of openness and sharing.[114] Even the trade secret espionage statute contemplates ownership[115] almost as a baseline for a

---

information to the National Highway Traffic Safety Administration after a recall, citing vital trade-secrets).

108 *See* SHARON K. SANDEEN & ELIZABETH A. ROWE, TRADE SECRET LAW INCLUDING THE DEFEND TRADE SECRETS ACT OF 2016 IN A NUTSHELL 204–05 (2d ed. 2018) (discussing considerations regarding the validity of contractual restrictions on reverse engineering).

109 *See* ELIZABETH A. ROWE & SHARON K. SANDEEN, TRADE SECRET LAW: CASES AND MATERIALS 199–201 (3d ed. 2020).

110 *See* Rowe, *Sharing Data*, *supra* note 4, at 303 ("[I]t is possible to envision contract law as a means to further support greater sharing in [the implantable medical device] context, while respecting the rights of manufacturers").

111 *See* Payne, *supra* note 29, at 387 ("Only if an individual owns something can she share it [in the sharing economy]" (citation omitted)).

112 *See generally* Grimmelmann & Mulligan, *supra* note 79 (contending that data can be protected by property and contract rights). Even the IRS Rules agree. *See* Fed. Tax Coordinator 2d (RIA) ¶ G-4560 (2023) ("The legal owner of intangible property under the intellectual property laws . . . or the holder of rights that are intangible property under a contract . . . , is considered the sole owner of the intangible property . . . unless this ownership is inconsistent with the economic substance of the underlying transactions.").

113 Elizabeth A. Rowe, *Academic Economic Espionage?*, 65 WM. & MARY L. REV 1, 7 (2023).

114 *Id.*

115 18 U.S.C. § 1832 (providing criminal liability for anyone who converts a trade secret to the benefit of anyone "other than the owner thereof").

rights holder. But without clear assertions of ownership by universities (compared to other business organizations), these assets are largely underappreciated relative to other kinds of intellectual property.[116]

III
CONTRACTS RULE

Contracts rule in an unregulated space. They are the glue that cements ownership rights and fill any gaps left bare by the absence of government regulation and any ambiguities in intellectual property law when it comes to data and intangible property. They epitomize the reign of private law in spaces where public law has been slow to enter. One contribution of this Essay is to underscore the extent to which contracts facilitate property rights in intellectual goods, like data.[117]

Contracts have always been integral to the structuring of intellectual goods.[118] For example, license agreements are typically used for all kinds of transactions, from publishing books to selling software.[119] In much the same way, they are also used for real property transactions, as anyone who has purchased a home or leased an apartment can readily attest.[120] One crucial difference is that while ownership under property law principles is bounded by limitations such as public policy exceptions, public registries, and zoning regulations,[121] contractually created property rights are not so limited.

Whether these contractual practices interfere with certain legal principles or are against public policy will likely be determined on a case-by-case basis. While some might argue that the contract merely represents an obligation between two parties,[122] there are much broader ramifications

---

116 *See* Rowe, *supra* note 113, at 68 (noting that the recognition and protection of trade secrets in the academic setting is in its infancy relative to the full maturity of other businesses and that universities will need to adapt).

117 *Cf.* Robert P. Merges, *A Transactional View of Property Rights*, 20 BERKELEY TECH. L.J. 1477 (2005) (focusing on how property rights facilitate contracts).

118 *See* Cohen, *supra* note 89, at 696 (noting the "pervasive use of licenses to structure relationships").

119 *See, e.g.*, 4DD Holdings, LLC v. United States, 169 Fed. Cl. 164, 172 (2023); iBio Inc. v. Fraunhofer USA, Inc., No. 10256-VCMR, 2016 WL 4059257, at *2 (Del. Ch. 2016); Triad Sys. Corp. v. Se. Express Co., No. C 92 1539-FMS, 1994 WL 446049, at *3 (N.D. Cal. 1994); Wall Data Inc. v. L.A. Cnty. Sheriff's Dep't, 447 F.3d 769, 773 (9th Cir. 2006).

120 *See, e.g.*, Neil S. Kessler, *Virginia Real Estate Purchase and Sale Issues for Buyers*, 2017 PRAC. REAL EST. LAW. 5, 5 (detailing several laws and customs structuring real estate transactions and contracts); Gary S. Moore, *Lawyers and the Residential Real Estate Transaction*, 26 REAL EST. L.J. 351 (1998) (studying lawyers' involvement (or lack thereof) with real estate contract negotiation across location and corresponding outcomes).

121 *See* Nash & Stern, *supra* note 14, at 481 (explaining that zoning provides a real-life example of how property rights have evolved to adopt certain limitations towards absolute property rights).

122 *See, e.g.*, W. Jack Grosse, *Moral Obligation as Consideration in Contracts*, 17 VILL. L. REV. 1, 32 (1971) ("From the viewpoint of the community, the enforcement of the promise merely completes an exchange of economic values between the two parties."); Jason P. Bergeron, Watkins

stemming from these agreements, particularly with respect to newer technologies which lack settled public law limitations—either statutorily or constitutionally created.

A. Data Ownership by Contract

Ownership is very important in our capitalist economy because it determines, among other things, who can monetize data.[123] A typical contract provision between a company and its supplier governing data might look like this:

> Data Rights and Restrictions.
>
> Company shall own all rights, title and interest to all Company Data, which shall also be subject to the confidentiality obligations set forth in this Agreement. Supplier agrees to (i) grant Company continuous and unrestricted access to all Company Data at all times as of and after the Effective Date and throughout the Term; (ii) not make any unauthorized copies of or allow any unauthorized access to the Company Data; (iii) not disclose or use Company Data for any purposes other than contemplated under this Agreement; and (iv) return and deliver all copies of the Company Data to Company and destroy or erase any Company Data in Supplier's servers, databases and systems, upon termination or expiration of the Agreement or request by Company in writing, provided that Supplier shall have no obligation to destroy or erase any Company Data securely maintained for archival purpose in the ordinary course of business as part of its electronic backup files or systems.[124]

In addition to imposing confidentiality obligations that are often associated with trade secret agreements, the above illustrates that contracts also define ownership: "Company shall own all rights . . . ." Often, even the contracts themselves are confidential,[125] so the interaction between confidentiality and control creates a "property squared" type obligation (unlike in real property when we usually know some information from public records about property transactions, these "secret agreement" provisions create complete opacity).

