Louisiana Law Review

Volume 81
Number 3 *Spring 2021*

Article 11

4-29-2021

A Modern-Day Gold-Rush: Applying Property Principles to Data Using Mineral Rights Concepts and the Rule of Capture

Andrew Crayden

Follow this and additional works at: https://digitalcommons.law.lsu.edu/lalrev

 Part of the Public Law and Legal Theory Commons

Repository Citation

Andrew Crayden, *A Modern-Day Gold-Rush: Applying Property Principles to Data Using Mineral Rights Concepts and the Rule of Capture*, 81 La. L. Rev. (2021)
Available at: https://digitalcommons.law.lsu.edu/lalrev/vol81/iss3/11

This Comment is brought to you for free and open access by the Law Reviews and Journals at LSU Law Digital Commons. It has been accepted for inclusion in Louisiana Law Review by an authorized editor of LSU Law Digital Commons. For more information, please contact kreed25@lsu.edu.

A Modern-Day Gold-Rush: Applying Property Principles to Data Using Mineral Rights Concepts and the Rule of Capture

Andrew Crayden[*]

TABLE OF CONTENTS

Copyright 2021, by ANDREW CRAYDEN.

* J.D. candidate 2021, Paul M. Hebert Law Center, Louisiana State University. I would like the thank Professors Corcos, Goring, and Moréteau for their expertise and guidance during the writing process, and I would like to thank the Board of the Louisiana Law Review for their tireless work in editing each Comment. This Comment is dedicated to my parents and fiancée for their steadfast support in all my pursuits.

"'Data! Data! Data!' he cried impatiently. 'I can't make bricks without clay!'"

-Sherlock Holmes[1]

INTRODUCTION

In a Target store outside of Minneapolis, Minnesota, a father angrily complained to a manager regarding baby coupons that the company mailed to his home and addressed to his teenage daughter.[2] After the store manager initially apologized for the mailings, he called the father later that week to once again express his regret for the mistake.[3] Surprisingly, the father made an apology of his own after learning his daughter was in fact pregnant.[4] Target knew to send the baby coupons to the pregnant teenager based on its analysis of customer shopping patterns over time in search of relationships between purchases that could indicate which consumers were pregnant.[5] The company was able to determine that pregnant consumers purchased certain combinations of items, like lotions, unscented soaps, and dietary supplements, at different stages of their pregnancies.[6] Target

1. ARTHUR CONAN DOYLE, THE ADVENTURES OF SHERLOCK HOLMES 278 (1892). The quote famously notes the importance of data; Holmes is powerless to make his stunning feats of deductive reasoning without data.

2. *See* Kashmir Hill, *How Target Figured Out a Teen Girl Was Pregnant Before Her Father Did*, FORBES (Feb. 16, 2012, 11:02 AM), https://www.forbes.com/sites/kashmirhill/2012/02/16/how-target-figured-out-a-teen-girl-was-pregnant-before-her-father-did/#7a617f766686 [https://perma.cc/KL4Z-3NQR].

3. *Id.*

4. *Id.*

5. To figure out whether a consumer is pregnant, Target analyzes purchases of items that are needed for a new baby. Then, to determine if a woman is pregnant earlier in time, models can be made based on the items purchased by people who Target determines ultimately had babies before they bought distinctive baby related items. *Id.*

6. *Id.*

then used this information to send customers, like the man's teenage daughter, coupons for baby items to increase sales.[7]

Like Target, modern businesses have discovered the value of data.[8] Data has evolved, increasing in both amount and complexity.[9] To use the analogy of Sir Arthur Conan Doyle from *The Adventures of Sherlock Holmes*, companies have much more "clay," or data, and are using it to make "bricks," or insight and information, that is increasingly valuable.[10] The Target anecdote illustrates how the retailer famously used its "clay" to make bricks that enabled it to predict a teenager's pregnancy before she told her parents.[11] Both consumer data, or data that companies collect on consumers like the teen's shopping habits, and industrial data, or data that companies generate internally in the normal course of business operations, have increased and become fundamental resources companies use to generate revenue.[12] Like a modern day gold rush, there has been a boom of data "miners" using technological tools to discover valuable nuggets of insight in an effort to deliver tremendous value to their companies.[13] Ever-

---

7. *Id.*

8. *See generally* Lothar Determann, *No One Owns Data*, 70 HASTINGS L. J. 3, 3–5 (2018).

9. *Id.*

10. DOYLE, *supra* note 1; *see also* Holger Hurtgen & Niko Mohr, *Achieving Business Impact with Data*, MCKINSEY & CO. (Apr. 2018), https://www.mckinsey.com/business-functions/mckinsey-analytics/our-insights/achieving-business-impact-with-data [https://perma.cc/WQ7V-Q5FV].

11. *See* Hill, *supra* note 2.

12. Alexander Furnas, *Everything You Wanted to Know About Data Mining but Were Afraid to Ask*, ATLANTIC (Apr. 3, 2012), https://www.theatlantic.com/technology/archive/2012/04/everything-you-wanted-to-know-about-data-mining-but-were-afraid-to-ask/255388/ [https://perma.cc/4CKJ-R9GW]; Jeffery Ritter & Anna Meyer, *Regulating Data as Property: A New Construct for Moving Forward*, 16 DUKE L. & TECH. REV. 220, 253–54 (2018) (noting that the amount of total "industrial data" grows by 40% each year).

13. In 1848, the discovery of gold in California sent many an aspiring miner into the western hills, sparking the California Gold Rush. *See The California Gold Rush*, PBS, https://www.pbs.org/wgbh/americanexperience/features/goldrush-california/ [https://perma.cc/FFE3-5R33] (last visited Nov. 13, 2020). The frenzy of activity sent hundreds of thousands of people to California, and although over $2 billion in gold was recovered, few of these prospectors ever struck it rich. Within a decade, with most of the easily accessibly deposits depleted, the Rush came to an end. *California Gold Rush*, ENCYCLOPEDIA BRITANNICA, https://www.britannica.com/topic/California-Gold-Rush [https://perma.cc/C5VW-8EAP] (last visited Nov. 13, 2020). The revolution in data has often been likened to a new gold rush, one where software, instead of pickaxes and shovels, are the tools of choice to mine for valuable insights. Brad Peters, *The Big Data Gold Rush*, FORBES

improving analytical techniques have allowed corporations to mine data for information and trends, such as the connection between shopping habits and pregnancy that Target discovered.[14] Although data collection and analysis present tremendous opportunities for businesses, they also threaten to compromise consumer privacy.[15]

Businesses cannot attain the value and opportunity that data collection and analysis provide without impacts on consumers' privacy.[16] Concern over consumer data collection methods, the scope of the data collected, and companies' use of the collected data have become prevalent issues.[17] Beyond the privacy implications of a business's internal use of consumer data, resourceful hackers and poor data governance[18] have led to corporations' increasingly common loss of consumer information in data breaches.[19] A data breach's severity can lead to significant data loss, exposing the records of 100 million consumers or more per event, leaving them vulnerable to identity theft and other misappropriations of their personal information.[20]

Due to these concerns, governments across the world have taken varying degrees of action to address the challenges that modern data collection and use pose.[21] The European Union recently enacted its most comprehensive and stringent data privacy regulation yet: the General Data Protection Regulation (GDPR), which regulates how data collected on EU

(June 21, 2012), https://www.forbes.com/sites/bradpeters/2012/06/21/the-big-data-gold-rush/#2a42103ab247 [https://perma.cc/73F8-LTKU].

14. *See* Furnas, *supra* note 12.

15. *See generally* Daniel Marcus, *The Data Breach Dilemma: Proactive Solutions for Protecting Consumers' Personal Information*, 68 DUKE L. J. 555, 556–65 (2018).

16. Herb Weisbaum, *The Total Cost of a Data Breach – Including Lost Business – Keeps Growing*, NBC NEWS (July 30, 2018), https://www.nbcnews.com/business/consumer/total-cost-data-breach-including-lost-business-keeps-growing-n895826 [https://perma.cc/C586-HN9K].

17. *See generally* Erika J. Nash, *Notice and Consent: A Healthy Balance Between Privacy and Innovation for Wearables*, 33 BYU J. PUB. L. 197 (2018) (discussing data collection with regard to wearable, connected devices).

18. Data governance is the "management of data availability, relevancy, usability, integrity and security in an enterprise." *Data governance*, IBM, https://www.ibm.com/analytics/data-governance [https://perma.cc/5C79-7WTM] (last visited Nov. 13, 2020).

19. *See generally* Robert Rabin, *Perspectives on Privacy, Data Security and Tort Law*, 6 DEPAUL L. REV. 313–19 (2017).

20. *Id.*

21. *See generally* Michael Rustad & Thomas Koenig, *Towards a Global Data Privacy Standard*, 71 FLA. L. REV. 365 (2019).

citizens is processed, stored, and used.[22] Alternatively, legislation in the United States mostly takes the form of individual state regulations, except for federal, sector-specific regulations such as the Health Insurance Portability and Accountability Act (HIPAA).[23] The most similar U.S. regulation to the GDPR is California's Consumer Privacy Act, which became effective on January 1, 2020.[24] Nationwide, the protection of data privacy is not as uniform or protective of consumers as it is abroad, which presents issues for consumers injured by the misuse of data.[25] Consumers have largely been unable to find relief in the aftermath of a data breach in both federal and state courts.[26] Federal courts are often unwilling to find Article III standing[27] after finding a lack of concrete and actual damages following a breach.[28] Similarly, state courts have found that the damages element of a negligence claim is not satisfied for reasons regarding proof of actual injury after a breach.[29] Without overarching privacy regulation in the United States providing a cause of action for data misuse and guidelines for good data governance, companies may continue to misuse consumer data, while the injured consumers remain without relief.[30]

Although much scholarly research on data protection has centered around the merits and creation of an overarching U.S. data privacy regulation like the GDPR, less authorship and more uncertainty surrounds the foundation of data protection and claims.[31] Lawsuits concerning data breaches are typically brought under privacy-based tort theories of liability, but there is an open question as to whether data protection issues

---

22. *Id.* at 375–78.

23. HIPAA protects specific health data and does not prescribe a general data protection regime outside of the healthcare field. *See id.* at 381.

24. *Id.* at 403–05.

25. Alex Bossone, *The Battle Against Breaches: A Call for Modernizing Federal Consumer Data Security Regulation*, 69 FED. COMM. L. J. 227, 230 (2018).

26. *Id*. at 228–29.

27. For a federal court to hear a case, the Supreme Court requires a party to have a "concrete and particularized," "actual or imminent" "injury in fact" to find Article III standing. Standing is what the Constitution requires for a person to bring a claim into, in this case, federal court. Clapper v. Amnesty Int'l USA, 568 U.S. 398, 409 (2016).

28. *See* Marcus, *supra* note 15, at 566–75.

29. *Id.*

30. *See* Jay Kesan & Carol Hayes, *Liability for Data Injuries*, 2019 U. ILL. L. REV. 295, 333–39 (2019).

31. Marcus, *supra* note 15, at 566–75 (discussing the need for a uniform privacy regulation).

should be redressed in tort or another body of law such as property.[32] The determination of this foundational question will impact the legal precepts applicable to data breach claims, significantly affect the outcome of a consumer's claim in the event of a breach, and impact corporate practices with respect to data.[33] Specifically, it must be decided, either judicially or legislatively, whether data privacy should be rooted in property law and whether data is susceptible of ownership.[34]

Scholars have penned arguments both for and against property rights in data.[35] On one side of the argument, scholars favoring the treatment of data as property argue that well-defined property rights in data are critical to support the modern information economy, as businesses depend more heavily on the data they collect and protect.[36] These scholars further recognize that in addition to the existing modes of property protection, courts and Congress must create supplemental mechanisms to regulate the complexity and amount of data property rights created if the law recognizes data as an item of property.[37] On the other side, scholars advocating against treating data as property focus on the immense complexity that a data property regime would entail and negative privacy implications as evidence of data being practically untenable as property.[38] They further contend that the costs of increased litigation from consumers asserting property rights to their data and the resulting impediment to information flow would outweigh any minimal benefit that may otherwise accrue.[39]

Despite contrary positions on the issue, treating data as an item of property can lay a foundation for any data privacy regulation in the United States, particularly a much needed general federal regulation, and provide clarity for courts to adjudicate data privacy disputes.[40] In Louisiana, data

32. *See* Jay Kesan & Carol Hayes, *Liability for Data Injuries*, 2019 U. ILL. L. REV. 295, 316, 323 (2019).

33. *See generally id.*

34. *See generally* Ritter & Meyer, *supra* note 12 (answering in the affirmative). *But see* Determann, *supra* note 8 (answering in the negative).

35. *See e.g.,* Ritter & Meyer, *supra* note 12, at 223; *but see* Determann, *supra* note 8, at 34–37.

36. Ritter & Meyer, *supra* note 12, at 223.

37. *Id.* at 269–77.

38. *See generally* Determann, *supra* note 8, at 34–42.

39. *Id.*

40. *See generally* Ritter & Meyer, *supra* note 12, at 223.

specifically merits classification as a corporeal movable,[41] and not as an intangible or incorporeal[42] thing.[43] To alleviate some of the issues, such as increased litigation that may accompany property rights in data, companies collecting the data should have the largest "bundle of rights" in the data, which would approximate ownership, or "quasi-ownership."[44] This would allow the data-driven economy to function more efficiently and potentially incentivize businesses to better protect their data from external interference by hackers and other criminals as they might protect other assets they own.[45] Although this deprives consumers of an absolute ownership right to "their" data, property rights, including ownership, are rarely absolute.[46] To protect consumers interests, courts or legislators must also craft rules to limit the data collectors' rights to exclude and transfer the data or to provide a remedy if it is misused.[47]

To effectively implement this data property regime, legislatures may draw by analogy from the principles of mineral rights.[48] Specifically, applying the rule of capture and its attendant concepts, like the doctrine of correlative rights, is instructive for assigning and limiting property rights to data.[49] From these precepts of mineral rights, a court would be able to apply an existing property framework to novel data problems.[50] Additionally, either Congress or the state legislatures can draw on these property concepts as the foundation for drafting a uniform data privacy regulation in the future.[51]

Part I of this Comment will introduce the concept of data as opposed to information, as well as the modern uses and proliferation of data, and will further describe the issues plaguing data use such as data breaches.