In the criminal justice system, when the government enters into contracts with private entities, those entities assert ownership over most new

---

v. Freeway Motors—*A Need to Clarify the Principle of Novation*, 58 LA. L. REV. 1241, 1243 (1998) ("A contract is an agreement by two or more parties whereby obligations are created, modified, or extinguished." (citation omitted)).

123 Payne, *supra* note 29, at 379.

124 Andrew J. Costa, Stephen Y. Chow, Elizabeth A. Rowe & Kim R. Jessum, Presentation at the 2023 ABA-IPL Section Annual Meeting, Data Is the New Oil: Protecting Big Data in the 21st Century (Apr. 14, 2023) (on file with author).

125 *See* Rowe & Prior, *supra* note 4, at 323 ("[C]ontracts likely include default terms requiring stringent confidentiality.").

technologies, their data, algorithms, and practically anything else that can be captured by intellectual property and trade secrecy, even when they are serving public functions. Thus, for instance, as a result of the asserted right to exclude (or restrict access and disclosure), ShotSpotter does not want gunshot data disclosed,[126] and the developer of Stingrays does not want police departments to report their use or courts to know about and review them.[127] Similarly, CMI, Inc., the developer of Intoxilyzer, a breathalyzer device, refuses to disclose its source code.[128]

Indeed, given the power of contracts to regulate in unregulated spaces, I, too, have proposed them as a tool to facilitate algorithmic transactions in the criminal justice system: "We propose a transaction-by-transaction procurement approach whereby those government agencies that value transparency and accountability can negotiate for and insert the appropriate disclosure provisions into their vendor contracts."[129] Negotiated contractual terms can serve to balance competing interests, and are routinely used with trade secrecy to assure confidentiality and nondisclosure.[130] Therefore, in the absence of public regulation regarding the disclosure of algorithms in the public sphere, contracts could be used to address the problem.[131]

B. Control & Access

Ownership means control. Ultimately, that is the key to and the prize for owning property. As noted earlier, property law sets priority of claims to control a good (tangible or intangible) by determining which uses of it are permitted.[132] Owners, through contractual provisions, reserve for themselves very broad powers to control a wide range of activities and behaviors relating to data, particularly access.[133] As such, contracts create de facto property rights, even though contracts are not property.[134] Even if there is legal ambiguity about whether data is property from an intellectual property

126 *See* Hannah Bloch-Wehba, *Access to Algorithms*, 88 FORDHAM L. REV. 1265, 1283–84 (2020).

127 *See* Wexler, *supra* note 67, at 1366–67 (noting that police departments were required to sign nondisclosure agreements "promising to conceal information about cellphone surveillance tools known as 'stingrays'—including how the devices work and even the mere fact that they exist").

128 *See* Andrea Roth, *Trial by Machine*, 104 GEO. L.J. 1245, 1272 (2016) ("To date, only one group of litigants has successfully gained access to a breath machine's source code, and even then, only upon court order after the state initially refused to disclose it.").

129 Rowe & Prior, *supra* note 4, at 350.

130 *See id.* at 342.

131 *See id.* ("[U]ntil there are legislative pronouncements that express public policy goals and interests regarding the disclosure of algorithms in the public sphere, private contracting . . . could be used to address the problem.").

132 *See* Irina D. Manta, *Keeping IP Real*, 57 HOUS. L. REV. 349, 354–55 (2019).

133 *See supra* note 15 and accompanying text.

134 *See supra* note 16 and accompanying text.

perspective,[135] the contracts declare them as such in the context of the transactions applicable to this Essay (where data resources are commodities of trade). Thus, the declaration of ownership, coupled with courts' broad enforcement of such contract terms[136] creates the property right or at a minimum, quasi-property right, that then coalesces with the accompanying property rights from trade secrecy.

The power and discretion to limit access in whatever way an owner chooses, without the benefit of exceptions (as with real property) has caused particular tension with public values.[137] Moreover, as some scholars have noted, there is a public-private vulnerability dynamic at play, especially as it concerns consumers with a power disparity.[138] As the contextual examples below reveal, those concerns are especially challenging in public-private partnerships. As such, they have led to calls for greater transparency and accountability.[139]

1. Tensions on Access Restrictions

Per the Blackstonian conception of property, the owner has sole and despotic dominion over their property.[140] The use of contracts to establish and buttress property rights to own and control data permits the owner to exert relatively unbounded control in the absence of guardrails. Generally, courts uphold contractual agreements unless there is a violation of public policy or proof of unconscionability.[141]

Perhaps the best example, from a personal autonomy perspective, is that of implantable medical devices. With these devices, manufacturers contractually assert ownership and control over all data generated from

---

135 *See* Ritter & Mayer, *supra* note 2, at 227 (noting that because no privacy or data protection laws expressly define what data ownership encompasses, there are ambiguities as to how data should be defined, licensed, transferred, and used).

136 *See infra* note 141 and accompanying text.

137 *See* Rowe & Prior, *supra* note 4, at 340 (noting a public-private tension at the heart of any attempt to understand and better balance private interests in intellectual property with the public's right to information).

138 *See supra* note 19 and accompanying text.

139 *See* Rowe & Prior, *supra* note 4, at 307 (noting that scholars have called for greater transparency, such as by abolishing a number of trade secret protections).

140 Cohen, *supra* note 89, at 699.

141 *See, e.g.*, TOA Sys. Inc., v. Int'l Bus. Machs. Corp., No. 18 CV 10685 (VB), 2019 WL 5693388, at *3 (S.D.N.Y. Nov. 4, 2019) (granting motion to dismiss a contract claim because the case involved sophisticated parties and there was no allegation of intentional wrongdoing); 4DD Holdings, LLC v. United States, 169 Fed. Cl. 164, 179 (2023) ("The government fraudulently and materially misrepresented the extent of its copyright infringement, and it cannot now invoke [the contractual release] to bar 4DD's copyright claim."); Arthur's Garage, Inc. v. Racal-Chubb Sec. Sys., Inc., 997 S.W.2d 803, 810 (Tex. App. 1999) ("An agreement to limit liability for future negligence is enforceable if the agreement does not violate public policy.").

patients' bodies.[142] Patients are left without any realtime access to the data (from implanted devices they purchased), and any reports from the data are provided only to the patient's physician.[143]

There is no regulation or any law that mandates such access.[144] There is also much regulatory fragmentation between and among the various government agencies that might each independently have some oversight over implantable medical devices. Several government agencies potentially have a hand in this regulatory space, including, for instance, the Copyright Office, the Federal Communications Commission, the Federal Trade Commission, the Food and Drug Administration, and the Department of Homeland Security. However, not even the Health Insurance Portability and Accountability Act (HIPAA), which normally governs the sharing of patient information, speaks directly to establishing a patient's rights to access their own data from implantable devices.[145]

Nor does the patient have control over what could happen to the data collected from their device. For one thing, HIPAA does not apply to data collected from implantable medical devices.[146] Ironically, data that may not be accessible to a patient themself, might nevertheless be used against them. For instance, it is foreseeable that insurers may try to increase rates or deny certain claims based on the data.[147] Further, even in court proceedings, the data might be used to incriminate an individual[148] or determine liability,[149] despite potential issues with the reliability and accuracy of the information.[150] Similarly, the patient does not receive knowledge of how the device works and whether there have been failures or vulnerabilities related to its use.[151]

---

142 *See supra* note 44 and accompanying text.

143 *See* Rowe, *Sharing Data*, *supra* note 4, at 295.

144 *See supra* note 47 and accompanying text.

145 *See* Access of Individuals to Protected Health Information, 45 C.F.R. § 164.524 (2023) (demonstrating silence on patient rights in the context of medical implantable devices).

146 *See id.* (lacking mention of data from implantable medical devices).

147 *See, e.g.*, Kashmir Hill, *Automakers Are Sharing Consumers' Driving Behavior with Insurance Companies*, N.Y. TIMES (Mar. 13, 2024), https://www.nytimes.com/2024/03/11/technology/carmakers-driver-tracking-insurance.html [https://perma.cc/2Q6A-GPRG] (reporting on auto insurers using data from cars about consumers' driving habits to increase insurance rates).

148 *See* Motion to Suppress at 3, State v. Compton, No. CR 2016-12-1826 (Ohio Ct. Com. Pl. May 5, 2017) (indicting defendant on charges of arson and insurance fraud using data from his pacemaker).

149 *See* Kate Crawford, *When Fitbit Is the Expert Witness*, THE ATLANTIC (Nov. 19, 2014), https://www.theatlantic.com/technology/archive/2014/11/when-fitbit-is-the-expert-witness/382936 [https://perma.cc/NFC8-V4KJ] (discussing first-known court case using Fitbit data in a personal injury claim).

150 For a comparison with the European approach to accuracy, see discussion *infra* Section IV.A.

151 Rowe, *Sharing Data*, *supra* note 4, at 297–98.

2. Tensions on Public-Private Values

Perhaps having a private-law-dominated scheme that leaves discretion to market participants is par for the course and not objectionable in many contexts. Indeed, it might be more efficient than the alternative.[152] However, does this view hold when one considers the ever-present and expanding model of public-private partnerships whereby private entities are contracted to provide public services for the government? As a greater range of public law values are likely to attach to government functions, chief among them constitutional concerns and statutorily created public policy exceptions, a contract model for structuring relationships to the benefit of the drafter becomes thorny. While in those instances the government may act more like a consumer and market participant, the absence of public law values such as accountability, transparency, and due process arising from those transactions might be more salient.[153]

As Professor Kristen Eichensehr observed years ago in her article on the trend of privatization in cybersecurity, "the United States has already backed into a de facto system of 'public-private cybersecurity'" which "create[s] risks that it may not effectuate the public law values, such as accountability and fairness, that the normal, formal processes of government functioning are designed to foster."[154]Similarly, the public-private partnerships that have been facilitated by contracts that provide for complete ownership, control, and access of data by private providers have been criticized for ignoring the public interests in transparency and accountability.

Recall, in particular, that trade secrecy is most often used to support owners' intellectual property rights in data.[155] The conception of trade secrets as property is fundamental to its design and underlying legal framework. This makes it almost antithetical to consideration of the public interest in governmental transparency.[156] When compared to the clarity of intellectual property rights for owners, the "public interest" generally is murky and

---

152 *See, e.g.*, Fordham Intell. Prop., Media & Ent. L.J., *The Private-Sector Ecosystem of User Data in the Digital Age*, 29 FORDHAM INTELL. PROP., MEDIA & ENT. L.J. 1099, 1108–09 (2019) (noting argument that traditional regulatory frameworks are ill-suited to govern data); Okediji, *supra* note 27, at 341 ("There is no question that in many cases, the private sector is better equipped to utilize data-driven tools to address social problems and thus enhance public welfare."). *But see* Robert P. Merges, *The End of Friction? Property Rights and Contract in the "Newtonian" World of On-Line Commerce*, 12 BERKELEY TECH. L.J. 115, 128 (1997) (lamenting the move away from universal registration for copyright because such policy may improve efficiency).