---

41. A corporeal moveable is what would be considered tangible personal property in common law and is found in Louisiana Civil Code article 471. LA CIV. CODE art. 471 (2020).

42. Incorporeals are intangible things such as rights and obligations on things. *Id.*

43. *See generally* Ritter & Meyer, *supra* note 12, at 223.

44. What is meant by "quasi-ownership" is rights approximating those of an owner, even if not in relation to a traditional item of property that may typically be owned. *Id.* at 267.

45. *See generally id.* at 223.

46. *See generally* Jacqueline Lipton, *Information Property: Rights and Responsibilities*, 56 FLA. L. REV. 135, 137–40 (2004).

47. *See generally id.*

48. *See generally id.* (noting that drawing on familiar property principles is instructive in achieving balance, in that case, in interests in information).

49. For a discussion of these concepts, see *infra* Part IV.B.

50. *See generally* Lipton, *supra* note 46.

51. *See generally* Ritter & Meyer, *supra* note 12, at 223.

Part II will address the data protection methods that the European Union and the United States have employed to address these issues and note current problems with data protection in the United States. Part III will argue for the application of property principles to data and the consideration of data as an item of property. Part IV will discuss how courts and legislatures may implement this property regime by using the mineral rights principles of the rule of capture and will then discuss the impact of such a regime. Ultimately, this Comment will conclude by addressing the need for the judiciary to establish clearly defined data property principles and call for the legislature to create a uniform data privacy regulation.

I. "DATA! DATA! DATA!"

Data collection and exploitation by businesses have become increasingly prevalent and pervasive parts of modern life.[52] With a digitally enabled and network-connected society whose technology is ever expanding, the scope and resulting implications of data continue to increase.[53] Legal issues accompanying the rise of "big data" include the manner in which data collectors may use the data and the appropriate remedy in the event of a breach.[54] Although usually synonymous, a distinction between "data" and "information" is necessary to clearly examine data and to analyze the legal regimes already in place.[55]

A. Bricks or Clay?

Merriam-Webster's Dictionary defines data in a number of different ways: first as "factual information . . . used as a basis for reasoning, discussion, or calculation," then as "information in digital form that can be transmitted or processed," and finally as "information output . . . [that] must be processed to be meaningful."[56] Although the definition of data

52. Terence Mills, *Why Big Data and Machine Learning Are Important in Our Society*, FORBES (Jan. 7, 2019, 8:30 AM), https://www.forbes.com/sites/forbestechcouncil/2019/01/07/why-big-data-and-machine-learning-are-important-in-our-society/#1332bf6f7aa2 [https://perma.cc/AE79-EHG5].

53. *See generally* Marcus, *supra* note 15, at 556–65.

54. *See generally id.*

55. Most scholarly articles on the subject of data also begin with an explanation of the term before they begin their explication. *See generally* Ritter & Meyer, *supra* note 12, at 225.

56. *Data*, MERRIAM WEBSTER, https://www.merriam-webster.com/dictionary/data [https://perma.cc/8WG9-ZDRG] (last visited Nov. 13, 2020).

includes the word "information," the field of information systems makes a meaningful distinction between data and information.[57] Accordingly, this Comment differentiates between data on the one hand, and information on the other.

In this Comment, "data" refers to the raw material, a fact, or a byte, which, by itself, is meaningless to the average person.[58] For instance, in the Target example, archived records of each individual Stock Keeping Unit (SKU)[59] for each purchase constitute data. In contrast, "information" is created by utilizing data to gain insight into a situation or problem.[60] Information represents the inferences and conclusions that have meaning and value to the person who generated them, depending on the context they are placed in.[61] When Target compiles and transforms the individual data points, or purchases, to create a shopping history for a single customer or a trend in shopping patterns for multiple customers, such as the pregnant customers in the Target example, the result of that analysis—the identification of trends and the ultimate determination of which customers are pregnant—then becomes valuable information for the retailer.

Scholars, and even data users, further distinguish between data that has the ability to identify a consumer and data that does not identify a consumer.[62] Data that has the ability to identify a consumer is generally termed "personally identifiable information," or PII, and is of the most notoriety and concern when discussing data protection issues.[63] Data that does not have the ability to identify a consumer is known by different names, such as industrial data, and it generally describes data produced in business operations or another area not connected to a consumer.[64] This

57. The study of information systems is the study of systems which collect, process, store, and distribute information, typically throughout an organization. EFFY OZ, MANAGEMENT INFORMATION SYSTEMS 9–10 (2009).

58. *Id.*

59. A stock keeping unit is the number on an item's barcode representing that particular item. The code is derived relative to the price, product, and manufacturer. *See Stock Keeping Unit (SKU)*, INVESTOPEDIA (Aug. 5, 2020), https://www.investopedia.com/terms/s/stock-keeping-unit-sku.asp [https://perma.cc/7KPW-CH9R]. The code itself or its numbers out of context are data; however, in the right context and to the right people, it may provide information about the item. This is in some ways an artificial distinction; however, it is necessary to make sure that even the data, the code itself, may also receive appropriate protection. *Id.*

60. OZ, *supra* note 57.

61. *Id.*

62. Ritter & Meyer, *supra* note 12, at 225.

63. *Id.*

64. *Id.*

Comment mainly focuses on consumer data, though the analysis proposed is largely applicable to industrial data as well.

In a legal analysis of PII, scholars usually do not explicitly make such a distinction between "data" and "information," likely owing to the lack of a definitive line between the two.[65] Generally, scholars use the terms data and information interchangeably but recognize data as a less refined subset of what the law traditionally recognizes as information.[66] However, the expectations regarding the legal protection available for each vary based on the policies each implicates.[67] For instance, at one end of the spectrum, a creative expression or compilation of information may be protected under intellectual property law with copyright, patent, trademark, or trade secret protection.[68] On the other end of the spectrum are bare facts, or pure data, which, without more, are generally not ownable or protectable.[69] Thus, if closer to the expression-of-information end of the spectrum, an item is more likely to obtain intellectual property protections. Conversely, an item is generally less likely to implicate intellectual property rights if it is closer to the data end of the spectrum.[70] The distinction between data and information is meaningful for determining ownership and other property rights and affects the existing legal precepts and regimes applicable to each.[71]

B. Why Bricks or Why Clay?

Intellectual property law affords consumer data little protection due to its dissimilarity with what is currently protected with patent, copyright,

---

65. *See id.* (defining data as information that is recorded); *see also* Determann, *supra* note 8, at 6 (declining to make a distinction between data and information although the author notes there are other approaches to the terms in other academic disciplines).

66. *See generally* Determann, *supra* note 8, at 6 (claiming data is the informational content of information).

67. Although many do not make a distinction in terminology, scholars do discuss and recognize the differing principles that are applicable to what this Comment refers to as data compared to information. *See generally id.* at 6–26.

68. *Id.* at 18–21 (discussing the ability of copyright to protect information and data).

69. *See generally* Int'l News Serv. v. Associated Press, 248 U.S. 215, 234 (1918).

70. *See generally* Feist Publ'ns v. Rural Tel. Serv. Co., 499 U.S. 340 (1991) (reasoning that because facts are not original, they may not be protected with copyright, although factual compilations may be, while rejecting a copyright claim over the white pages of a local phone book).

71. *See generally* Determann, *supra* note 8, at 6–26.

and other forms of intellectual property.[72] Significantly, data lacks the creative or expressive elements inherent in protection under intellectual property and thus may not be protected with intellectual property law.[73] Patents, copyrights, and trademarks protect certain uses of specific types of information, or the particular expression of that information, that Congress has decided to protect and promote for policy reasons.[74] These intellectual property devices provide the holder who has performed some inventive or creative work a right to limit the public's use of that information to create an invention in patent, or copy an expression of information in copyright.[75] Congressional grants of rights under intellectual property law seek to strike a balance between protecting the inventor or artist's creation and not overly infringing upon the public domain of information that should remain open to everyone.[76] This balance motivates the restrictions of functionality in trademark law, the limitation of copyright to an author's expression, and the nonobvious requirement in patent.[77]

---

72. *See generally id.*

73. *See generally id.* at 14–21 (discussing what may be protected under trade secret, copyright, trademark, and patent law).

74. *Id.*; *see also* 35 U.S.C. § 101 (stating what may be patented is "new and useful"). Under patent, for example, in an effort to encourage innovation, an inventor with an idea for an invention can secure the exclusive right to produce that invention for a specified period. *Id.*

75. *See* 35 U.S.C § 271 (providing a cause of action for a patent holder against one who infringes his patent). The ability to license patents, copyrights, and trademarks encompasses a right to exclude others from using them as well. However, this does not mean the information cannot be used at all, the public just cannot use the patent information to create the patented invention, or directly copy the expression of an author. Intellectual property does not generally protect the information itself. *See generally Feist*, 499 U.S. 340.

76. *See generally Feist*, 499 U.S. at 349–52 (discussing the fact/expression dichotomy and noting others are encouraged to build freely upon the author's work, a result which is the purpose of the act).

77. For the nonobvious requirement in patent, see 35 U.S.C. § 103 ("A patent for a claimed invention may not be obtained, . . . if the differences between the claimed invention and the prior art are such that the claimed invention as a whole would have been obvious before the effective filing date of the claimed invention to a person having ordinary skill in the art to which the claimed invention pertains."), and for the functionality requirement in trademark, see 15 U.S.C. §1053(e)(5). Such limitations on intellectual property protection ensure that ideas that were originally in the public domain, or obvious as in patent, are not removed from public use by intellectual property protection.

Information that receives some benefit of intellectual property protection is generally that which was creatively processed, transformed, or has competitive value to an organization.[78] In granting such protection, legislatures determined that society's interest in restricting the unauthorized use of that information and rewarding the efforts of the creator of the information outweighs the interest of allowing unfettered use of that information or expression.[79] Intellectual property does not absolutely protect the underlying information, as its goal is to promote and expand society's body of knowledge.[80] It does, however, limit certain uses or practices of that information, such as limiting manufacture of a patented invention, in order to promote invention, authorship, or another socially desirable goal.[81] Intellectual property law does not prohibit the general public's use of bare facts, information, or ideas; thus, it would not generally protect consumer data.[82]

In *International News Service v. Associated Press*, the U.S. Supreme Court discussed the extent to which intellectual property may provide property rights in bare facts, equivalent to data, that are not traditionally protected.[83] The plaintiff news provider, Associated Press (AP), generated revenue by collecting facts for news stories and distributing articles for newspapers to publish based on those bare facts collected.[84] AP sued another news provider, International News Service (INS), after it discovered that the INS was waiting to get the facts from AP's articles to generate its own articles for subscribers rather than gathering the facts themselves.[85] In the case, the Court ultimately held that there was some protectable "quasi-property interest" in the news despite the traditional notion of the news as merely facts in the public domain.[86] The Court found that the underlying facts were not susceptible of ownership and distinguished them from the compilation of the facts into the news articles.[87] The Court reasoned that the underlying facts were insusceptible

78. *See generally* Determann, *supra* note 8, at 14–21.

79. *Id.* (discussing what may be protected under trade secret, copyright, trademark and patent law).

80. *Id.*

81. *Id.*

82. *See generally* Feist Publ'ns v. Rural Tel. Serv., 499 U.S. 340, 349–52 (1991).

83. *See generally* Int'l News Serv. v. Associated Press, 248 U.S. 215 (1918).

84. *Id.* at 229.

85. *Id.*

86. *See generally id.* at 215.

87. *Id.* at 234.

of ownership in the "absolute sense."[88] However, in the context of two competitors compiling and selling the news, the news providers gathered the facts at a cost and had to further transform the facts for the stories to be distributed.[89] Accordingly, it found that AP had obtained limited property rights against INS in the facts it collected, rights that AP may not otherwise have against the world.[90]

The holding in *International News Service* demonstrates an application of the concept of "relativity of title"[91] applied to the "facts" underlying the news.[92] Facts, like data, may not generally be protectable, but the decision to assign property rights, and to whom, may depend on the relationship of the parties and the respective value of the item when held by each.[93] This will ultimately help justify, in part, property rights in data.[94] In his dissent in *International News Service*, Justice Brandeis was reluctant to extend property rights to what amounted to facts traditionally in the public domain.[95] His reluctance to do so stemmed from his belief that the imposition of property rights in facts, though cognizable, would be best left to the legislature, which could better weigh societal interests and provide an appropriate framework for enforcement.[96] Although the decision predated *Erie Railroad Co. v. Tompkins*, this case remains heavily referenced and illustrates the important distinction between protections on the spectrum of information and data as well as the traditional approach to such "data" or facts.[97] Since 1918, when *International News Service* was decided, digital technology has dramatically shaped society and enabled the rise of consumer data with various attendant consequences.

---

88. *Id.*

89. *Id.*

90. *Id.*

91. Relativity of title is an old common law notion that "title is not absolute but a priority against another's claim." *See Relativity of Title*, BOUVIER LAW DICTIONARY (2012). It recognizes that property rights are not absolute, but are "enforceable only against particular individuals under certain circumstances." *Id.*

92. *See generally Int'l News Serv.*, 248 U.S. 215.

93. *See* discussion *infra* Part IV.B.

94. *See* discussion *infra* Part IV.B.

95. *Int'l News Serv.*, 248 U.S. at 264–67.

96. *Id.*

97. *See generally id.* This case was decided before the Supreme Court's ruling in *Erie Railroad Co. v. Tompkins*, which held that there is no general federal common law. *See generally* Erie R.R. Co. v. Thompkins, 304 U.S. 64 (1938). Courts and scholars have continued to cite *International News Service*, even over the last decade, and the analysis regarding property rights in facts is still instructive in determining whether such property rights should be created in data.