153 *See* Kristen E. Eichensehr, *Public-Private Cybersecurity*, 95 TEX. L. REV. 467, 471–72 (2017).

154 *Id.* at 470, 472.

155 *See supra* notes 104–10 and accompanying text.

156 As it pertains to this context, a more comprehensive discussion of the public interest and trade secrecy is beyond the scope of this Article.

unsettled.[157] Indeed, it should be noted plainly that there is no mechanism for robust consideration of "the public interest" in the U.S. trade secret framework, except in some rather limited circumstances that themselves are underdeveloped.[158] Other than whistleblower protections[159] and some First Amendment[160] exceptions, public interest considerations most frequently arise (albeit in a relatively cursory fashion) in the consideration of equitable principles[161] for injunctive relief in trade secret misappropriation cases. This public-secret tension is at the heart of any attempt to understand and better balance private interests in intellectual property with the public's right to information.[162]

It is not uncommon that owners will typically try to claim intellectual property rights as broadly as they can.[163] This tendency to overclaim can pose tensions with public values,[164] as the legal structure places a perceived thumb on the scale in favor of intellectual property owners.. As a caveat, while this Essay addresses data resource outputs that are developed by private entities, it is worth noting that sometimes the origin of the data may be from government or public databases.[165] Whether special rules should apply to

157 *See* Charles Tait Graves & Sonia K. Katyal, *From Trade Secrecy to Seclusion*, 109 GEO. L.J 1337, 1419 (2021) (noting that at present, laws do not generally call for an examination of public interests and calling for a reform that would grant courts permission to do so).

158 *See* Sharon K. Sandeen & Ulla-Maija Mylly, *Trade Secrets and the Right to Information: A Comparative Analysis of E.U. and U.S. Approaches to Freedom of Expression and Whistleblowing*, 21 N.C. J.L. & TECH. 1, 55 (2020) (noting that a public interest exception to trade secret protection exists but is not well developed); Peter S. Menell, *Tailoring a Public Policy Exception to Trade Secret Protection*, 105 CALIF. L. REV. 1, 30 (2017) (noting that courts have recognized that trade secret protection, for example, can implicate public interest and have therefore developed a limited but murky privilege to disclose trade secrets).

159 18 U.S.C. § 1833 (2016).

160 *See, e.g.*, Elizabeth A. Rowe, *Trade Secret Litigation and Free Speech: Is It Time to Restrain the Plaintiffs?*, 50 B.C. L. REV. 1425, 1433 (2009) (noting that courts tend to lend greater weight to property right interests when balancing against First Amendment concerns); Pamela Samuelson, *Principles for Resolving Conflicts Between Trade Secrets and the First Amendment*, 58 HASTINGS L.J. 777, 808–11 (2007) (noting that First Amendment defenses have succeeded in many intellectual property cases).

161 *See* Elizabeth A. Rowe, eBay, *Permanent Injunctions, and Trade Secrets*, 77 WASH. & LEE L. REV. 553, 567 (2020) (referencing "equitable principles" as a consideration courts typically take into account, even if not directly relying on the Supreme Court's highly significant patent case *eBay Inc. v. MercExchange, L.L.C.*).

162 *See* Sandeen & Mylly, *supra* note 158, at 19 ("[A] critical question is how the right to information and the rights of trade secret owners can be properly balanced, particularly when the subject trade secrets are of great public interest").

163 *See, e.g.*, Sharon K. Sandeen & Tanya Aplin, *Trade Secrecy, Factual Secrecy and the Hype Surrounding AI*, *in* RESEARCH HANDBOOK ON INTELLECTUAL PROPERTY AND ARTIFICIAL INTELLIGENCE 452 (Ryan Abbott ed., 2022) ("[C]laiming secrecy with respect to the entirety of an AI system is a gross over assertion of trade secret rights.").

164 *See* Rowe & Prior, *supra* note 4, at 340 ("As some scholars have argued, the struggle for transparency from secrecy may be further exacerbated by developers' overclaiming their trade secret rights.").

165 *See* Okediji, *supra* note 27, at 333–36.

such information is outside the scope of this paper.[166] However, in such instances, the same pattern follows: private owners use contracts to claim ownership over their outputs.[167]

As illustrated by the example of algorithms in the criminal justice system, contractual nondisclosure agreements, coupled with asserted trade secret rights of ownership, reflect an example of intellectual property laws providing greater protection than contract law alone would provide. As the government increasingly relies on private vendors to supply its technologies and the attendant algorithms that aid decision-making, the public's call for transparency will present significant challenges. Private vendors' assertions of trade secret rights in these technologies seemingly conflict with the public's need for disclosure.

Ideally, legislated exemptions (both state and federal) could make the terms and conditions governing disclosure of algorithms in the public sphere clearer. Such exemptions, however, are unlikely to occur on a wide scale. While a few states have recognized that it is against the public interest to enter into settlement agreements that shield information about dangers to the public's health and safety[168] and to forbid whistleblowing by employees,[169] no such exception exists for trade secrets related to technologies in the criminal justice system or even, generally, technologies acquired from private vendors by government agencies for public decisionmaking or critical public functions.

However, until there are legislative pronouncements that express public policy goals and interests regarding the disclosure of algorithms in the public sphere, I have recommended private contracting through government procurement to address the problem.[170] Indeed, in this context and others, it is possible to envision contract law as a means of simultaneously supporting greater sharing of data in this context while also protecting the rights of vendors.[171]

Similarly, there is currently no federal regulation of biometric data in

166 For a discussion of potential special rules, see *id.* at 336 (arguing for possible government ownership of "downstream goods created as a result of its open access policies").

167 *See* Noto La Diega & Sappa, *supra* note 15, at 436 (noting that private entities have imposed contracts to appropriate and reuse both personal and non-personal data and to gain control over data produced by their proprietary algorithms).