C. That's a Lot of Clay

Many different sources generate and collect modern consumer data daily.[98] Consumer data may come from sources such as customer input in web forms, browser cookies, credit card usage, and GPS locations.[99] In contrast, industrial data may be generated by sensors on a production line, in accounting transactions from point-of-sale systems at business-to-business enterprises, and through numerous other business processes.[100] With the expansion of technology and the advent of new network-connected devices such as the "Internet of Things"[101] and autonomous vehicles,[102] the amount of consumer and industrial data that corporations collect and analyze has increased tremendously.[103]

Many companies have realized the value gained through the exploitation of data.[104] One study recently estimated that major internet platforms, such as Google, derived approximately $57 billion in revenue from data analysis and transactions in 2018 alone.[105] Sectors aside from technology, like healthcare and finance, also generate significant value

---

98. Melody Ucros, *10 Sneaky Ways Companies Are Collecting Data to Understand Customers*, MEDIUM (Jan. 12, 2018), https://medium.com/@melodyucros/10-sneaky-ways-companies-are-collecting-data-to-understand-customers-be0b9089d54a [https://perma.cc/9MKA-HU4U].

99. *Id.*

100. *Industrial Internet of Things*, AMAZON WEB SERVICES, https://aws.amazon.com/iot/solutions/industrial-iot/ [https://perma.cc/2PA7-2FYM] (last visited Nov. 13, 2020).

101. The "Internet of Things" is a term used to describe devices that are connected to the internet, which are networked and generally contain sensors for data collection. Watches, coffee pots, and televisions may now be connected to the internet. *See generally* Jacob Morgan, *A Simple Explanation Of 'The Internet of Things'*, FORBES (May 13, 2014, 12:05 AM), https://www.forbes.com/sites/jacobmorgan/2014/05/13/simple-explanation-internet-things-that-anyone-can-understand/#3a31cd871d09 [https://perma.cc/84SW-SAA3].

102. *See* ACCENTURE, AUTONOMOUS VEHICLES: THE RACE IS ON 5 (2018), https://www.accenture.com/_acnmedia/pdf-73/accenture-autonomous-vehicles-the-race-is-on.pdf [https://perma.cc/CB9J-V4Z7] (discussing the amount of data generated by a self-driving car).

103. Peters, *supra* note 13.

104. Determann, *supra* note 8, at 4 (describing data as the fuel of the digital economy).

105. ROBERT SHAPIRO & SIDDHARTHA ANEJA, FUTURE MAJORITY, WHO OWNS AMERICAN'S PERSONAL INFORMATION AND WHAT IS IT WORTH? (Apr. 13, 2019), https://www.sonecon.com/docs/studies/Report_on_the_Value_of_Peoples_Personal_Data-Shapiro-Aneja-Future_Majority-March_2019.pdf [https://perma.cc/8NW2-CHZW].

from data.[106] To capture that value, organizations developed data mining techniques and software to gain insights about consumers from the data that is constantly being collected about them.[107] Companies perform sophisticated analyses to find trends that predict customer behavior and to discover patterns to improve financial metrics, such as revenue, and non-financial metrics like customer satisfaction.[108] As illustrated in the Target anecdote, data as innocuous as a list of items purchased while shopping can provide an opportunity for companies to pinpoint their advertisements and seek greater revenue.[109] Though now heavily used in many business' operations, data and the proliferation in its collection and analysis have not come without complications for consumers.

D. A Muddy Mess

In recent years, data transactions, which entail sales and transfers of data, have been a point of concern for consumers and a key reporting area for the media.[110] Entire markets have emerged for data transactions, particularly consumer data, through data brokers, on account of the value that consumer data analysis can provide.[111] Unlike large companies with the resources to develop their own databases and data analysis techniques, small and midsize companies can use this intermediary market to tap into the value of data.[112] Brokers compile consumer data and sell it to companies, which, in turn, use the data to target advertisements and marketing campaigns to a particular consumer based on his search history and other data points, such as age and location.[113] In 2018, American

106. *Id.*

107. *Data Mining: What It Is and Why It Matters*, SAS, https://www.sas.com/en_us/insights/analytics/data-mining.html [https://perma.cc/8F8A-ECJD] (last visited Nov. 13, 2020).

108. *Id.*

109. *See* Hill, *supra* note 2.

110. Douglas MacMillan, *How to Stop Companies from Selling Your Data*, WASHINGTON POST (June 24, 2019), https://www.washingtonpost.com/business/2019/06/24/how-stop-companies-selling-your-data/ [https://perma.cc/PZW3-MGBW].

111. Brian Naylor, *Firms Are Buying, Sharing Your Online Info. What Can You Do about It?*, NPR (July 11, 2016, 4:51 PM), https://www.npr.org/sections/alltechconsidered/2016/07/11/485571291/firms-are-buying-sharing-your-online-info-what-can-you-do-about-it [https://perma.cc/VT6A-S5SU].

112. SHAPIRO & ANEJA, *supra* note 105.

113. Naylor, *supra* note 111.

companies spent approximately $19 billion dollars obtaining data and new software for data analysis.[114]

Data transfers that move consumer data outside the collecting company pose risks to consumers' data privacy.[115] The most important recent example of such data use outside of the collecting company is the Facebook Cambridge Analytica Scandal.[116] The scandal involved a third-party researcher who provided hundreds of thousands of Facebook users' profile data to a consulting company based in the United Kingdom, which allegedly then used the profile data to impact U.S. political elections.[117] Although Facebook maintains that it has never condoned the transfer of information to such data intermediaries, the Federal Trade Commission fined the company $5 billion dollars as part of a settlement agreement in 2019.[118] In a recent suit filed in the U.S. District Court for the Northern District of California, the court, in ruling on Facebook's motion to dismiss, permitted a class of users to sue Facebook over the scandal.[119] In so holding, the court found that the plaintiffs had shown a sufficient privacy injury to have Article III standing.[120] The court rejected two of three of the

---

114. *U.S. Firms to Spend Nearly $19.2 Billion on Third-Party Audience Data & Data- Use Solutions in 2018, Up 17.5% From 2017*, IAB. (Dec. 5, 2018), https://www.iab.com/news/2018-state-of-data-report/ [https://perma.cc/KW3M-N5XF].

115. *See generally* Naylor, *supra* note 111.

116. *See* Kevin Granville, *Facebook and Cambridge Analytica: What You Need to Know as the Fallout Widens*, N.Y. TIMES (Mar. 19, 2018), https://www.nytimes.com/2018/03/19/technology/facebook-cambridge-analytica-explained.html [https://perma.cc/YY7Z-2PUP].

117. *Id.*

118. *Facebook 'to Be Fined $5bn over the Cambridge Analytica Scandal'*, BBC NEWS (July 13, 2019), https://www.bbc.com/news/world-us-canada-48972327 [https://perma.cc/J3KS-A922]. The Federal Trade Commission "[p]rotect[s] consumers and competition by preventing anticompetitive, deceptive, and unfair business practices through law enforcement, advocacy, and education without unduly burdening legitimate business activity." *About Us,* FED. TRADE COMM'N, https://www.ftc.gov/about-ftc [https://perma.cc/3252-F23W] (last visited Nov. 13, 2020).

119. Joel Rosenblatt, *Facebook Faces Massive Damages in Cambridge Analytica Suit*, BLOOMBERG (Sept. 9, 2019), https://www.bloomberg.com/news/articles/2019-09-09/facebook-users-gain-leverage-in-cambridge-analytica-privacy-suit [https://perma.cc/2STQ-Q9GW].

120. *In re* Facebook, Inc., Consumer Priv. User Profile Litig., No. 18-md-02843-VC, slip op. at 13–18 (N.D. Cal. Sept. 9, 2019) (Pretrial Order No. 20: Granting in Part and Denying in Part Motion to Dismiss First Amended Complaint).

plaintiffs' arguments for relief, including the plaintiffs' allegation of a loss of value the users could have derived from exploitation of their own data and a risk of damage from identity theft.[121] However, according to the court, an intangible privacy harm can certainly be—and in fact was—a cognizable injury in federal court under the facts alleged.[122] Facebook may ultimately be exposed to significant damages in the numerous cases filed after the scandal if other courts follow the Northern District of California's reasoning.[123]

Sales and misuse of consumer data, such as the Facebook Cambridge Analytica Scandal, are neither the only risks that consumers face with corporate data use nor the only ways in which their data is compromised.[124] Cyberattacks by hackers and other cybercriminals resulting in data breaches are on the rise.[125] Hackers may seek technological weaknesses to exploit in retailers that store customer data or "second-party data sources" that aggregate and store consumer data for a purpose separate from retail, such as a government agency.[126] The massive Equifax data breach, which exposed the personal data of 147 million consumers, is a prime example of a second-party data breach.[127] Unfortunately, the Equifax breach is merely one of a multitude of data breaches that occur each year.[128]

---

121. *Id.*

122. *Id.*

123. Rosenblatt, *supra* note 119.

124. *Consumer Data under Attack: The Growing Threat of Cyber Crime*, DELOITTE. (2015), https://www2.deloitte.com/tr/en/pages/risk/articles/consumer-data-under-attack.html [https://perma.cc/QUH6-4UXY].

125. *See* Juliana De Groot, *The History of Data Breaches*, DIGITAL GUARDIAN (Oct. 5, 2020), https://digitalguardian.com/blog/history-data-breaches [https://perma.cc/N7B5-S6KP] (discussing trends in the number and scope of data breaches).

126. *See* Nicole Martin, *What is a Data Breach?*, FORBES (Feb. 25, 2019), https://www.forbes.com/sites/nicolemartin1/2019/02/25/what-is-a-data-breach/#e1ac14514bbe [https://perma.cc/9CWT-7WN8].

127. The Equifax data breach occurred in 2017 and exposed the data of approximately 147 million people, including social security numbers, birth dates, addresses, and driver's license numbers. Equifax was forced to pay $700 million in fines to consumers who were affected by the breach. *See* Alvaro Puig, *Equifax Data Breach Settlement: What You Should Know*, FED. TRADE COMM'N (July 22, 2019), https://www.consumer.ftc.gov/blog/2019/07/equifax-data-breach-settlement-what-you-should-know [https://perma.cc/B6CL-RSRC].

128. Davey Winder, *Data Breaches Expose 4.1 Billion Records In First Six Months Of 2019*, FORBES (Aug. 20, 2019, 06:31 AM), https://www.forbes.com/sites/daveywinder/2019/08/20/data-breaches-expose-41-billion-records-in-first-six-months-of-2019/#21cb1d22bd54 [https://perma.cc/K7BE-BQX9].

Consumers face potential injury, and corporations may face liability after data breaches and other failures in data protection.[129] The extent of each, however, may depend on the data protection regulations of the relevant nation.[130]

II. GLOBAL AND U.S. RESPONSE

In light of the risks that data sales, transfers, and breaches pose to consumers' privacy interests, nations across the world have begun to regulate the protection of consumer data.[131] Countries have enacted various regulations that focus on achieving data privacy goals, such as allowing consumers access to their data and adopting regulations governing corporations' use of consumer data.[132] Comparatively, the state of data protection in the United States is significantly less developed than in the European Union.[133] Additionally, data protection regimes vary among the states in the United States.[134]

A. Data Privacy and Protection in the European Union

The European Union recently enacted a uniform data privacy regulation that grants consumers considerable rights regarding their data.[135] The EU's General Data Protection Regulation (GDPR) took effect in May 2018 and builds upon the foundation of "the Directive," its previous data regulation scheme.[136] The GDPR, however, includes more detailed practices that companies must follow to protect consumer data, significantly increased fines for non-compliance, and an expanded jurisdictional provision that will allow the regulation to affect most U.S.

---

129. Marty Puranik, *What is the Cost of a Data Breach?*, FORBES (Dec. 2, 2019, 08:40 AM), https://www.forbes.com/sites/forbestechcouncil/2019/12/02/what-is-the-cost-of-a-data-breach/#1612f45429e7 [https://perma.cc/WJ3N-FUAU].

130. Justin Pierce, *Shifting Data Breach Liability: A Congressional Approach*, 57 WM. & MARY L. REV. 975, 985 (2016).

131. *See generally* Rustad & Koenig, *supra* note 21.

132. *See generally id.*

133. *See generally id.*

134. *See generally id.* at 384–85.

135. *See generally id.* at 375–81.

136. The Data Protection Directive was in place in the European Union since 1995, and similarly to the GDPR, it gave citizens rights of access and more control over the data that was collected about them. 6 DAVID BENDER, COMPUTER LAW: A GUIDE TO CYBERLAW AND DATA PRIVACY LAW § 51.04 (2020).

companies that transact business with and collect data on EU citizens.[137] It ultimately serves as a significant step forward in the protection of consumer data privacy in Europe.[138]

1. GDPR

The GDPR's focus is more proactive than prior regulations because it mandates specific rules and safeguards for protecting consumers' data that companies must implement in their data processing operations.[139] Under the regulation, consumers' "personal data" is data that identifies or is capable of identifying the consumer.[140] "Data processing" includes activities such as the collection, storage, and use of data.[141] Additionally, part of the significance of the new GDPR is its penalty structure that allows the pertinent regulatory body of each EU member to fine violating companies up to 4% of revenue.[142] For companies like Facebook, which had a 2018 revenue of over $55 billion, the fine structure could potentially be in excess of $2 billion.[143]

Perhaps the most significant concern with the GDPR is that many U.S. companies will need to comply with the regulation, as it applies to all entities processing EU residents' data, even if the entities are not EU corporations.[144] The broad applicability of the regulation means that U.S. companies may face compliance or fines if their operations bring them

137. The GDPR purports to apply to all entities which process European Union citizens' data. Specifically, article III of the GDPR applies to U.S. companies who collect the data of EU citizens in marketing or sales, or who collect behavioral information such as with cookies. Alexander Torpey & Emily Carter, *GDPR Compliance for US Companies*, LEXOLOGY (Apr. 5, 2019), https://www.lexology.com/library/detail.aspx?g=28f3e303-b454-4b5a-935c-5f96bc60b89e [https://perma.cc/9M8Q-BZTY]. Thus, U.S. companies in e-commerce that collect EU citizens' data and meet other requirements may be subject to compliance with the GDPR. BENDER, *supra* note 136, § 51.04.

138. *See generally* Rustad & Koenig, *supra* note 21, at 375–81.

139. 6 BENDER, *supra* note 136, § 51.04.

140. *Id.*

141. *Id.*

142. Kate Fazzini, *Europe's Huge Privacy Fines against Marriott and British Airways Are a Warning for Google and Facebook*, CNBC (July 10, 2019, 11:53 AM), https://www.cnbc.com/2019/07/10/gdpr-fines-vs-marriott-british-air-are-a-warning-for-google-facebook.html [https://perma.cc/Z8FB-DHFD].

143. Facebook, Inc., Annual Report (Form 10-K) (Jan. 31, 2019), *available at* https://www.sec.gov/Archives/edgar/data/1326801/000132680119000009/fb-12312018x10k.htm [https://perma.cc/8NQZ-EJJK].

144. 6 BENDER, *supra* note 136, § 51.04.

within the GDPR's scope.[145] Since the GDPR took effect, the United Kingdom Information Commissioner's Office (UK ICO) has levied massive fines against U.S. companies.[146] For instance, the UK ICO fined American hotel chain Marriott $123 million after a breach compromised one of the company's databases, exposing the data of 339 million guests.[147] Fines may potentially be levied against major U.S. tech companies like Google and Facebook as well, which are already under investigation.[148] Facebook, in particular, was already penalized for the Cambridge Analytica scandal, but it is also under investigation for a breach of users' usernames and passwords on Instagram and Facebook.[149] Unlike the relatively weak consumer data protection in the United States, companies transacting business in the EU and subject to the GDPR are forced to comply with this strong data protection regulation to avoid significant penalties.[150]

2. Origins of Data Privacy in Europe

The strong protection of consumer data privacy in the EU as a "fundamental right" evident in the GDPR stems in part from historical events that occurred in the European Union.[151] Commentators have argued

145. *Id.*

146. *See* Fazzini, *supra* note 142.

147. It is worth noting that although the GDPR allows a maximum fine of 4% of revenue, this fine was only 1.5% of Marriott's revenue. *See id.*

148. The U.K.'s Information Commissioner's Office, responsible for enforcing the provisions of the GDPR in the country, is investigating Google for leaking consumer data relating to its advertising platform. Google was already fined 50 million euros (roughly $57 million) in January 2019 for not properly disclosing how data was being used in advertising. *Id.*; *see also*, Adam Santariano, *Google Is Fined $57 Million Under Europe's Data Privacy Law*, N.Y. TIMES (Jan. 21, 2019), https://www.nytimes.com/2019/01/21/technology/google-europe-gdpr-fine.html [https://perma.cc/U2V3-NXRN].

149. *See* Fazzini, *supra* note 142.

150. *See generally* Rustad & Koenig, *supra* note 21, at 389–90.

151. *See generally id.* at 372–73; *see also* Council Directive 2016/680, of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data by Competent Authorities for the Purposes of the Prevention, Investigation, Detection or Prosecution of Criminal Offences or the Execution of Criminal Penalties, and on the Free Movement of Such Data, and Repealing Council Framework Decision 2008/977/JHA, 2016 O.J. (L 119) (recognizing the protection of personal data in data processing is a fundamental right of natural persons); Gregory Voss &

this status as a fundamental right has its origin in major historical events in Europe, such as World War II, in which Nazis and others misused personal data to oppress individuals.[152] Importantly, this history caused European countries to enact broad regulation of data privacy as far back as 1995, with the EU Data Protection Directive, which gave consumers many rights regarding their data.[153]

The strong protection of data privacy also arguably stems from European countries' treatment of a general right to privacy as a personality right.[154] A personality right does not constitute the traditional assets or property of a person.[155] Instead, a personality right "function[s] as a metaphor for the non-bodily aspects of the personality" and is used to legally protect personality interests.[156] Privacy, dignity, and autonomy are aspects of the person that are protected under personality rights.[157] Personality rights are protected under the law of delicts, otherwise known in the United States as torts.[158] Such rights are non-patrimonial,[159] inalienable, and not heritable.[160] This treatment of data as a personality right removes data from the realm of property and places it where a consumer cannot divest their right to privacy.[161] Further, Europe's right to publicity is a "hybrid" right, which incorporates patrimonial property

---

Kimberly A. Houser, *Personal Data and the GDPR: Providing a Competitive Advantage for U.S. Companies,* 56 AM. BUS. L. J. 287, 291 (2019).

152. Rustad & Koenig, *supra* note 21, at 372–73 (discussing the use of records in oppression in the post war period).

153. *Id.* at 373–75 (describing the directive and noting a right to access, a requirement for adequate protection and consent, and a right to collect or delete personal data).

154. *See generally id.* at 372–73.

155. NIALL R WHITTY & REINHARD ZIMMERMANN, RIGHTS OF PERSONALITY IN SCOTS LAW: A COMPARATIVE PERSPECTIVE 316–17 (2009).

156. *Id.*

157. *Id.*

158. *Id.*

159. A person's patrimony is generally considered to be the sum of the person's assets and liabilities, or what otherwise may be considered their net worth. *See* Ronald J. Scalise Jr., *Some Fundamentals of Trusts: Ownership or Equity in Louisiana?*, 92 TUL. L. REV. 53, 67–68 (2017).

160. WHITTY & ZIMMERMANN, *supra* note 155.

161. Umberto Bacchi, *Lack of Rules Leaves Experts Puzzled about Data Ownership after Death*, REUTERS (Feb. 13, 2019, 07:04 PM), https://www.reuters.com/article/us-britain-dataprotection-privacy-analys-idUSKCN1Q304F [https://perma.cc/2MKW-G7P8] (discussing ownership of data relative to various nations after death).

elements while still protecting the personality of the person.[162] Far from a "personality right," protection of data privacy in the United States often leaves consumers without sufficient protection and redress in the event of a data breach.[163]

B. Data Privacy and Protection in the United States

Although the European Union has passed stringent and uniform regulations like the GDPR to address data privacy and protection issues, the United States has not passed a comprehensive consumer data privacy and protection regulation.[164] Consumers have struggled to find relief in the event of a data breach and are left to rely on traditional tort theories of recovery.[165] Statutory protection in the United States is typically in the form of either a state data breach notification law or a sector-specific federal regulation that protects one particular type of data.[166]

1. Traditional Federal Regulations

U.S. data protection laws that affect data privacy are a patchwork of "narrow and sector based" regulations whose protection is limited to a particular type of data and a particular manner of protection for that data.[167] One example of such sector-specific data privacy regulation is the Health Insurance Portability and Accountability Act (HIPAA), which Congress specifically enacted to protect information concerning personal health.[168] HIPAA's main effect on privacy is that it largely prohibits disclosure of patient health information without consent and gives patients distinct rights regarding their own health information.[169] Another sector-specific privacy regulation is the Family Education Rights and Privacy Act of 1974

162. WHITTY & ZIMMERMANN, *supra* note 155.
163. Pierce, *supra* note 130, at 985–88.
164. *Id.*
165. *Id.*
166. Voss & Houser, *supra* note 151, at 291.
167. *Id.* at 300–02.
168. Nash, *supra* note 17, at 215–16.
169. *Id.* Such other rights include a right to access their health records or change them. *Summary of the HIPAA Privacy Rul*e, HHS.GOV, https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html [https://perma.cc/4WB4-KZ72] (last visited Nov. 13, 2020). Additionally, the regulation seeks to balance the legitimate needs for information transfer against privacy interests of individuals.

(FERPA).[170] FERPA imposes limits on the release of certain students' records to third parties and creates methods for students and their guardians to access their educational records.[171] FERPA was one of the first federal laws passed to address important public privacy concerns.[172] Both HIPAA and FERPA represent typical federal data privacy regulations in the United States, as they regulate a single area, health records or student records, respectively, in a very specific manner. Besides this type of federal regulation, individual states have also provided some protection for consumer data.[173]

2. Traditional State Regulations

All 50 states have enacted laws requiring notification in the event of a data breach.[174] However, the laws are not uniform and generally do not prescribe measures that would prevent data protection failures from occurring in the first place.[175] State notification laws vary with respect to events that trigger the notification requirement, the type of data or information covered, and the form of notification.[176] This lack of uniformity does not provide U.S. citizens with a consistent standard of data protection across the country for general consumer data.[177] Although the laws are not uniform, a review of Louisiana's data breach law is instructive of what a data breach notification law generally entails.

---

170. *See* The Family Educational Rights and Privacy Act of 1974, 20 U.S.C. § 1232(g).

171. 5 JAMES RAPP, EDUCATION LAW § 13.04 (2020).

172. Elana Zeide, *Student Privacy Principles for the Age of Big Data: Moving beyond FERPA and FIPPs*, 8 DREXEL L. REV. 339, 354 (2016) (online corrected).

173. Rustad & Koenig, *supra* note 21, at 422–24.

174. *Id.*

175. *Id.*

176. Jeff Kosseff, *Hamiltonian Cybersecurity*, 54 WAKE FOREST L. REV. 155, 175 (2019). For instance, Utah does not require notification after a breach if it appears no misuse of the data has or is likely to occur. UTAH CODE ANN. § 13-44-101, § 13-44-202 (West 2020). However, Texas requires disclosure of a breach if a person's personal information was reasonably believed to be acquired by an unauthorized person. *See* TEX. BUS. & COM. CODE ANN. § 521.053 (West 2020). For a comparison of all states' data breach notification laws, see FOLEY & LARDNER LLP, STATE DATA BREACH NOTIFICATION LAWS (Jan. 10, 2020), https://www.foley.com/en/insights/publications/2019/01/-/media/files/insights/publications/2020/20mc25837-data-breach-chart-010920.pdf [https://perma.cc/38YT-YY6A].

177. *See generally* Pierce, *supra* note 130.

The Louisiana Legislature passed its notification law, the Louisiana Database Security Breach Notification Law, in 2005 and amended it most recently in 2018.[178] In doing so, the legislature recognized that the "privacy and financial security of individuals are increasingly at risk" and aimed to combat identity theft though the statute.[179] The statute protects "personal information," which the law specifies as information that contains a Louisiana resident's last and first names, social security number, bank account number, or driver's license number.[180] The most recent amendment imposes an obligation on persons and legal entities using Louisiana residents' data to "maintain reasonable security procedures" to protect the information, although few specific practices are mandated.[181] Additionally, after a data breach, the data user must notify affected residents within 60 days.[182] The statute further provides a limited civil right of action to residents who were injured as a result of the breach to recover actual damages.[183] Interestingly for the analysis of data ownership, the Louisiana statute already references the ownership or licensing of consumer data by the person responsible for notifying the consumer of the breach.[184]

While a step forward for consumers, state data breach notification laws, like Louisiana's, are substantially less protective of consumers than comprehensive data protection regulations like the GDPR.[185] The purpose and application of most notification statutes are focused on reacting to a data breach, rather than proactively preventing a data breach.[186] California,

178. *See* LA. REV. STAT. § 51:3071–77 (2018); *see also* Micah J. Fincher & Jessica C. Engler, *One Year Later: Louisiana's Database Security Breach Notification Law 2.0*, 67 LA. BAR J. 90 (2019).

179. *See* LA. REV. STAT. § 51:3072.

180. Fincher & Engler, *supra* note 178, at 90.

181. *Id.* at 91.

182. *Id.*

183. *Id.* at 92.

184. *See* LA. REV. STAT. § 51:3074. The statute already contemplates that the data owner or licensor is the appropriate party to protect the data ("maintain reasonable security procedures") and notify consumers in the event of a data breach. It seems that the legislature, in passing the act, assumed that such consumer data can have an owner. *Id.*

185. *See generally* Gergana Sivrieva, *The Equifax Breach Amid a Lawless Landscape: Changes are Afoot For Privacy & Data Security Due to the European Union's General Data Protection Regulation*, 64 WAYNE L. REV. 553, 561–63 (2019).

186. *Id.* at 561.

however, is an exception to the general trend and has passed regulation beyond a general data breach notification statute.[187]

3. The California Consumer Privacy Act: A New Hope in U.S. Data Protection

California enacted the strongest state regulation for protecting consumer data privacy.[188] In 2018, California passed the California Consumer Privacy Act (CCPA), which became effective on January 1, 2020.[189] The CCPA provides consumers with the right to see the information collected on them, to deny consent to the transfer of their data, and to sue those who violate the statute with a limited statutory cause of action.[190] Like the GDPR, the CCPA is designed to protect the data of California consumers by regulating business's processing and use of it.[191] The CCPA and GDPR are similar, as each provides consumers with increased access rights to their data and more control over how companies may use their data.[192] However, there are some major differences between the two, such as the GDPR's profit-based calculation of damages, its requirement of process mapping,[193] and its requirement of an impact assessment.[194] Companies around the world that conduct business in California or collect information from its residents are potentially subject to the CCPA's provisions if they meet certain statutorily defined criteria,

187. *See generally* CAL. CIV. CODE §§ 1798.100–.192 (West 2018) (known as the California Consumer Privacy Act of 2018).

188. *See generally* Determann, *supra* note 8, at 24–25.

189. Rustad & Koenig, *supra* note 21, at 403.

190. *Id.*

191. *Id.*

192. *Id.* at 403 n.215.

193. GDPR compliance requires data process mapping, which requires companies to examine the process of collecting and storing data to ensure they are compliant with the requirements of the regulation. *See* Allan Rooney, *Effective Data Mapping and GDPR Compliance*, FORBES (Nov. 1, 2018, 01:57 PM), https://www.forbes.com/sites/entrepreneursorganization/2018/11/01/effective-data-mapping-and-gdpr-compliance/#52ebb6b2421b [https://perma.cc/H526-QTFM]. The impact analysis is a similar exercise and requires organizations to identify and minimize risks associated with data processing.