168 *See* Elizabeth E. Spainhour, *Unsealing Settlements: Recent Efforts to Expose Settlement Agreements that Conceal Public Hazards*, 82 N.C. L. REV. 2155, 2158–61 (2004) (discussing state laws, like Florida's, that declare private settlements that conceal public hazards void as a matter of public policy).

169 *See* MARK A. ROTHSTEIN, CHARLES B. CRAVER, ELINOR P. SCHROEDER, ELAINE W. SHOBEN & L. CAMILLE HÉBERT, EMPLOYMENT LAW § 9.12 (5th ed. 2014).

170 *See* Rowe & Prior, *supra* note 4, at 342–62.

171 *Id.* at 342 (citation omitted).

the U.S.[172] As noted earlier, while a few states have stepped in with their own regulations,[173] government use is unregulated.[174] Federal and state agencies share database information with each other, such as Immigration and Customs Enforcement (ICE) having access to state databases, raising concerns about civil liberties.[175] Businesses are also left with uncertainty about how to handle biometric data in their business practices as they operate across the country with a patchwork of state regulations, and even they have pushed for federal regulation.[176]

C. Liability

Just as contracts bolster property rights in this context by giving owners ownership over data, they also tend to simultaneously disclaim liability.[177] But with ownership comes responsibility. Query whether a system that allows private law to permit complete ownership and control while rejecting responsibility for harm achieves a fair balance.The exponential strength to property rights offered by combining contracts and property law results in a land of private law where parties pick and choose terms that are most beneficial to them. Public law values are thus subservient to the terms of the contract.Will it take instances of significant harm to expose private law's dominance in this space without boundaries, or will other areas of private law (like tort law) serve as a stop gap? These questions have no definitive answers and must instead be explored on a context-by-context basis.

Years ago, Professor Jacqueline Lipton, writing about databases, suggested that data property rights should be granted but that "commensurate legal duties" should attach.[178] She argued that rights holders had certain legal duties "attached to the privilege of property ownership."[179]She further suggested that the state (public law) should have a responsibility to monitor such private duties given that the state has supported the private system of property rights allocation.[180] In light of this Essay's thrust, that private law has flourished where public law has regressed on the issue of ownership, her

---

172 Rowe, *Regulating Facial Recognition Technology*, *supra* note 4, at 34.

173 *See id.* at 39–40 (discussing states that have adopted statutes to regulate biometric data).

174 *Id.* at 34.

175 *See* Dustin Volz, *ICE Taps States' Photo Databases to Hunt Criminal Suspects*, WALL ST. J. (July 8, 2019, 6:28 PM), https://www.wsj.com/articles/ice-taps-states-photo-databases-to-hunt-criminal-suspects-11562615932 [https://perma.cc/32RT-TMDJ].

176 *See* Rowe, *Regulating Facial Recognition Technology*, *supra* note 4, at 37–39 (discussing corporate involvement by Amazon and other companies in pursuing regulation in light of uncertainties).

177 Courtney K. Meyer, *Exculpatory Clauses and Artificial Intelligence*, 51 STETSON L. REV. 259, 260 (2021).

178 Payne, *supra* note 29, at 382.

179 *Id.*

180 *Id.*

suggestions are a reasonable start.

Contracts can be, and often are, drafted to limit liability to a party on which it may otherwise fall.[181] Take, for instance, a classic tort-law-accident scenario with an automobile. Now add in new technology with data inputs and outputs, processing algorithms, and AI (a semiautonomous or autonomous vehicle), and the traditional legal principles for liability become less clear.[182] For example, Tesla uses limitation-of-liability clauses in its contracts with purchasers that read:

> Tesla hereby disclaims any and all indirect, incidental, special and consequential damages arising out of or relating to your vehicle . . . . Tesla shall not be liable for any direct damages in an amount that exceeds the fair market value of the vehicle at the time of the claim. The above limitations and exclusions shall apply whether your claim is in contract, tort (including negligence and gross negligence), breach of warranty or condition, misrepresentation (whether negligent or otherwise) or otherwise at law or in equity . . . .[183]

When a Tesla vehicle is involved in an accident because of a failure in its AI capabilities, for instance, plaintiffs seeking relief must contend with these types of contractual limitations.[184] Among other things, they would need to resort to state public policy exceptions, if any, to attempt to argue that the clause is unenforceable. However, this can be difficult where exceptions have not been legislated for injuries resulting from these kinds of new technologies.[185]

---

181 Meyer, *supra* note 177, at 260; *see also* RESTATEMENT (SECOND) OF CONTS. § 195 (AM. L. INST. 1981) (describing contract terms exempting tort liability).

182 *See, e.g.*, Michael L. Rustad, *Products Liability for Software Defects in Driverless Cars*, 32 S. CAL. INTERDISC. L.J. 171, 212 (2022) (noting that the rise of autonomous vehicles will raise complex new liability questions); Melis Ozdel, *Reconceptualising the Nautical Fault Exception in the Fog of Emerging Technologies*, 51 INDUS. L.J. 672, 675–79 (2022) (discussing liability in the context of autonomous sea vessels).

183 TESLA, NEW VEHICLE LIMITED WARRANTY 11 (2021), https://www.tesla.com/sites/default/files/downloads/tesla-new-vehicle-limited-warranty-en-us.pdf [https://perma.cc/V9D7-LMPF].