194. Rustad & Koenig, *supra* note 21, at 404 (noting that the GDPR fine structure allows up to 4% of revenue for violators while the CCPA is not as stringent; additionally, the GDPR provides for even more proactive assessments of risk and more controls that must be in place to not be violating the act).

such as particular gross revenue requirements.[195] Although the CCPA provides stronger consumer protection, some scholars have argued that the broad extent of the CCPA may unduly interfere with interstate commerce in violation of the Dormant Commerce Clause.[196]

No court has decided whether a comprehensive state data protection regulation like the CCPA violates the Dormant Commerce Clause.[197] The jurisprudence surrounding the Dormant Commerce Clause holds that a state statute may be invalid if the burden on interstate commerce is excessive when compared to the local benefits, even if it regulates a valid local interest.[198] In the data context, a court may hold that a patchwork of state privacy regulations controlling and impeding the flow of data across state lines is unconstitutional for placing a higher burden on interstate commerce than necessary to effectuate a state's interest.[199] It is, therefore, unclear whether each of the 50 states even have the constitutional ability to regulate data collection and use in such a manner as the GDPR because any state regulation may unconstitutionally interfere with interstate commerce.[200] Such privacy laws would likely regulate conduct occurring outside of the state, thereby "excessively burden[ing] interstate commerce," and creating statutory inconsistencies across the states.[201] Each of these aspects of a broad state data privacy regulation would likely offend the Dormant Commerce Clause.[202] Consequently, the CCPA and any similar regulation is subject to a constitutional challenge to its validity in the future, especially once other states pass comprehensive privacy

195. Companies that collect data from California residents; conduct business in the state; and that have yearly gross revenues of more than $25 million, sell the information of 50,000 or more consumers each year, or receive 50% or more of revenue each year from selling personal information will be subject to the CCPA. Stuart D. Levi & Daniel Healow, *California Consumer Privacy Act: A Compliance Guide*, SKADDEN, ARPS SLATE, MEAGHER & FLOM LLP & AFFILIATES, https://www.skadden.com/insights/publications/2019/03/california-consumer-privacy-act [https://perma.cc/36FZ-Q9EX] (Mar. 20, 2019).

196. *See generally* Kosseff, *supra* note 176, at 178–84 (discussing the respective power of states and Congress to regulate cyber security, which affects interstate commerce).

197. *See generally id.*

198. Pike v. Bruce Church, Inc., 397 U.S. 137, 142 (1970).

199. Kosseff, *supra* note 176, at 192–93.

200. *See id.* at 178–84.

201. *Id.* at 192–93. While the regulation of interstate commerce is within the constitutional powers of Congress, states have some ability to regulate areas that may affect commerce among the several states as long as the burden imposed on interstate commerce by doing so is not too great. *Id.*

202. *Id.*

regulations that conflict with one another.[203] Conflict with the Dormant Commerce Clause may ultimately limit a state's ability to legislatively protect consumers from data breach.

4. Protection in Tort: Foundation, Current State, and Issues

Although data privacy in Europe stems from the protection of privacy as a "fundamental right," protection of the right to privacy in the United States is arguably not as extensive and historic.[204] Scholars suggest that the first real appearance of the right to privacy in the United States was in Samuel Warren and Louis Brandeis's Harvard Law Review article "The Right to Privacy."[205] The article discussed how the law of persons and property inevitably evolved to require protection of one's solitude and privacy.[206] In cases involving infringement of privacy rights, courts have noted that private information is that which is "intended for or restricted to the use of a particular person or group or class of persons" and not "freely available to the public."[207]

Although privacy protection in the United States continues to increase, it is still not as strong as Europe's non-patrimonial right of privacy.[208] Federal and state courts' protection of privacy has led many victims of data breach or misuse to sue for recovery under various privacy torts or a negligence theory.[209] Currently, plaintiffs in the United States may seek redress for an invasion of privacy under several recognized privacy torts such as appropriation of name or likeness, intrusion upon seclusion, publication in a false light, or public disclosure of private facts.[210] However, in the data breach context, there are special issues that may limit the effectiveness of such a consumer's tort claim.[211]

---

203. *See id.* at 178–84.

204. Voss & Houser, *supra* note 151, at 295–96.

205. *Id.* (noting that the right to privacy is not mentioned in the Constitution).

206. Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 193–95 (1890).

207. U.S. Dep't of Just. v. Reps. Comm. for Freedom of the Press, 489 U.S. 749, 763–64 (1989).

208. *See generally* Voss & Houser, *supra* note 151, at 296–97.

209. Michael Simpson, *All Your Data Are Belong to Us: Consumer Data Breach Rights and Remedies in an Electronic Exchange Economy*, 87 U. COLO. L. REV. 669, 685 (2016).

210. Bradix v. Advanced Stores Co., 226 So. 3d 523, 530 (La. Ct. App. 4th Cir. 2017).

211. *See id.* (declining to find standing or an invasion of privacy over an inability to prove damages in a data disclosure context).

In *In re Facebook, Inc., Consumer Privacy User Profile Litigation*, the U.S. District Court for the Northern District of California addressed the success of a privacy tort claim in the data breach context.[212] There, Facebook users brought suit over the company's disclosure of profile data during the Cambridge Analytica scandal.[213] The court found the plaintiffs had standing on only the privacy claim regarding the general widespread disclosure of their personal information.[214] The court reasoned that a privacy invasion, here in the form of an unauthorized data sale, could be an "actual injury" sufficient to confer standing.[215] In reaching its conclusion on the standing issue, the court noted the longstanding protection of privacy in addition to many other cases where common law courts allowed claims of injuries allegedly caused by data breaches to proceed.[216] Nonetheless, the court recognized that courts in other data breach cases did not find an actionable privacy injury or standing on their tort claims.[217] Although this particular court found standing on the plaintiff's privacy claims, in the absence of any regulation conferring a right of action, victims of data breach in the United States have faced significant hurdles to relief in the courts, mainly in the form of standing.[218]

In contrast to the *In re Facebook* court, other federal courts have held that data breach victims lack Article III standing after reasoning that the victims' injuries are not "actual or imminent" because no actual harm from the breach has occurred yet.[219] State courts have also been reluctant to find standing in data cases over the harm issue.[220] Federal and state judges have reached such a holding in spite of the supposed general judicial protection from injury to one's privacy.[221] As scholars have noted, much of a data breach victim's protection, or lack thereof, depends upon overcoming this

212. *See* discussion *supra* Part I.C.

213. *See generally In re* Facebook, Inc., Consumer Priv. User Profile Litig., No. 18-md-02843-VC, slip op. at 14 (N.D. Cal. Sept. 09, 2019) (Pretrial Order No. 20: Granting in Part and Denying in Part Motion to Dismiss First Amended Complaint).

214. *Id.* at 13–18.

215. *Id.*

216. *Id.*

217. *Id.*

218. *See generally* Sivrieva, *supra* note 185, at 558–61.

219. Marcus, *supra* note 15, at 566-69; *see also*, Clapper v. Amnesty Int'l USA, 568 U.S. 398, 398 (2016).

220. *See* Bradix v. Advanced Stores Co., 226 So. 3d 523, 530 (La. Ct. App. 4th Cir. 2017) (declining to find standing or an invasion of privacy over an inability to prove damages in a data disclosure context).

221. *See id.*

standing hurdle.[222] The requirement to prove an injury for standing is particularly difficult to show in the data breach context because several courts require a showing that the hacker or thief actually used the stolen consumer data and an actual injury already occurred or that such use and injury is imminent.[223] Although the court in *In re Facebook* found standing on the privacy claim, a motion to dismiss for lack of standing may defeat other privacy claims in the data breach context.[224]

Even if the court finds that the plaintiff has standing, a case brought under a negligence tort theory of recovery[225] may still fail because of an inability to prove damages.[226] As part of a general negligence analysis in tort, one must prove damages.[227] Like the standing issue for such a case to be brought in federal court, courts often require the plaintiff to show damages in the data breach context beyond the mere unauthorized disclosure of information.[228] Although data breach or misuse impedes a victim's control of his data, actual damage, beyond the minimal impairment of a right, must generally be shown in a traditional negligence context.[229] The requirement of actual harm or damage may limit what is redressed in a privacy tort context compared to what could potentially be redressed with property rights and the tort of conversion or trespass.[230]

Generally, no tort prevents the dissemination of truthful information that is not damaging to a person's reputation because in such a case no harm has occurred.[231] Pure data is not harmful because it is solely a fact or manifestation of a fact, and until used in a fashion detrimental to the

---

222. For a federal court to hear a case, the Supreme Court requires a party to have a "concrete and particularized," "actual or imminent" "injury in fact" to find Article III standing. Standing is what the Constitution requires for a person to bring a claim into, in this case, federal court. *See* Clapper v. Amnesty Int'l USA, 568 U.S. 398, 409 (2013).

223. Marcus, *supra* note 15, at 566–75.

224. *See generally* Sivrieva, *supra* note 185, at 558–561.

225. *See Bradix*, 226 So. 3d at 529 (noting that to prevail under Louisiana's duty risk analysis a plaintiff must prove: existence of a duty, breach of that duty, the breach was cause in fact of the damage, and actual damage).

226. *See* Kesan & Hayes, *supra* note 30, at 316, 323.

227. For the duty risk analysis under Louisiana Law, see generally Tyson v. King, 29 So. 3d 719 (La. Ct. App. 3d Cir. 2010).

228. *See generally id.* at 722 (noting that in the duty-risk analysis, actual damages must be shown).

229. Simpson, *supra* note 209, at 685–87.

230. *See generally* CamSoft Data Sys. v. S. Elecs. Supply, Inc., 2019 CA 0731, 2019 WL 2865359, at *6 (La. Ct. App. 1st Cir. July 2, 2019).

231. *See In re* Horizon Healthcare Servs. Data Breach Litig., 846 F.3d 625, 639 (3d Cir. 2017).

consumer, actual tangible damages have not occurred.[232] One further issue with tort claims is that they are generally based on the common law torts of an individual state; thus, the elements of a claim, such as the standard of care, may differ depending on the forum.[233] Although a single corporation collecting data can operate in multiple states, a consumer may obtain a different result in a data breach case depending on the forum in which he sues.[234] Thus, tort law does not guarantee a predictable result for corporations or consumers in the aftermath of a data breach.

Plaintiffs are also unable to contract around the pitfalls of tort to find relief.[235] The modern realities of a technologically-driven society require consumers to accept privacy agreements for access to increasingly necessary digital services.[236] Essentially, these privacy agreements are contracts of adhesion[237] that consumers must sign if they want access to such services.[238] The disparity in bargaining power between a single consumer and technological giants, such as Apple, is evident.[239] As such, even though the contract may not be enforceable as a contract of adhesion, consumers are still unable to effectively bargain for more data privacy protections.[240] The limitations of consumers' ability to contract around privacy concerns and the inability to find relief in the courts necessitates a novel solution.

III. DATA AS AN ITEM OF PROPERTY

While also recognizing business needs for data in light of its increasing importance, the interests of the consumer in data privacy must be safeguarded to adequately provide redress following a data breach.[241] The general privacy-based tort approach has not adequately protected

232. *See generally* Int'l News Serv. v. Associated Press, 248 U.S. 215 (1918).

233. Kosseff, *supra* note 176, at 177–78.

234. *Id.*

235. *See generally* Anne Logsdon Smith, *Alexa, Who Owns My Pillow Talk? Contracting, Collateralizing, and Monetizing Consumer Privacy Through Voice-Captured Personal Data*, 27 CATH. U. J. L. & TECH. 187 (2018).

236. *Id.* at 203–07. Such privacy agreements may be present in using a music streaming software, setting up an online bank account, or in online shopping.

237. A contract of adhesion is a standard form contract were one party has less bargaining power than the other. *See* Aguillard v. Auction Mgmt. Corp., 884 So. 2d 1257, 1259 (La. Ct. App. 3d Cir. 2004) (discussing jurisprudence and doctrinal definitions of adhesion contracts).

238. *See generally* Smith, *supra* note 235, at 205–08.

239. *Id.*

240. *Id.*

241. *See generally* Marcus, *supra* note 15.

victims of a data breach, and privacy agreements provide little aid to a consumer who seeks redress under contract.[242] Courts and legislatures should recognize property rights, or quasi-property rights, in data, which would allow questions involving data protection and breach to be dealt with more effectively using a property regime.[243] Specifically, rights of or akin to ownership should be created for data, the "raw materials" that corporations are using to derive information.[244]

Currently, whether data is an item of property is unsettled, and much debate centers on whether data can or should be owned at all.[245] To some extent, consumers believe they should own their data, although they currently cannot utilize it, and corporations act as though they own consumer data when they exploit it and structure complex data transactions.[246] If courts are able to apply well-established property principles on a state-by-state basis, even in the absence of a federal uniform privacy regulation, they can more effectively deal with data issues and protect the interests of all involved. When a state or national regulation is passed, the conception of data as property would provide a useful foundation for the structure of the regulation.[247] To determine whether and how property rights may be applied to data, this Comment first examines data's fit into the traditional notion of property law. Specifically, an analysis of data's fit in Louisiana's civilian property law under the Louisiana Civil Code serves as guidance.