184 *See, e.g.*, In re Tesla Advanced Driver Assistance Sys. Litig., No. 22-cv-05240, 2023 WL 6391477, at *4 (N.D. Cal. Sept. 30, 2023) (involving arbitration clause in Tesla contract); Williams v. Tesla, Inc.., No. 20-cv-08208, 2021 WL 2531177, at *4 (N.D. Cal. June 21, 2021)(involving warranty clause in Tesla contract for alleged defects); Meyer, *supra* note 177, at 268–71 (discussing whether Tesla's exculpatory clause can be enforceable and limit its liability in a claim arising out of a Tesla vehicle accident); *see also* TESLA, FULL SELF-DRIVING (SUPERVISED) SUBSCRIPTION AGREEMENT, https://www.tesla.com/legal/additional-resources#full-self-driving-capability-subscription-agreement [https://perma.cc/YU2G-GV8G] (containing similar "Limitation of Liability" clause).

185 Currently, no state or federal legislation has been enacted to govern injuries resulting from autonomous vehicles. Therefore, these cases have taken the form of product liability cases, similar to how a victim would sue a manufacturer for a faulty airbag.*See* Jenna Greene, *Driverless Car Problems Are Outpacing Liability Laws*, REUTERS (Dec. 11, 2023, 12:45 PM), https://www.reuters.com/legal/transactional/column-driverless-car-problems-are-outpacing-

Thus, private law will be the de facto regulatory framework, whether through contract and/or tort law, that manages possible solutions. In addition, market participants, particularly insurance companies, will also be compelled to problem-solve and self-regulate.[186] Indeed, in Australia and Hong Kong, Tesla is reportedly experimenting with offering customized car insurance with its vehicles.[187]Although companies can use contract law, the lack of a public law response, especially on the federal level, can be unsatisfying to companies who are frustrated by piecemeal state regulation.[188] These concerns apply across all industries, from automobiles to medical care.[189]

IV
POSSIBLE RESPONSES

As the various contextual examples interwoven through this Essay have demonstrated, in the United States, public law and regulation of data, AI, and new technologies in general continue to be sparse or nonexistent. This is especially so on a federal level where no federal regulation exists for determining data ownership and access in such areas as implantable medical devices, biometric data, or algorithmic models in the criminal justice system. As a result, private law mediated through contracts rule the space.

This Part considers possible high-level structural responses to some of the concerns that have been identified, particularly involving public-private partnerships. One contrasting public law approach can be seen in the pending

liability-laws-2023-12-11 [https://perma.cc/H4U9-V5RC]; *see also* Stephanie L. Lee, *Clicking Away Consent: Establishing Accountability and Liability Apportionment in Direct-to-Consumer Healthcare Artificial Intelligence*, 88 BROOK. L. REV. 1355, 1369 (2023) ("In the current legal landscape, most states generally recognize exculpatory clauses to be enforceable if valid."); WILSON ELSER MOSKOWITZ EDELMAN & DICKER LLP, EXPRESS ASSUMPTION OF RISK/WAIVER/EXCULPATORY CLAUSES 1 (2012) (on file with author) (discussing state court standards for upholding exculpatory clauses).

186 *See* Anat Lior, *Insuring AI: The Role of Insurance in Artificial Intelligence Regulation*, 35 HARV. J.L. & TECH. 467, 481 (2022).

187 Rachel Theodorou, Note, *"With Cars Like These, Who Needs Policies?"—The Inevitable Battle Between Autonomous Vehicles, the Insurance Industry, Manufacturers and Consumers*, 35 SYRACUSE J. SCI. & TECH. L. 72, 93 (2018–2019); *see also* Danielle Muoio, *Tesla Is Pushing the Insurance Industry to Prepare for Massive Disruption*, BUS. INSIDER (May 25, 2017, 9:59 AM), http://www.businessinsider.com/how-tesla-self-driving-cars-are-changing-insurance-industry-2017-5 [https://perma.cc/AQ82-FZWV] (noting that autonomous driving technologies like Tesla's may drive changes in insurance plans by making cars less prone to accidents).

188 *See* Theodorou, *supra* note 187, at 94–95 (noting concern by Volvo's CEO about the lack of federal guidelines in the United States); K.C. Webb, *Products Liability and Autonomous Vehicles: Who's Driving Whom?*, 23 RICHMOND J.L. & TECH., no. 4, 2016, at 46 ("AV proponents petitioned Congress to regulate the industry in order to avoid letting states construct a patchwork of laws which could hamper innovation.").

189 *See, e.g.*, Bethany A. Corbin, *When "Things" Go Wrong: Redefining Liability for the Internet of Medical Things*, 71 S.C. L. REV. 1, 3 (2019) (noting the lack of a comprehensive liability framework to regulate innovative technologies in the healthcare sector).

and recently passed legislation in the European Union for new technologies. Alternatively, jurisdictions in the United States could choose to expand public law to reach or modify contractual agreements regarding ownership. Further, with respect to the liability concern, in the absence of public law expansion (or even in conjunction with it), other areas of private law—in particular, tort law—might be modified to address and assign duties and liabilities for those areas where public law has been silent.

A. EU Public Law Approaches

Public law and regulation are more salient in the EU, relative to the U.S. legal system where private law and property rights prevail. Indeed, the EU Trade Secrets Directive, adopted around the same time as the federal Defend Trade Secrets Act in the United States, does not recognize property rights in trade secrets.[190] Nevertheless, the results of a recent report suggest that European companies (similar to U.S. companies) place reliance on the use of trade secret laws coupled with contracts to engage in transactions involving data sharing and access.[191] Further, regulation of new technologies for the public interest, while stalled in the United States, has moved at a feverish pace in the EU.[192]

For example, for the last few years,[193] the European Union has been "working on the world's first comprehensive law to regulate artificial intelligence."[194] The proposal offers a tiered approach to regulating AI (defined as systems that use machine learning, logic, or knowledge-based

190 *See* Eur. Innovation Council and SMEs Exec. Agency of the Eur. Comm'n, *Study on the Legal Protection of Trade Secrets in the Context of the Data Economy: Final Report*, at 22, GRO/SME/20/F/206 (July 2022) [hereinafter *EU Study on Trade Secrets*]; Tanya Aplin, Alfred Radauer, Martin A. Bader & Nicola Searle, *The Role of EU Trade Secrets Law in the Data Economy: An Empirical Analysis*, 54 INT'L REV. INTELL. PROP. & COMPETITION L. 826, 834 (2023).

191 *See EU Study on Trade Secrets*, *supra* note 190, at 83.

192 *See, e.g.*, *Commission Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts*, COM (2021) 206 final (Apr. 21, 2021); Council Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on Contestable and Fair Markets in the Digital Sector and Amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act), 2022 O.J. (L 265) 1 (EU).

193 The Artificial Intelligence Act, first proposed in 2021 and passed in late 2023, continues to undergo revisions and a trilogue stage review, and is likely to have an effective date no earlier than 2025. *See* Kate Brimsted & Jack Dunn, *AI Regulation Tracker: UK and EU Take Divergent Approaches to AI Regulation*, LEXOLOGY (May 17, 2023), https://www.lexology.com/library/detail.aspx?g=b0b84c21-dfb5-4163-8f8d-b03962dd8342 [https://perma.cc/SA9U-KK3Y].

194 Luca Bertuzzi, *Europe's Rulebook for Artificial Intelligence Takes Shape*, INT'L ASS'N OF PRIV. PROS. (May 23, 2023), https://iapp.org/news/a/europes-rulebook-for-artificial-intelligence-takes-shape [https://perma.cc/U6N9-3WSR].

approaches).[195] It ties regulation to level of risk, such that the higher-risk products face stricter regulations.[196] The outputs from systems classified as high risk, for instance, require review by at least two people.[197] Those applications determined to be of unacceptable risk are banned by default.[198] Biometric identification systems, predictive policing software, and applications that use untargeted scraping for facial images to build databases fall within this category.[199] So are systems that "exploit[] vulnerabilities of individuals or specific groups."[200] Interestingly, per the public values of accountability and transparency discussed above, high-risk systems will need to meet specific standards for, among other things, quality and accuracy; and they will also need to be registered in an EU database that will be available to the public.[201] In addition, the Digital Services Act and Digital Markets Act, passed in November 2022, also aim to create greater public transparency by, for example, requiring independent audits.[202]

With respect to liability issues, the EU has also proposed the AI Liability Directive, which is aimed at ensuring that, in non-contractual situations,[203] victims of damage caused by AI can seek legal recourse in the same way that victims of harm caused by other products can.[204] This is an attempt by Parliament to adapt private law to create a civil liability regime for AI.[205] It is part of the much broader initiative, described above, to govern AI systems in the marketplace generally.[206] Among other things, it creates a rebuttable presumption of causality when certain conditions are met, including a failure to comply with a duty of care and damage caused by the

---

195 *Id.*

196 *Id.*

197 *Id.*

198 *Id.*

199 Ryan Browne, *Europe Takes Aim at ChatGPT with What Might Soon Be the West's First A.I. Law. Here's What It Means*, CNBC (May 15, 2023, 5:34 AM), https://www.cnbc.com/2023/05/15/eu-ai-act-europe-takes-aim-at-chatgpt-with-landmark-regulation.html [https://perma.cc/5QZX-RLTA].

200 *Id.*

201 *See* Alex Engler, *The EU and U.S. Diverge on AI Regulation: A Transatlantic Comparison and Steps to Alignment*, BROOKINGS (Apr. 25, 2023), https://www.brookings.edu/research/the-eu-and-us-diverge-on-ai-regulation-a-transatlantic-comparison-and-steps-to-alignment [https://perma.cc/VZU9-2AJY].

202 *Id.*

203 *See* Tambiama Madiega, Eur. Parliamentary Rsch. Serv., *Artificial Intelligence Liability Directive*, at 5 (Feb. 2023), https://www.europarl.europa.eu/RegData/etudes/BRIE/2023/739342/EPRS_BRI(2023)739342_EN.pdf [https://perma.cc/S23S-22KD] (noting the directive provides for compensation in civil liability claims irrespective of a contractual link between the victim and the liable entity).

204 *Commission Proposal for a Directive of the European Parliament and of the Council on Adapting Non-Contractual Civil Liability Rules to Artificial Intelligence (AI Liability Directive)*, at 3, COM (2022) 496 final (Sept. 28, 2022).

205 *See id.* at 2, 12.

206 Madiega, *supra* note 203, at 2.

output from an AI system.[207]

B. Expand Public Law

In stark contrast to the EU, it is important to understand that the United States tends to take a less public-interest-focused approach when it comes to intellectual property rights. For instance, we have neither an explicit public interest exemption to trade secret protection,[208] nor a General Data Protection Regulation (GDPR) that grants rights of access, portability, and information to consumers.[209] In the United States, federal and state governments (or courts) could expand public law to reach or influence contractual agreements regarding ownership. To be sure, this might not necessarily mean granting greater benefits to the public and could further solidify the de facto contractual ownership provisions for owners. This has been done, for instance, in less than a handful of states regarding customers' electric meter data.[210]

Generally utility companies own customers' meter data.[211] Washington, D.C. rules provide that "the utility company owns the data when dealing with third parties."[212] In Oklahoma, "[a]ll data generated, recorded, stored or transmitted by Smart Meter and supporting technology and infrastructure is, and shall at all times be and remain, the sole and exclusive property of the Company."[213] In Texas, "[a]ll meter data, including all data generated . . . by advanced meters . . . shall belong to a customer, including data used to calculate charges for service, historical load data, and any other proprietary customer information. A customer may authorize its data to be provided to one or more retail electric providers . . . ."[214]

With respect to the liability issue specifically, some states have considered or adopted legislation,[215] and some scholars have proposed safe

---

207 *See id.* at 6–7.