A. Making "Things" with Clay

The question of whether an individual can own data lies at the core of an attempt to assign property rights to data.[248] Data must be a thing or type of thing to which property rights can attach for a property-based approach to apply.[249] Property in civilian legal doctrine is traditionally considered a "thing" or a right to a thing.[250] Under Louisiana law, if data is a "thing" to

242. *See generally id.* at 581–82.
243. *See generally* Ritter & Meyer, *supra* note 12.
244. *See generally id.*
245. *See generally* SHAPIRO & ANEJA, *supra* note 105.
246. *Id.*
247. *See generally* Ritter & Meyer, *supra* note 12.
248. *See generally* Determann, *supra* note 8, at 4.
249. *See generally* Ritter & Meyer, *supra* note 12, at 223 (arguing that data is a thing and for a property-based approach to data transactions).
250. *See* LA. CIV. CODE art. 448 (2018). Although the titles of articles are not the law, this article concerns the division of things in Book 2 of the Civil Code, on things and the different modifications of ownership.

which property rights are assigned, Book 2 of the Louisiana Civil Code titled "Things and the Different Modifications of Ownership" must govern it.[251] Under the Civil Code, things are classified based on who may own them, their corporeality, and their movability.[252]

1. Data: A Corporeal Movable

The Louisiana Civil Code divides things into several categories, including immovables and movables and corporeals and incorporeals.[253] Data's fit in the aforementioned categories will determine if data falls into a recognized category of property and thus is amenable to the application of property principles.[254] In general, land and its component parts are immovables, and every other type of property, such as phones, cars, and other personal property, is a movable.[255] If legal scholars, judges, and legislators are to classify data as either type, it must be a movable because it is not land. Beyond that initial classification, corporeal things are those that are tangible.[256] In contrast, incorporeals are things that are "comprehended by the understanding" and include rights, such as ownership, to things including both movable and immovable property.[257] Accordingly, if "rights, obligations and actions" are granted over a movable thing, they are incorporeal movables, and they are incorporeal immovables if granted over an immovable.[258] Consumer data is not a "right, obligation, or action" on land so it may not be an incorporeal immovable.[259] Although data does not have "a body" that one can touch in the traditional sense contemplated for a corporeal thing, there is Louisiana jurisprudence suggesting that data could be corporeal.[260]

---

251. LA. CIV. CODE art. 448–76 (2019) (Book II, Title 1, entitled "Things").

252. *Id.* art. 448. These divisions are the main distinctions between the types of property in Louisiana law and things of property must find a classification among them.

253. *Id.*

254. *Id.*

255. *Id.* art. 462; *id.* art. 471; *id.* art. 475.

256. *Id.* art. 461. Tangibility itself is often the distinction outside of Louisiana where the concept of corporeality is not used. In the common law, tangible items may be the subject of an action for conversion or intangible items that are merged with a document. 7 STUART SPEISER ET AL. AMERICAN LAW OF TORTS § 24:6 (2020), Westlaw AMLOT.

257. *Id.* art. 461.

258. *Id.* art. 740; *id.* art. 473.

259. *Id.* art. 740; *id.* art. 473.

260. *Id.* art. 461.

In *South Central Bell Telephone Co. v. Barthelemey*, the Louisiana Supreme Court held that software was a corporeal movable for purposes of a sales and use tax imposed on "tangible personal property."[261] In deciding the case, the court noted that scholars such as Planiol [262] typically distinguished between incorporeals as rights and corporeals as physical objects.[263] Due to this distinction, the court reasoned that the recordings of software at issue are not rights "to be comprehended by the understanding" but are things that existed in the physical world.[264] The court further noted that as software became a more frequent focus of legal disputes, judicial understanding increased and judicial attitudes shifted across the country toward holding software to be tangible.[265]

Like the software at issue in *South Central Bell Telephone*, data is "physically manifested in machine readable form" using electrical input.[266] Additionally, like the software, data is not solely incorporeal knowledge.[267] Data is knowledge "recorded in a physical form which has physical existence" and "can be perceived by the senses."[268] It is less like a right or idea than a recorded "arrangement of matter" and should thus be classified as corporeal.[269] Additionally, electronic data must be stored somewhere; therefore, it is intertwined with other corporeal technological elements.[270] Just as software may have property rights affecting it, such as a copyright, without the software itself being a right, so should rights be allowed in data, primarily a right of ownership or quasi-ownership.[271]

Although *South Central Bell Telephone* supports the idea that data can be classified as an item of property, the Louisiana First Circuit Court of Appeal declined to extend the Louisiana Supreme Court's reasoning in

---

261. *See* S. Cent. Bell Tel. Co. v. Barthelemy, 643 So. 2d 1240 (La. 1994).

262. Planiol was a well-respected professor and scholar of the 19th and early 20th century whose *Civil Law Treatise* is heavily relied upon in interpretations of Louisiana law. *See generally* 1 MARCEL PLANIOL & GEORGE RIPERT, TREATISE ON THE CIVIL LAW, 13–23 (12th ed. 1939).

263. *S. Cent. Bell Tel. Co.*, 643 So. 2d at 1244.

264. *Id.*

265. *Id.* at 1245.

266. *Id.* at 1246.

267. *See generally id.*

268. *See generally id.*

269. *See generally id.*

270. *See generally id.* at 1248.

271. "Quasi-ownership" in this sense refers to similar rights that would accompany an owner of a thing, even if the item at issue may not fit perfectly with traditional conceptions of property. It essentially is an attempt to assign rights of ownership without necessarily resolving completely the issue of whether the item fits into the traditional categories of property. *See generally id.* at 1248–49.

South Central to *CamSoft Data Systems v. Southern Electric Supply, Inc.* in 2019.[272] In *CamSoft,* the plaintiff sued for the appropriation of business plans, pricing information, and other information from its business under the tort of conversion, which provides owners with a remedy for unlawful interference with a movable.[273] Ultimately, the court declined to "extend the tort of conversion to immovable, intangible information."[274] In so holding, the court noted the result in *South Central Bell Telephone* but focused purely on the Supreme Court's analysis of the physicality of the recording of software in that case.[275] The court ultimately did not allow a claim for conversion of the information, including some data, due to its focus on the physicality of the information, the lack of any evidence that the defendants stole the information in a physical form, and the continued ability of the plaintiff to use the information after the misappropriation.[276]

The *Camsoft* holding, however, does not focus on the Supreme Court's analysis of the nature of software as digital information, which is far more similar to data than the information allegedly converted in the case.[277] Additionally, the First Circuit's categorization of the information was in error, as an "immovable, intangible" thing would be an incorporeal immovable, which the Civil Code defines as a right to immovable property.[278] From the facts reported in the case, this characterization is not an appropriate classification under the Civil Code.[279] For these reasons, *South Central Bell Telephone* and not *Camsoft* should govern a consideration of data as property and supports data's characterization as such. Once data may be classified as a thing of property, the next obstacle to a property-based data regime , particularly under Louisiana law, centers on who may own the data. The Louisiana Civil Code's distinction between private, common, and public things answers the question of who may own a thing.[280]

---

272. *See generally* CamSoft Data Sys. v. S. Elecs. Supply, Inc., 2019 CA 0731, 2019 WL 2865359 (La. Ct. App. 1st Cir. July 2, 2019).
273. *Id.* at *7.
274. *Id.*
275. *Id.* at *8 n.3.
276. *Id.*
277. *See generally id*.
278. LA. CIV. CODE art. 470 (2018).
279. *Id.*; *id.* art. 473.
280. *See id.* art. 448.

2. Who May Own the Data?

The Louisiana Civil Code provides that a thing must be either a public thing, a private thing, or a common thing.[281] The state or its political subdivisions own public things in their public capacity, and such things include public roads and the seashore.[282] Civil Code article 453 states that private things are owned by those other than the state or its subdivisions, or by the state or its political subdivisions "in their capacity as private persons."[283] Private things are susceptible of ownership, and they are generally what a lay person would consider as "property," such as vehicles and buildings.[284] Finally, common things are those which "may not be owned by anyone" such as "the high seas."[285] Accordingly, persons may freely use common things in conjunction with nature's intended use.[286] Common things may be susceptible of ownership when removed from the commons.[287] Although the entire high seas are not capable of ownership, removing a gallon of water or a container of air for a person's reasonable use may reduce that captured subset of the thing to possession and ultimately ownership by occupancy.[288] Data may be considered public, private, or common; in particular, the idea of "the commons" or common things may have much relevance to data.

Data may be analyzed as a public, private, or common thing.[289] Because public things are "owned by the state or its political subdivisions," a private company's data or an individual's data cannot be classified as a public thing.[290] However, voter information or other data a state actor holds in its public capacity that is generally available to the public may fall under the public category.[291] Data that individuals or legal entities such as corporations "own" may also be classified as a private

281. *Id.*
282. *Id.* art. 450.
283. *Id.* art. 453.
284. *Id.* These things may include cars, cell phones, and any other number of items that the reader may own or possess. *Id.*
285. *Id.* art. 449.
286. *Id.*
287. *See generally* Pierson v. Post, 3 Cai. R. 175 (N.Y. 1805) (discussion of ownership by occupancy of a fox, once held in the commons, that had been killed.)
288. *Id.* art. 3412; *id.* art. 3413 (which notes that animals may be owned in public by the state or may not have an owner, which would be in the commons like in Pierson).
289. *See generally id.* art. 448.
290. *Id.* art. 450.
291. *Id.*; *see Find Voter or Parish Specific Information*, LA. DEP'T OF STATE, https://voterportal.sos.la.gov [https://perma.cc/PMU6-GXZ7].

thing.[292] Under a property regime for protecting consumer data, much of the data that corporations hold may be a private thing once captured.[293]

Additionally, some types of data can be a common thing at various points in the generation and life of the data.[294] "The commons" is described as neither private nor public in a general sense and also in the distinction between types of property in the Louisiana Civil Code.[295] A key attribute of a thing in the commons is that it cannot be put on a market to obtain its "exchange value," or the value it may be worth in a transaction.[296] The commons is recognized for the community interest, like the recognition of the high seas as available for all to use.[297] Specifically in the context of intellectual property law, information is generally not protected when it is found to be in the commons or otherwise in the public domain.[298] Privacy may also yield to the commons.[299] For instance, in criminal law, it is not a search or an invasion of privacy when an officer observes evidence of a crime in a public place where he is allowed to be.[300] Like constitutional privacy rights, data privacy may necessarily yield if data exists as part of the commons. For example, a data point which details a GPS location in a public park is seemingly describing information that was in the commons.[301] Someone may legitimately follow a subject and observe their location in the park, and the person would have no expectation that that "data point" may be a secret.[302] Although an oversimplification, in such

---

292. *See generally id.* art. 453.

293. *See generally id.* In this context, data is captured when it is recorded in a tangible medium.

294. *See generally id.* art. 452.

295. *See generally* FRITJOF CAPRA & UGO MATTEI, THE ECOLOGY OF LAW: TOWARD A LEGAL SYSTEM IN TUNE WITH NATURE AND COMMUNITY 149 (2015).

296. *Id.*

297. *Id.*

298. Feist Publ'ns, Inc. v. Rural Tel. Serv. Co., 499 U.S. 340, 348 (1991) (noting that facts are part of the public domain available to every person and may not be copyrighted).

299. *See generally* Florida v. Riley, 488 U.S. 445 (1989).

300. *See generally id.* (holding that a fly-over by police in helicopter was not a search where the helicopter followed aviation guidelines and was where it was allowed to be in the airspace).

301. If a person records the fact independently, such as when a person happens to be in another's photograph, there is seemingly no claim that the photographer has taken something that is theirs. The fact is something for all to perceive as they move through their daily life. *See, e.g.*, CAPRA & MATTEI, *supra* note 295.

302. Obviously, this poses problems of criminal activity, stalking and the like. However, it does illustrate that certain data points, at certain times, should be

case, it may be said that they have effectively released it to the public domain.[303]

In *Moore v. Regents of the University of California*, the California Supreme Court's finding that any property rights a blood donor held over the sample that he relinquished can approximate this idea of a release of property into the commons.[304] The court held that a patient had no protectable property interest in samples of blood that researchers used without his knowledge to create extremely valuable cell lines for treating leukemia.[305] In reaching this conclusion, the court noted the patient's lack of expectation of a retention of ownership interest in his blood after the researchers drew the samples.[306] Although *Moore* is a case from California, under Louisiana Law the sample in *Moore* could properly be classified as abandoned because the patient did not intend to own it any further.[307] Additionally, under the law of occupancy,[308] one who takes possession of a corporeal movable that no one owns acquires ownership upon taking possession.[309] Thus, if data is a corporeal movable as discussed above, it is susceptible, if unowned at some point, to being acquired by occupancy.[310]

Ultimately, data is susceptible to categorization under Louisiana's property law scheme and potentially in the property regimes of other states.[311] Although data may fall within a well-defined category of property, it is worth considering whether property rights should be allowed in data at all. Indeed, data does not engender the same policy considerations of promoting creativity and invention that prompted property rights in intellectual property, as data is more like a fact.[312] Additionally, certain elements of data may be in the public domain and perhaps should not be owned by an individual.[313] However, there are

---

insusceptible of ownership by themselves and outside of the context of recordation.

303. *See generally Riley*, 488 U.S. 445.

304. *See generally* Moore v. Regents of the Univ. of Cal., 793 P.2d 479 (Cal. 1990).

305. *Id.* at 480–81.

306. *Id.* at 488.

307. LA. CIV. CODE. art. 3418 (2018).

308. *Id.* art. 3412. "Occupancy is the taking of possession of a corporeal movable that does not belong to anyone. The occupant acquires ownership the moment he takes possession." *Id.*

309. *Id.*

310. *Id.*

311. *See* discussion *supra* Part III.

312. *See generally* Determann, *supra* note 8, at 25–26.

313. *See generally id.* at 38–39.

considerations that affect and support the application of property principles and rights to data.

B. Should Property Rights in Data Be Allowed?

Although data can fit into a property regime, the question remains as to whether it should. Property rights are flexible, and the law provides remedies for the impairment of a property right when other areas of the law may not.[314] Property enjoys strong protection and has evolved to reflect social determinations about the balances between competing parties' rights.[315] Although data misuse implicates privacy, which has traditionally been redressed in tort, U.S. courts have largely been unable or unwilling to protect the individual associated with the data after a breach for issues such as standing and damages.[316] For whomever would possess the property rights to data, data property rights would theoretically alleviate the standing issue in the event of a breach, as the cognizable injury would be the impairment of one or more of a data holder's well-established bundle of rights.[317] Furthermore, a property regime may allow new theories of recovery for plaintiffs to bring claims under existing property-based torts such as conversion or trespass.

Failure to treat data as property ignores the reality of data itself and how businesses in the information-based economy function.[318] According to Justice Holmes in *International News Service*, property rights do not necessarily arise from the fact that a thing has value, but from the need for other rights, such as the right to exclude others from the thing or to be free from interference in the thing.[319] Companies already act to exclude others from the data they have collected through firewalls and other security measures.[320] Once businesses collect consumer data they should

314. *See generally* Lipton, *supra* note 46.

315. *See generally id.* at 160–67 (discussing the balancing of rights in intellectual property and how a similar balance could be made in information property rights more broadly).

316. For an example, see Bradix v. Advanced Stores Co., 226 So. 3d 523, 529 (La. Ct. App. 4th Cir. 2017).

317. In the tort of conversion, the interference with the ownership or possessory rights of a corporeal moveable is grounds for the action. *See* CamSoft Data Sys. v. S. Elecs. Supply, Inc., 2019 CA 0731, 2019 WL 2865359, at *6–7 (La. Ct. App. 1st Cir. July 2, 2019).

318. *See generally* Ritter & Meyer, *supra* note 12.

319. Int'l News Serv. v. Associated Press, 248 U.S. 215, 234 (1918).

320. Bianca Male, *10 Essential Data-Security Measures Every Business Should Take*, BUS. INSIDER (June 8, 2010, 10:08 AM), https://www.business

reasonably protect that data, regardless of who owns it, because it contains private information that may cause harm in the wrong hands.[321] Collected consumer data is not open to the public domain at that point, and if a hacker appropriates this stored data, he may have criminal charges brought against him.[322] If property rights arise from such needs as the right to exclude as Holmes posited, it appears data is already being treated in a similar manner—as if it were owned—and it should merit similar property rights.[323] Holders of consumer data may restrict access to consumer data to outsiders, and are even expected to do so under regulations like the GDPR.[324] The owner or holder of property interests in data should have some version of a right to exclude and other property rights to protect their own efforts and to protect consumers from others' misuse.[325]

Furthermore, the flexibility of property rights, which allows courts and legislatures to modify and limit them for societal balances, supports the application of property rights to data.[326] Although data is a poor fit with and generally excluded from protection under current U.S. intellectual property law, intellectual property law is illustrative of the nuanced balancing between the competing interests that property may seek to protect.[327] Intellectual property seeks to encourage invention and creativity by balancing the promotion of information in the public domain to keep open the building blocks of such innovation, while also providing limited monopolies to incentivize creation.[328] A similar balance between the interests of consumers and companies in data may be struck in property law.[329] As property rights are not absolute, the judiciary or legislature

---

insider.com/10-essential-data-security-measures-every-business-should-take-2010-6 [https://perma.cc/Z2DC-NVCZ].

321. *Protecting Personal Information: A Guide for Business*, FED. TRADE COMM'N (Oct. 2016), https://www.ftc.gov/tips-advice/business-center/guidance/protecting-personal-information-guide-business.

322. Sinead Baker, *A Russian Man Pleaded Guilty over One of the Biggest-Ever Hacks, Where 100 Million People's Data Was Stolen from US Companies Like JPMorgan Chase*, BUS. INSIDER (Sept. 24, 2019, 07:33 AM), https://www.businessinsider.com/andrei-tyurin-russian-pleaded-guilty-hacking-us-firms-jpmorgan-chase-2019-9 [https://perma.cc/X6UX-LBYX].

323. *See generally* Ritter & Meyer, *supra* note 12.

324. *See generally id.*; *see also* 6 BENDER, *supra* note 136.

325. *See generally* Ritter & Meyer, *supra* note 12, at 222–23.

326. *See generally* Lipton, *supra* note 46 (discussing the application of some traditional property principles to information property in general).

327. *See generally id.* at 153–65 (for a discussion of the balancing of interests in "fair use" of copyright).

328. *See generally id.*

329. *See generally id.*

could fashion a workable solution to balance competing interests in data.[330] Though many different property principles, such as licensing, may apply to data depending on how it is categorized and to whom property interests are assigned, assigning property interests will allow courts to more clearly decide cases and provide consumers and businesses with clearer expectations in the use of data.[331]

Based on the properties of data, data's ability to be defined with familiar property classifications, its value, the economic realities of modern data, and the need for traditional property rights in data such as the right to exclude, property rights or quasi-property rights should be assigned to data, if not true ownership.[332] Well-settled property principles are helpful to determine what property interests may apply and to whom they will be granted.[333]

IV. FROM CLAY TO CRUDE

As technology changes and society evolves, new things are created that may be classified as property. Other scholars have found comparisons between new things and well-established property law to be instructive in determining how to treat these new items of property.[334] Therefore, an approach derived from the rule of capture found across the country in the area of mineral rights may be illustrative of how property principles could be applied to data. The history of the rule of capture and its role in general property law are fundamental to understanding the rule and how it can apply to data.

A. Whose Oil Is It Anyway?

The rule of capture was initially a common law rule developed in the 1800s out of the need to address a timely and unique problem—the drilling of oil wells.[335] The rule gradually evolved in state courts after the first oil well was drilled in Pennsylvania in 1859.[336] Under the rule of capture, a party with the right to explore for minerals on a tract of land, whether through ownership or another mineral right such as a mineral servitude,

330. *See generally id.* at 135.
331. *See generally id.*
332. *See generally* Ritter & Meyer, *supra* note 12.
333. *See generally* Lipton, *supra* note 46.
334. *See generally id.*
335. *See* Bruce M. Kramer & Owen L. Anderson, *The Rule of Capture – An Oil and Gas Perspective*, 35 ENV'T L. 899, 900 (2005).
336. *See id.*

takes ownership of the oil and gas when it is reduced to possession.[337] The lawful possessor then becomes the owner of that oil and gas once produced from his well and reduced to possession, even if it migrated from under the land of another.[338] Courts developed the rule because of the difficulty of determining whose subsurface the oil and gas actually came from.[339] The difficulty occurs because oil and gas are fugitive and may migrate from the land under which they originally resided.[340] For policy reasons, it would be difficult, if not impossible, if landowners had a property interest in individual molecules of oil and gas beneath their land and could bring an action for trespass or conversion of those molecules when others reduced them to possession through a lawfully drilled well on neighboring property.[341] Additionally, courts adopting the rule of capture intended to promote the exploitation of oil and gas by rewarding those who were actively trying to produce it.[342] Historically, the only remedy for the party who could not claim production from a well on another's property was to drill an offset well of one's own to capture as much oil as possible from the common reservoir.[343] Ultimately, this "self-help" remedy of offset drilling led to waste and inefficiency in production from a single pool.[344] Because of this, states created conservation statutes that were designed to reduce waste and to efficiently protect the mineral supply.[345] These regulations provided for pooled or unitized drilling, area restrictions, and other methods to control production.[346]

Although most states recognize the rule of capture in the oil and gas context, a divide exists among states on whether fugitive minerals, such as oil and gas, can be owned "in place" with the land while still in the

337. *See generally* Kelley v. Ohio Oil Co., 49 N.E. 399 (Ohio 1897) (an early case discussing the rule of capture); *see also* LA. MIN. CODE art. 8 (2019). "Minerals are reduced to possession when they are under physical control that permits delivery to another." *Id.* art. 7.

338. *See generally Kelley*, 49 N.E. 399; *see also id.* art. 8.

339. *See* Kramer & Anderson, *supra* note 335, at 906.

340. *See id.*

341. Elliff v. Texon Drilling Co., 210 S.W.2d 558, 561–62 (Tex. 1948).

342. *See generally id.*

343. *See generally* Barnard v. Monongahela Nat. Gas Co., 65 A. 801 (Pa. 1907).

344. *Elliff*, 210 S.W. 2d at 562.

345. *Id.* (noting that the Railroad Commission promulgated conservation statutes for well spacing, which while protecting the general interest, allow fairness in each getting his share of the oil and gas in the reservoir).

346. *Id.*

ground.[347] Ownership-in-place states, like Texas, dictate that the owner of the land owns the oil and gas under the ground as part of the land before it migrates to another property, provided there is no outstanding mineral interest.[348] Other states, like Louisiana, provide that fugitive minerals such as oil and gas belong to no one while they are still in the ground and are only owned once they are reduced to possession.[349] Louisiana Mineral Code article 6 codifies this initial lack of ownership and is similar to the law of occupancy.[350] In these non-ownership-in-place states, a landowner of a parcel with no outstanding mineral interest has the right to explore for and produce the minerals, although he does not own them in place.[351] Both types of states still recognize the rule of capture because of the aforementioned logistical problems associated with determining from under whose property the extracted oil originated.[352]

The rule of capture's result—that the one who captures the minerals owns them—may seem unfair to a landowner with an interest in the exploration of or the ownership of the minerals under his land.[353] However, the landowner whose land is drained is not without a remedy in all cases.[354] Besides the self-help remedy of offset wells, a doctrine of "correlative rights" is often recognized judicially and even by statute in Louisiana. The doctrine of correlative rights provides that one exercising his mineral right must exercise it with "reasonable regard" for the rights of the landowner and surrounding owners.[355] This doctrine both limits the property rights of the producer and protects the rights of others with an interest in the minerals.[356] Courts have held that if a producer acts unreasonably in his

347. *See* LA. MIN. CODE art. 7 (2019) (noting that although the landowner has the right to search for fugitive minerals such as oil and gas, ownership of the land does not include ownership of those minerals).

348. Texas is an ownership-in-place state. *See Elliff*, 210 S.W. 2d at 582.

349. *See id.* art. 6; *id.* art. 7 (noting what constitutes possession).

350. *See id.* art. 6 (noting that although the landowner has the right to search for fugitive minerals such as oil and gas, ownership of the land does not include ownership of those minerals).

351. *Id.* art. 8 ("A landowner may use and enjoy his property in the most unlimited manner for the purpose of discovering and producing minerals, provided it is not prohibited by law."). This article codifies the ability of an owner to explore for oil and gas, even though Louisiana is not an ownership-in-place state.

352. *Elliff*, 210 S.W. 2d at 582.

353. *See generally id.*

354. *See generally id.*

355. LA. MIN. CODE arts. 9, 11.

356. *Elliff*, 210 S.W. 2d at 583 (noting that the correlative rights in production among landowners was created due to the distinct nature of oil and gas).

production, for example, if he is wasteful or causes a blowout,[357] he can be liable to others for the damage to their interest in the underlying reservoir.[358] In this way, the right to explore is not absolute and cannot be exercised without regard for others.[359] In Louisiana, restriction on drillers' unbridled use of their property interest is codified in Mineral Code article 10, which provides for liability for a person who "deprive[s] another intentionally or negligently of the liberty of enjoying his rights" or causes him damage.[360] Thus, a party's interests may be protected from another's undesirable behavior.

Although found in oil and gas law, the rule of capture has roots in the law of occupancy and a similar result may also be found in other contexts.[361] For instance, in the *Moore* case, the scientists obtained ownership of the donor's blood by capturing it and possessing it.[362] To use property law terminology, with no expectation of retention of ownership in the blood sample, the sample could be said to be abandoned and released into the commons by the donor.[363] By exerting effort, intending to own them, and further developing the samples, the researchers could then assert an ownership claim to the ultimate product.[364] This is similar to the producer of oil gaining ownership of the oil once it is extracted and reduced to possession.[365] Additionally, the complexity and amount of disputes that would arise from patients' ownership of each medical sample drawn implicates similar logistical considerations as the ownership of individual oil molecules.[366] Occupancy and the rule of capture in a mineral rights context are instructive in defining property rights in data for many of the same reasons they have been applied in an oil and gas context.

---

357. A blowout is the "uncontrolled flow of formation fluids from a well" that "cannot be contained using previously installed barriers" and may consist of water, oil, natural gas, or a combination of the three. *blowout,* SCHLUMBERGER | OILFIELD GLOSSARY (last visited Feb. 2, 2020), https://www.glossary.oilfield.slb.com/en/Terms/b/blowout.aspx [https://perma.cc/5VZH-2W96].

358. *See generally Elliff*, 210 S.W. 2d at 558.

359. *Id.* at 582–84.

360. *Id.* art. 10.

361. *See* discussion *supra* Part III.A.2. *See generally* Kramer & Anderson, *supra* note 335.

362. *See* discussion *supra* Part III.A.2. *See generally* Moore v. Regents of the Univ. of Cal., 51 Cal. 3d 120 (Cal. 1990).

363. *See generally Moore*, 51 Cal. 3d at 136–37.

364. *See generally id.* at 142–47.

365. *See generally id.* at 120.

366. *See generally id.*

B. Drill Baby, Drill!

The rule of capture allows ownership rights to be defined, to be limited relative to others interests, and to enforce responsibility in the mineral rights context.[367] The rule of capture framework can help scholars, judges, and legislators understand how rights in data property should be delineated, limited, and otherwise protected. Much of the rule of capture can apply to the new problems attending data property rights by analogy, just as the rule of capture was developed to deal with the complexities of property rights after the discovery of oil.[368] Similarly to how oil migrates from parcel to parcel under the subsurface, data appears to move from the person from which it is derived once it springs into existence and is recorded. Additionally, the rule of capture is one example of the balancing of multiple interests in property often undertaken by the judiciary and legislature.[369] As applied to data, the rule of capture may balance both the interests of consumers and businesses in its application. The first step under the application of the rule of capture is to define who owns the data and when. The admittedly uncomfortable result compelled is that the corporations who are actively collecting the data should own it.[370]

1. Data Property Rights Should Be Given to Corporations Capturing It

Like a surface owner's interest in fugitive minerals in a non-ownership-in-place state, a consumer should have a protectable interest in their underlying data.[371] Although consumers cannot monetarily exploit this interest as of yet, as the court in *In re Facebook, Inc., Consumer Privacy User Profile Litigation* noted, a person does have a protectable right to publicity and privacy.[372] In the comparison to mineral rights, it is arguable whether the data subject should own their data "in-place" or whether data should not be owned "in-place," as it may not exist unless

367. *See* discussion *supra* Part IV.A.

368. *See generally* Lipton, *supra* note 46.

369. *See* discussion *supra* Part IV.A. Conservation statutes, correlative rights, and other measures protect others with interests in the underlying oil and gas.