208 *See, e.g.*, Rowe & Prior, *supra* note 4, at 339; *cf.* Noto La Diega & Sappa, *supra* note 15, at 442 (describing France's explicit exception to the Trade Secrets Directive for freedom of expression and information); Loi 2018-670 du 30 juillet 2018 relative à la protection du secret des affaires [Law 2018-670 of July 30, 2018, on the Protection of Trade Secrets], JOURNAL OFFICIEL DE LA RÉPUBLIQUE FRANÇAISE [J.O.] [OFFICIAL GAZETTE OF FRANCE], July31, 2018 (providing for public interest exceptions for freedom of expression, communication, and information).

209 *See* Noto La Diega & Sappa, *supra* note 15, at 457 (describing the General Data Protection Regulation that applies in the EU).

210 Payne, *supra* note 29, at 374–76.

211 *Id.* at 374.

212 Payne, *supra* note 29, at 375.

213 *Id.* at 375–76.

214 *Id.* at 376.

215 *See, e.g.*, *California Privacy Rights Act of 2020, Proposition 24 in the November 2020 General Election*, CAL. PRIV. RTS. ACT, https://thecpra.org [https://perma.cc/8HD3-KGZS]; Theodore Claypoole, *Ohio Enacts First Cybersecurity Safe Harbor*, JD SUPRA (Nov. 7, 2018), https://www.jdsupra.com/legalnews/ohio-enacts-first-cybersecurity-safe-80727

harbor and other structures that limit liability in exchange for engaging in other precautions.[216]

C. Expand Private Law—Torts

In the absence of public law, scholars have suggested various ways, including resorting to another area of private law—torts—to address and assign some of the duties and liabilities for these areas where public law has been silent.[217] The legal question mark arises in a traditional products liability scheme where intangible goods, like data and AI, may not be considered products.[218] In such circumstances, when injury occurs from alleged failures in such intangible processes, who should be responsible? As noted above, owners would have likely disclaimed liability in their contracts.

Interestingly, most of the recent work in this area has been related narrowly to AI but could nonetheless offer some insights, at least generally, with respect to how scholars envision the interaction and how public and private law could structure liability for intangible goods. Proposals such as granting corporate personhood to AI,[219] modifying assumption-of-risk principles,[220] expanding negligence principles,[221] and adopting a strict liability regime[222] are all conscious of (intellectual) property owners' secret "black box" approach to protecting their source codes, algorithmic models, and data.[223] Finally, one author, consistent with the theme of data ownership in this Essay, proposes that, in the context of autonomous vehicles and other connected devices, the manufacturer who owns the proprietary software that runs the device and thereby has continuous interaction with it "should be

---

[https://perma.cc/X5CT-8A82]; OHIO REV. CODE ANN. §§ 1354.01–1354.05 (West 2019); N.Y. GEN. BUS. LAW § 899-bb (McKinney 2020).

216 *E.g.*, Corbin, *supra* note 189, at 5–6.

217 *E.g.*, Jessica Litman, *Information Privacy/Information Property*, 52 STAN. L. REV. 1283, 1288 (2000).

218 *See, e.g.*, Madiega, *supra* note 203, at 3; *see also* F. Patrick Hubbard, *"Sophisticated Robots": Balancing Liability, Regulation, and Innovation*, 66 FLA. L. REV. 1803, 1853 (2014) ("[S]ophisticated robotic vehicles might present difficulties in applying the distinction between manufacturing defects and design defects where software is concerned.")

219 *E.g.*, Alicia Lai, *Artificial Intelligence, LLC: Corporate Personhood as Tort Reform*, 2021 MICH. ST. L. REV. 597, 600 (2021); Benedict See, *Paging Doctor Robot: Medical Artificial Intelligence, Tort Liability, and Why Personhood May be the Answer*, 87 BROOK. L. REV. 417, 437 (2021); Megan Sword, *To Err Is Both Human and Non-Human*, 88 UMKC L. REV. 211, 233 (2019).

220 *E.g.*, Amy L. Stein, *Assuming the Risks of Artificial Intelligence*, 102 B.U. L. REV. 979, 1022 (2022).

221 *E.g.*, Andrew D. Selbst, *Negligence and AI's Human Users*, 100 B.U. L. REV. 1315, 1353 (2020).

222 *E.g.*, Anat Lior, *AI Strict Liability Vis-à-Vis AI Monopolization*, 22 COLUM. SCI. & TECH. L. REV. 90, 95 (2020); Lior, *supra* note 186, at 472.

223 *See, e.g.*, Lee, *supra* note 185, at 1356–57 (noting that AI in the healthcare system is known as "black-box medicine" because of the lack of transparency with respect to how the algorithm is structured and how its reasoning works).

accountable when it fails to perform in a safe manner."[224]

CONCLUSION

This Essay exposed the extent to which private law plays an outsized role in regulating spaces where public law has left a void. Using illustrations from a variety of contexts, including implantable medical devices, facial recognition technology, and algorithmic models in the criminal justice system, it demonstrated the interconnected reliance on contract law, intellectual property law, and property law to regulate ownership and access to data resources. In particular, contracts facilitate property rights in intellectual goods, like data, and they epitomize the reign of private law in spaces where public law has been slow to enter. However, this phenomenon has implications for owners, consumers, and the public interest as we continue to develop and rely on new technologies. This is because, while ownership under property law principles is bounded by limitations such as public policy exceptions, contractually created property rights are not similarly limited. I posit that this private law creep leads to a new property formulation: Intellectual property + Contracts = Property squared. Private law has become the de facto regulatory framework for new technologies, one in which there are no public guardrails. However, this status quo need not be. Whether through exploring the approach of the European Union, domestic electric meter regimes, or product liability reform, this Essay has identified several high-level possibilities for crafting a legal landscape where public interests can co-exist with private law.

224 Robert S. Peck, *The Coming Connected-Products Liability Revolutio*n, 73 HASTINGS L.J. 1305, 1320–22, 1326 (2022).