370. *See* discussion *supra* Part IV.A. The rule of capture in an oil and gas context states that he who produces the oil owns it, and thus he who produces or collects the data would own it under this regime.

371. *See generally* Lipton, *supra* note 46.

372. *In re* Facebook, Inc., Consumer Priv. User Profile Litig., No. 18-md-02843-VC, slip op. at 13-18 (N.D. Cal. Sept. 09, 2019) (Pretrial Order No. 20: Granting in Part and Denying in Part Motion to Dismiss First Amended Complaint).

separate from the person.[373] Whatever interest a consumer initially may have in his data changes, however, when a company drills the data "well" and the personal data starts "flowing." Assuming a consumer has some interest in his data "in-place," once separated from the person, especially if consented to in a privacy agreement, a consumer arguably has no reasonable expectation of ownership once the data is collected in a form apart from his person.[374] This is analogous to the lack of an expectation of an ownership interest in the blood samples once drawn and effectively abandoned.[375] Alternatively, data, or any interest in data, might be deemed only to exist at or shortly before its recordation, separately from the consumer who cannot exploit its value, even if consumers believe they have the ownership interest in their data and do not expressly consent to its collection.[376]

At this point, if the data is effectively abandoned or becomes a new thing entirely, the data is fugitive, unowned, and susceptible to capture.[377] If the data is abandoned and in the commons, the party who first takes possession through occupancy could then establish ownership of data, which we have classified as a corporeal movable.[378] Like oil migrating from underneath an owner's land to an adjoining well, by using websites that legally collect data, the data collectors should gain a property interest in the data that is seemingly abandoned, which they capture or collect.[379] The Louisiana Database Notification Law is even written in terms of the data collectors as owners or licensees of personal data.[380] Although value of the thing is not dispositive, much money and effort are spent on data

373. This depends on at what point one believes that data is "conceived." Is it when it is recorded, or does the data reside within the person before it is recorded because the data relates to aspects of the person? *See generally* THE BRITISH ACADEMY, DATA OWNERSHIP, RIGHTS AND CONTROLS: REACHING A COMMON UNDERSTANDING (Oct. 3, 2018), https://royalsociety.org/-/media/policy/projects/data-governance/data-ownership-rights-and-controls-October-2018.pdf [https://perma.cc/9Q2K-3PU6]. Like how the rule of capture applies to both ownership and non-ownership in place states, it might be applied to data regardless of the answer to this question. *See e.g.,* Elliff v. Texon Drilling Co., 210 S.W. 2d 558, 582 (Tex. 1948),

374. *See* generally Moore v. Regents of the Univ. of Cal., 51 Cal. 3d 120, 136 (Cal. 1990).

375. *Id.*

376. *See generally id.*

377. *See* LA. CIV. CODE art. 3418 (2018).

378. *Id.* (establishing that "one who takes possession of an abandoned thing with the intent to own it acquires ownership by occupancy").

379. *Id.*

380. LA. REV. STAT. § 51:3074 (2019).

collection.[381] Additionally, even though the data is not yet refined into information, its disclosure could be damaging to consumers, and those collecting data should have an incentive and right to exclude certain others and protect it from disclosure.[382] Policy considerations regarding value generation, found also at the core of the rule of capture, support businesses having the most data property rights.[383]

Businesses are generally the only party to the generation of consumer data that have the ability to derive economic value from the data.[384] Consumers cannot readily extract the value of their data, as there is not a widely accessible commercial marketplace.[385] However, in business contexts, both through a business's own use and data transactions, data is very valuable.[386] This disparity in the value of data based on who owns it may prompt an application of the principle of relativity of title.[387] Ultimately, organizations may have a better claim to title than the consumers, considering that a thing may be assigned property rights relative to the person in a position to derive value from it.[388]

In *In re Facebook, Inc., Consumer Privacy User Profile Litigation*,[389] the court indirectly discussed this concept of relativity of title regarding data subjects in ruling on Facebook's motion to dismiss.[390] In the case, the

---

381. Betty Ho, *Companies Spend More Than $20b on Data Solutions Each Year*, CRITEO (Dec. 5, 2017), https://www.criteo.com/insights/companies-spend-20b-data-solutions/ [https://perma.cc/E7Z7-J69M].

382. *See generally* Ritter & Meyer, *supra* note 12, at 252–254 (noting that property rights entail corresponding obligations).

383. *See generally* Elliff v. Texon Drilling Co., 210 S.W.2d 558 (Tex. 1948).

384. John Akred & Anjali Smani, *Your Data Is Worth More Than You Think*, MIT SLOAN MGMT. REV. (Jan. 18, 2018), https://sloanreview.mit.edu/article/your-data-is-worth-more-than-you-think/ [https://perma.cc/LA8T-TG44].

385. *In re* Facebook, Inc., Consumer Priv. User Profile Litig., No. 18-md-02843-VC, slip op. at 13–18 (N.D. Cal. Sept. 09, 2019) (Pretrial Order No. 20: Granting in Part and Denying in Part Motion to Dismiss First Amended Complaint).

386. Alan Mitchell, *What Is the Economic Value of Data?*, MEDIUM (Feb. 25, 2019), https://medium.com/mydex/what-is-the-economic-value-of-data-ef129e6485e1 [https://perma.cc/9NCK-WAD5] (discussing how value is derived from data, although the author does not assign monetary figures to the analysis).

387. Relativity of title contemplates that property rights are not necessarily absolute, and that the assignment of property rights often varies depending on the circumstances and parties involved. *See generally* JOSEPH SINGER ET AL., PROPERTY LAW: RULES, POLICIES, AND PRACTICES 155 (2017).

388. *In re Facebook, Inc.*, slip op. at 13–18.

389. *See* discussion *supra* Part I.D.

390. *In re Facebook, Inc.*, slip op. at 13–18.

plaintiffs asserted that they lost the economic value of their data and that had there been no breach, they might have sold the data to brokers or advertisers themselves to realize that value.[391] The court noted that although Facebook derives value from consumers' data by providing it to companies, the once private information did not have "independent economic value to an individual user" in the absence of the breach.[392] Accordingly, the court dismissed this argument and found no injury for the consumers.[393] The court found the plaintiffs had not plausibly alleged that they could find a buyer or a market for their individual information or that they intended to sell it.[394]

Ultimately, if property rights are to be created at all in data, they should not be given to consumers who lack the ability to generate economic value.[395] Consistent with the rule of capture, data property rights should be granted to the capturer who is in a position to generate economic value from them.[396] Consumers still need protection for their data though, as they may suffer more and highly personal damage through data misuse than an adjacent landowner in the mineral rights context.

2. Protecting the Consumer

Although consumers may desire an absolute ownership interest in their own data, to grant them such interest may create significant problems by heavily burdening modern, data-dependent business operations in lengthy disputes over consumers' individual data points.[397] Problems associated with consumers owning their own data may sufficiently invoke the policy considerations of the rule of capture. To assign consumers property rights in individual data points or in other rule-of-capture contexts, such as oil or blood molecules, may "open the floodgates of litigation," which courts are unfit to deal with currently.[398] Conversely, if corporations hold property interests in the data, litigation might more effectively be reduced to the event of a breach or other misuse.[399] Additionally, by placing ownership with the corporations, the burden of protecting the data could be more effectively placed with those who are

391. *Id.*
392. *Id.*
393. *Id.*
394. *Id.*
395. *See generally* Ritter & Meyer, *supra* note 12, at 267–268.
396. *See generally* Elliff v. Texon Drilling Co., 210 S.W.2d 558 (Tex. 1948).
397. *See generally* Determann, *supra* note 8.
398. *See generally id.*
399. *See generally* Ritter & Meyer, *supra* note 12, at 267–68.

using it.[400] Also, at this time it may be more desirable and feasible to place the obligations of data ownership and transactions, such as taxes and other burdens, on the corporations aggregating the data, rather than individual consumers with less financial resources.[401] Assigning consumers or data subjects broad property interests in data would also hinder corporations' ability to generate value from it, thus limiting the value that the marketplace could derive.[402] However, consumers still need protection, and the legal principles attendant to the rule of capture can provide remedies.

Through the creation of correlative rights and conservation statutes in data equivalent to those created in the law of mineral rights, consumers' interests in their data can be protected.[403] Throughout property law, property rights—even the greatest of them, ownership—are rarely absolute.[404] Time limits on patents and other intellectual property, building codes, and even the doctrine of correlative rights are judicially or legislatively imposed restrictions on some aspect of an owner's bundle of property rights.[405] For initial protection for consumers under the data rule of capture, the application of recovery for waste and the doctrine of correlative rights can be structured to allow a consumer to bring an action for negligent or "wasteful" data use, such as allowing a data breach or selling to an irreputable third party.[406] Furthermore, a uniform data protection and privacy regulation like the GDPR can take the place of the conservation statutes used to protect a mineral pool.[407] Federal and state legislatures are likely best suited to serve societal interests, create the aforementioned limits on the data "owner's" bundle of rights, and provide well-defined causes of action for injured consumers.[408] Such limits may include a reasonable limitation on alienability, likely necessary in the personal data context, although generally disfavored in the law,[409] or a

400. *See generally* Lipton, *supra* note 46, at 172.
401. *See generally id.*
402. *See generally* Determann, *supra* note 8.
403. *See* discussion *supra* Part IV.A.
404. *See* Lipton, *supra* note 46.
405. *See generally id.*
406. Elliff v. Texon Drilling Co., 210 S.W.2d 558, 583–84 (Tex. 1948).
407. *See generally* Kramer & Anderson, *supra* note 335, at 952–953.
408. Int'l News Serv. v. Associated Press, 248 U.S. 215, 264–67 (1918) (Brandeis, J., dissenting).
409. Although generally disfavored, restraints on alienation may be valid if reasonable. Particularly in Louisiana, they are upheld if they do not permanently remove the item from the stream of commerce and do not violate public policy. As such, it appears a restraint on the sale of data may be reasonable and promote

limit on the right to exclude the data subject from accessing their data. In these ways, the data owner's right would not be absolute, and consumer interests would be protected.

Eventually, if Americans demand an ownership interest in their data, and if other factors, such as the ability to monetize their own data, materialize, then perhaps the ownership rights would and should vest in consumers.[410] In this case, consumers would be able to exert more authority in the contractual bargaining process with corporations over privacy and might effectively resist consent to data collection.[411] At such a point, other property concepts such as licensing would be required to deal with consumer and corporate data ownership and use.[412] If one could monetize their data, relativity of title would weigh towards greater property interests lying with the subjects of the data.[413] Over time and with the help of legislatures and courts, existing property law principles can be applied to data property in a flexible "quasi-property" manner to accommodate changes in the balance of consumer and business interests in consumer data.

CONCLUSION

The modern issues in the United States surrounding data protection and privacy may be examined and analyzed using old, well-established legal principles.[414] By thinking of data as property, the interests of consumers and business can be better balanced.[415] While recognizing business necessities, the property rights of the business may still be limited to protect consumers' interests in their data.[416] Traditionally, U.S. privacy law in tort has not been an effective remedy for data breach victims.[417] By applying the rule of capture and the corresponding doctrines of correlative rights, consumers may have a stronger right of action when their data is misused.[418] To some degree, this solution simply recognizes how

---

a valuable public policy of consumer protection. *See e.g.,* Mardis v. Brantley, 717 So. 2d 702 (La. Ct. App. 2d Cir. 1998).

410. *See generally* THE BRITISH ACADEMY, *supra* note 372.

411. *Id.*

412. *See generally* Lipton, *supra* note 46.

413. *See* discussion *supra* at Part IV.B.1.

414. *See generally* Lipton, *supra* note 46.

415. *See generally* Ritter & Meyer, *supra* note 12.

416. *See generally id.*

417. *See generally* David Bier, *Integrating Integrity: Confronting Data Harms in the Administrative Age*, 99 B.U. L. REV. 1799 (2019).

418. *See* discussion *supra* Part IV.B.

businesses already operate and how they are treated regarding the data they collect.[419] By recognizing this, however, legislators, courts, and scholars can establish a foundation for data protection regulations and a basis for consumer protection.

Initially, state courts can recognize the application of property principles and rights to data without the immediate need for legislation. Applied by the state and due to ownership resting with the data collector, the property regime may not conflict with the Dormant Commerce Clause.[420] Additionally, this allows courts to draw on well-established and familiar property principles when dealing with novel data breach issues.[421] One method for applying a data property regime would be to use the rule of capture to deal with data issues as described in this Comment. As it stands, it appears that Louisiana is already well positioned to implement such property principles through the Louisiana Civil Code and the legislature's consideration of data ownership in its Database Security Breach Notification Law.[422] While the judicial utilization of a property regime in data would provide a workable solution for many issues regarding data protection and privacy, it would also provide a foundation for subsequent uniform data protection legislation.[423] If, as Justice Brandeis said, policy decisions regarding societal values of property are best left to the legislature, then they may be well advised to also rely on a traditional property-based approach in regulating data when crafting a general data protection law.[424] The most ideal option for consumers, however, may be a recognition that data privacy is an extra-patrimonial right, which may even exceed the protections that a congressional, uniform data privacy act based in property could afford. Given the United States' interest in protecting corporations and the prevalence of data in the modern information-driven economy, this result seems unlikely. In the absence of broad data privacy regulation in the United States, the interests of consumers and organizations can be more effectively balanced as the arena of data protection develops by recognizing that property principles can and should apply to data, and acknowledging that data is a thing of property.[425]

---

419. Ritter & Meyer, *supra* note 12, 221–23.

420. *See generally* Kosseff, *supra* note 176, at 175.

421. *See generally* Lipton, *supra* note 46.

422. LA. REV. STAT. § 51:3074 (2019).

423. Ritter & Meyer, *supra* note 12, at 221–223.

424. Int'l News Serv. v. Associated Press, 248 U.S. 215, 264–67 (1918) (Brandeis, J., dissenting).

425. *See generally* Lipton, *supra* note 46; Ritter & Meyer, *supra* note 12, at 221–23.